ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Управління корпоративною інфраструктурою в середовищі Windows: використання доменних функцій для оптимізації розгортання та налаштування техніки»**

на здобуття освітнього ступеня бакалавра
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

_____ Євген ВОСКОЛУП
(підпис) *(Ім'я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр. КНД-41
Євген ВОСКОЛУП
(Ім'я, ПРІЗВИЩЕ)

Керівник: Микола ГНІДЕНКО
Науковий ступінь, вчене звання *(Ім'я, ПРІЗВИЩЕ)*

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерних наук

Ступінь вищої освіти «Бакалавр»

Спеціальність 122 «Комп'ютерні науки»

Освітньо-професійна програма «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерних наук

_____ Віктор ВИШНІВСЬКИЙ
«_____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Восколуп Євген Олександрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Управління корпоративною інфраструктурою в середовищі Windows: використання доменних функцій для оптимізації розгортання та налаштування техніки
керівник кваліфікаційної роботи Микола ГНІДЕНКО к.т.н, доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» 02.2024 р. №36
2. Строк подання кваліфікаційної роботи «31» травня 2024 р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, документація по використовуванню Server Manager, Microsoft Deployment Toolkit та Local Group Policy Editor.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
    1. Розгортання операційної системи за допомогою Windows Deployment Services та Microsoft Deployment Toolkit.
    2. Розгортка ПЗ та керування клієнтським ПК через групові політики.
    3. Робота з віддаленим доступом до робочих станцій.
5. Перелік графічного матеріалу:
    1. Мета роботи, об'єкт та предмет дослідження
    2. Методи розгортання

3. Опис основного функціоналу
4. Середовище використання автоматизованої системи
5. Підготовка ПК-Сервера
6. Первинні налаштування
7. Налаштування WDS та MDT
8. Імпортування ОС та ПЗ
9. Створення та налаштування сценарію
10. Генерація образу
11. Налаштування віддаленого підключення
12. Встановлення додаткового ПЗ
13. Висновки

6. Дата видачі завдання «23» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Літературний огляд теми	25.02-22.03.24	Виконано
2	Формулювання проблеми та мети дослідження	23.03-30.03.24	Виконано
3	Аналіз інструментів для управління корпоративною інфраструктурою в середовищі Windows	31.03-09.04.24	Виконано
4	Розробка методології дослідження	10.04-14.04.24	Виконано
5	Виконання практичних етапів дослідження	15.04-29.04.24	Виконано
6	Аналіз результатів дослідження	30.04-05.05.24	Виконано
7	Написання тексту дипломної роботи	06.05-11.05.24	Виконано
8	Редагування та оформлення дипломної роботи	12.05-15.05.24	Виконано

Здобувач вищої освіти _____ Євген ВОСКОЛУП
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Микола ГНІДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 56 сторінок, 75 рисунків, 10 джерел.

Мета роботи – вивчення методів розгортання операційних систем, розробка та реалізація ефективного процесу автоматизованого налаштування інфраструктури мережевого середовища з використанням різноманітних інструментів.

Об'єкт дослідження – процеси автоматизації розгортання та налаштування серверних та клієнтських операційних систем.

Предмет дослідження – інструменти для розгортання операційних систем, групові політики, налаштування віддаленого доступу, процеси автоматизації у сфері інформаційних технологій.

Короткий зміст роботи: у даній роботі досліджується та реалізується процес автоматизованого розгортання та налаштування серверних та клієнтських операційних систем у мережевому середовищі.

Для досягнення цієї мети використовуються такі інструменти, як VMware Workstation, Windows Deployment Services, Microsoft Deployment Toolkit, тощо. Робота включає в себе використання технологій віртуалізації.

У ході роботи детально розглядаються методи налаштування групових політик, зокрема для дозволу віддаленого управління та підтримки через Windows Remote Assistance. Також досліджується інтеграція з Active Directory для централізованого управління комп'ютерами та користувачами у доменній інфраструктурі.

КЛЮЧОВІ СЛОВА: ГРУПОВІ ПОЛІТИКИ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВІДДАЛЕНЕ КЕРУВАННЯ, АВТОМАТИЗОВАНЕ РОЗГОРТАННЯ

ABSTRACT

Text part of the qualification work for the bachelor's degree: 56 pages, 75 pictures, 10 sources.

The aim of the work – to study methods of operating system deployment, development, and implementation of an efficient process for automated configuration of network environment infrastructure using various tools.

The object of research – the processes of automating the deployment and configuration of server and client operating systems.

The subject of research – tools for operating system deployment, group policies, remote access configuration, automation processes in the field of information technology.

Summary of the work: this paper explores and implements the process of automated deployment and configuration of server and client operating systems in a networked environment.

To achieve this goal, tools such as VMware Workstation, Windows Deployment Services, and Microsoft Deployment Toolkit are utilized. The work involves the use of virtualization technologies.

The methods for configuring group policies are examined in detail, particularly for enabling remote management and support through Windows Remote Assistance. Additionally, the integration with Active Directory for centralized management of computers and users in a domain infrastructure is investigated.

KEYWORDS: GROUP POLICIES, SOFTWARE, REMOTE MANAGEMENT, AUTOMATED DEPLOYMENT.

ЗМІСТ

Стор.

ВСТУП

У сучасному корпоративному середовищі ефективне управління інфраструктурою є однією з ключових складових успіху для підтримки бізнес-процесів і забезпечення безперебійної роботи. Зокрема, управління технічним парком компанії, його розгортання та налаштування, є важливим аспектом інформаційної стратегії підприємства. У цьому контексті, використання сучасних засобів та технологій, які надає платформа Windows, стає ключовим фактором для забезпечення оптимальної продуктивності та безпеки IT-середовища.

Ця дипломна робота присвячена дослідженню та розробці практичних рішень у сфері управління корпоративною інфраструктурою в середовищі Windows. Ключовою метою роботи є аналіз та впровадження ефективних стратегій встановлення операційних систем, розгортання та налаштування нової техніки та техніки, що вже знаходиться у використанні з використанням доменних функцій. Під час дослідження буде розглянуто такі аспекти, як вибір оптимальних конфігурацій встановлення операційних систем, встановлення необхідного програмного забезпечення з заданою конфігурацією та налаштування параметрів системи для максимальної продуктивності.

Окрім того, робота присвячена аналізу і впровадженню методів контролю та моніторингу технічного парку компанії на основі доменних політик Windows. Використання цих інструментів дозволить підприємствам забезпечити високий рівень безпеки, дотримання стандартів та ефективне управління ресурсами. Крім того, буде розглянуто можливості віддаленого управління технічним парком за допомогою інструментів, таких як RDP та msra, що є важливим аспектом сучасного корпоративного IT-управління.

Далі в роботі будуть розглянуті основні аспекти теми, проведено аналіз існуючих підходів та технологій, а також наведено практичні рекомендації та висновки щодо оптимальних стратегій управління корпоративною інфраструктурою в середовищі Windows.

1 ОБҐРУНТУВАННЯ МЕТОДІВ І ТЕХНОЛОГІЙ

1.1 Методи розгортання

У сучасних корпоративних середовищах виникає необхідність у швидкому, ефективному та автоматизованому розгортанні операційних систем та програм на комп'ютерах для забезпечення безперебійної роботи працівників та оптимізації управління IT-інфраструктурою. Існує декілька методів, які зазвичай використовуються компанії для розгортання операційних систем у корпоративних середовищах:

1. Ручне розгортання - один з найбільш простих, але в той же час часо- та ресурсозатратних методів розгортання ОС - це ручне встановлення ОС та необхідного програмного забезпечення на кожному комп'ютері вручну. Цей метод зазвичай використовується у невеликих компаніях або при рідкісному розгортанні нових комп'ютерів. Він передбачає фізичну присутність адміністратора для кожного комп'ютера під час процесу встановлення, що робить його непрактичним для масштабних проектів.

2. Масове розгортання - метод масового розгортання передбачає автоматизацію процесу встановлення ОС та необхідного програмного забезпечення на багатьох комп'ютерах одночасно за допомогою спеціального програмного забезпечення. Такі інструменти як Microsoft Deployment Toolkit (MDT) або дозволяють адміністраторам значно економити час та зусилля, що зазвичай витрачаються на ручне розгортання. Метод працює завдяки розгортанню через мережу, зазвичай через протокол PXE, та широко використовується в корпоративних середовищах будь-якого масштабу.

Доменні функції у Windows надають можливості автоматичного розгортання ОС, управління політиками безпеки та централізованого управління. Ці функції спрощують та оптимізують процеси розгортання та налаштування комп'ютерної техніки в корпоративних середовищах, включаючи:

1. Автоматичне розгортання та оновлення ОС - використання доменних функцій дозволяє налаштувати процес автоматичного розгортання операційних систем на комп'ютерах, що приєднуються до домену. Це забезпечує консистентність установки та оновлення ОС та програмного забезпечення на всіх пристроях у мережі.

2. Управління політиками безпеки- за допомогою доменних політик безпеки адміністратори можуть створювати правила та обмеження для комп'ютерів у домені. Це включає в себе налаштування параметрів безпеки, таких як політики паролів, обмеження доступу до файлів та додатків, а також застосування патчів і оновлень безпеки. Управління політиками безпеки забезпечує високий рівень безпеки та стабільності інфраструктури.

3. Централізоване управління - доменні функції дозволяють адміністраторам централізовано керувати всією інфраструктурою комп'ютерів у домені. Це включає в себе надання прав доступу, управління ресурсами та службами, моніторинг та збір даних про пристрої в мережі. Централізоване управління спрощує процеси адміністрування, забезпечуючи однорідність та стандартизацію конфігурацій комп'ютерів.

1.2 Опис функціоналу GPO, RDP та MSRA

Group Policy Objects (GPO) - це ключовий компонент в адмініструванні Windows-системами в корпоративних мережах. Вони надають адміністраторам засоби для централізованого керування налаштуваннями комп'ютерів та користувацьких облікових записів.

GPO дозволяють адміністраторам встановлювати, змінювати та керувати різноманітними параметрами налаштувань для комп'ютерів та користувачів у мережі. Це можуть бути політики безпеки, налаштування проксі, обмеження доступу до файлів, налаштування мережі тощо.

Адміністратори можуть створювати різні GPO для різних груп користувачів чи комп'ютерів. Це дозволяє точно налаштовувати параметри в залежності від потреб цих груп.

GPO мають механізм визначення пріоритетності налаштувань. Це означає, що якщо налаштування в різних GPO конфліктують між собою, буде використане налаштування з вищим пріоритетом.

Налаштування, встановлені на вищому рівні (наприклад, на рівні домену), можуть успадковуватися на нижчі рівні (наприклад, на рівні організаційних одиниць).

Після зміни GPO, налаштування автоматично поширюються на всі комп'ютери та користувачі відповідно до правил реплікації.

GPO надають можливість моніторити стан налаштувань та генерувати звіти про їх виконання.

Крім централізованих GPO, Windows також підтримує локальні групові політики, які можуть бути використані для налаштування окремих комп'ютерів.

GPO дозволяють встановлювати правила безпеки, такі як складність паролів, обмеження доступу до ресурсів, шифрування даних тощо, на всіх комп'ютерах у мережі з централізованого місця.

Remote Desktop Protocol (RDP) - це протокол, який дозволяє користувачам віддалено керувати комп'ютером через мережу. Основна ідея RDP полягає в тому, що користувач може підключитися до іншого комп'ютера, використовуючи віддалене робоче середовище, і взаємодіяти з ним, якби він був присутній перед цим комп'ютером фізично.

RDP дозволяє користувачам отримати доступ до віддаленого комп'ютера з будь-якого місця, що має мережеве підключення. Це особливо корисно для адміністраторів систем, які потребують доступу до серверів або інших комп'ютерів у мережі з будь-якого місця.

Користувачі можуть віддалено керувати комп'ютером, виконуючи різні операції, такі як запуск програм, керування файлами, налаштування системи тощо.

Підключений користувач може мати доступ до ресурсів, що знаходяться на віддаленому комп'ютері, таких як файли, друкувальні пристрої та інші пристрої.

RDP може бути використаний для спільного використання робочого столу між декількома користувачами, дозволяючи їм одночасно взаємодіяти з одним комп'ютером.

Для забезпечення безпеки, RDP шифрує всі дані, які передаються між віддаленим комп'ютером та клієнтом.

RDP підтримує передачу аудіо та відео між віддаленим комп'ютером та клієнтом, що дозволяє користувачам працювати з мультимедійним вмістом на віддаленому комп'ютері.

MSRA (Microsoft Remote Assistance) - це інструмент, який дозволяє користувачам взаємодіяти з комп'ютером іншого користувача в режимі реального часу через мережу.

MSRA надає можливість одному користувачеві надавати допомогу іншому користувачеві, який має проблеми з комп'ютером. Це дозволяє швидко вирішувати технічні проблеми та надавати підтримку без необхідності фізично присутнього адміністратора.

За допомогою MSRA, допоміжний користувач може взаємодіяти з комп'ютером в режимі реального часу, спостерігати за діями основного користувача та надавати вказівки або вирішувати проблеми.

MSRA дозволяє користувачам контролювати рівень доступу допоміжного користувача до свого комп'ютера. Основний користувач може надати допоміжному користувачу повний доступ або обмежити його можливості взаємодії з системою.

MSRA забезпечує захищений канал зв'язку між комп'ютерами, що використовують шифрування для захисту від несанкціонованого доступу.

Під час сеансу допомоги, основний користувач може поділитися своїм робочим столом з допоміжним користувачем, щоб той міг переглядати та взаємодіяти з програмами та файлами.

MSRA дозволяє обмінюватися діалоговими вікнами між основним та допоміжним користувачем, що спрощує процес спільної роботи та вирішення проблем.

2 ПІДГОТОВКА ІНФРАСТРУКТУРИ

2.1 Середовище використання

Для початку зазначу середовище та вимоги, де може використовуватись рішення представлене у цій дипломній роботі.

У рамках інфраструктури офісу повинна бути наявна локальна мережа (LAN), яка є ключовим елементом забезпечення зв'язку між комп'ютерами, принтерами та іншими мережевими пристроями в офісі. Ця мережа дозволяє спільний доступ до ресурсів, обмін даними та забезпечує комунікацію між співробітниками.

В залежності від масштабування офісу LAN складається з розгалужених мережевих комутаторів та маршрутизаторів, які забезпечують підключення до локальної мережі та до зовнішніх ресурсів Інтернету. Також в мережі присутні сервери, що забезпечують доступ до спільних ресурсів та додаткових послуг, таких як сховище даних, електронна пошта та інші.

В мережі можуть бути реалізовані заходи безпеки, такі як використання паролів, шифрування даних, фаєрвол та інші методи захисту для забезпечення конфіденційності та цілісності інформації, що передається через мережу, тому слід заздалегідь розблокувати порти, які використовує Microsoft Deployment Toolkit, а саме:

1. TCP порт 135 - використовується для прийому запитів на віддалену допомогу у MSRA.

2. TCP порт 139 - для доступу до файлового сервера або розподіленого сховища, де знаходяться образи операційних систем та програм.

3. TCP порт 445 - аналогічно, для доступу до файлового сервера або сховища.

4. TCP порт 3389 - для віддаленого доступу до серверів, де розміщені засоби MDT.

В моєму випадку нема великої кількості обладнання, тому для створення віртуальних машин у рамках дипломної роботи використовуватиму програмне забезпечення VMware Workstation. VMware Workstation є одним з провідних рішень

у галузі віртуалізації, що надає можливість створення, налаштування та управління віртуальними середовищами.

Це програмне забезпечення дозволяє ефективно використовувати ресурси комп'ютера для створення та розгортання віртуальних машин, що дозволяє проводити тестування, розробку та експерименти з різними операційними системами та програмним забезпеченням без необхідності фізичного наявності окремих пристроїв.

Для ефективного виконання завдань буде створена віртуальна машина, яка імітуватиме серверне середовище. Ця віртуальна машина буде налаштована з 6 ядрами процесора та 4 гігабайтами оперативної пам'яті.

Використання такої конфігурації дозволить забезпечити оптимальну продуктивність та ресурси для виконання різноманітних завдань, пов'язаних з дослідженням та розробкою програмного забезпечення, в тому числі і для тестування великих серверних застосунків.

Для реалізації серверного середовища був використаний образ операційної системи Windows Server 2022, англомовна версія, що завантажена з офіційного веб-сайту Microsoft, посилання зазначено у списку використаних джерел.

Цей образ забезпечує доступ до останніх функцій та можливостей, які пропонує Windows Server 2022, що дозволяє ефективно використовувати різноманітні серверні додатки та сервіси.

2.2 Підготовка ПК-Сервера

Після завантаження образу Windows Server 2022 він був інтегрований у віртуальну машину.

Після завантаження віртуальної машини з образу Windows Server 2022, процес встановлення розпочався за допомогою інтерактивного інсталятора, який надавав можливість вибору мови, редакції, та інших параметрів конфігурації.

Після цього було обрано відповідну редакцію, а саме Windows Server 2022 Standard Evaluation з рідним інтерфейсом (Desktop Experience) та тип установки, включаючи вибір простору для установки операційної системи. Після завершення

цих кроків та введення необхідних параметрів, процес встановлення розпочався, і Windows Server 2022 був успішно інстальований на віртуальну машину.

Обрана редакція Windows Server 2022 Standard Evaluation з Desktop Experience забезпечує повноцінне графічне середовище та широкий спектр можливостей для розгортання серверних додатків та послуг, що робить її ідеальним вибором для цілей дослідження та розробки.

У версії Windows Server 2022 без Desktop Experience, користувач отримує операційну систему, яка працює в режимі Core, тобто без графічного інтерфейсу користувача. Це означає, що доступ до операційної системи здійснюється лише через командний рядок або віддалено з іншого комп'ютера за допомогою інструментів управління віддаленими серверами. Вибір цієї версії може бути доцільним у випадках, коли важлива ефективність ресурсів та безпека, оскільки вона має менший обсяг системи та менше потребує ресурсів комп'ютера, порівняно з версією з Desktop Experience.

Після успішного завершення процесу встановлення та першого входу у систему, зазвичай користувачі одразу потрапляють у Server Manager - це централізоване керувальне вікно, яке надає доступ до різноманітних інструментів управління та моніторингу сервера. Server Manager є ключовим інструментом для адміністрування операційної системи Windows Server 2022 та його функціональність включає в себе управління серверними ролями та функціями, моніторинг стану системи, установку та управління програмним забезпеченням, а також доступ до інших адміністративних інструментів. Server Manager дозволяє адміністраторам керувати декількома серверами з одного місця. Це зменшує час, необхідний для управління кожним сервером окремо. Він допомагає виконувати оновлення для операційних систем, ролей та функцій, а також налаштовувати параметри безпеки та мережі. Server Manager дозволяє створювати та планувати автоматичні завдання для виконання різних операцій на сервері при цьому надає зручний та інтуїтивно зрозумілий інтерфейс для ефективного управління сервером та його ресурсами (рис. 2.1).

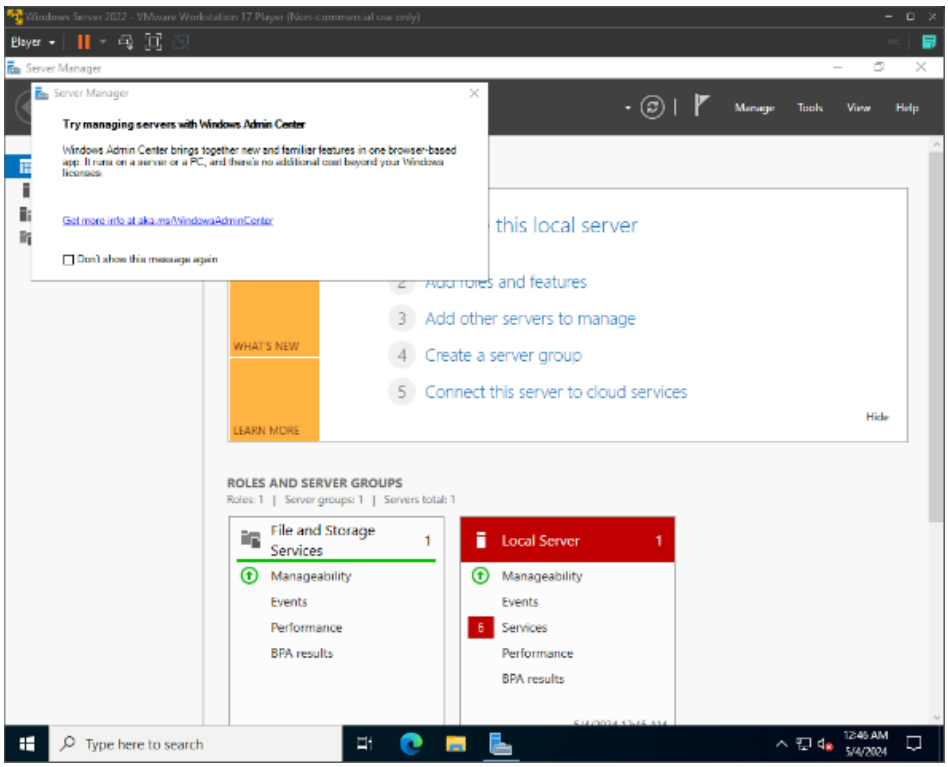


Рис. 2.1 Вікно Server Manager

В самому Server Manager, було виконано кілька кроків для налаштування сервера. Спочатку було змінено ім'я комп'ютера на 'DeployServer' для відповідності конкретним функціональним завданням (рис. 2.2).

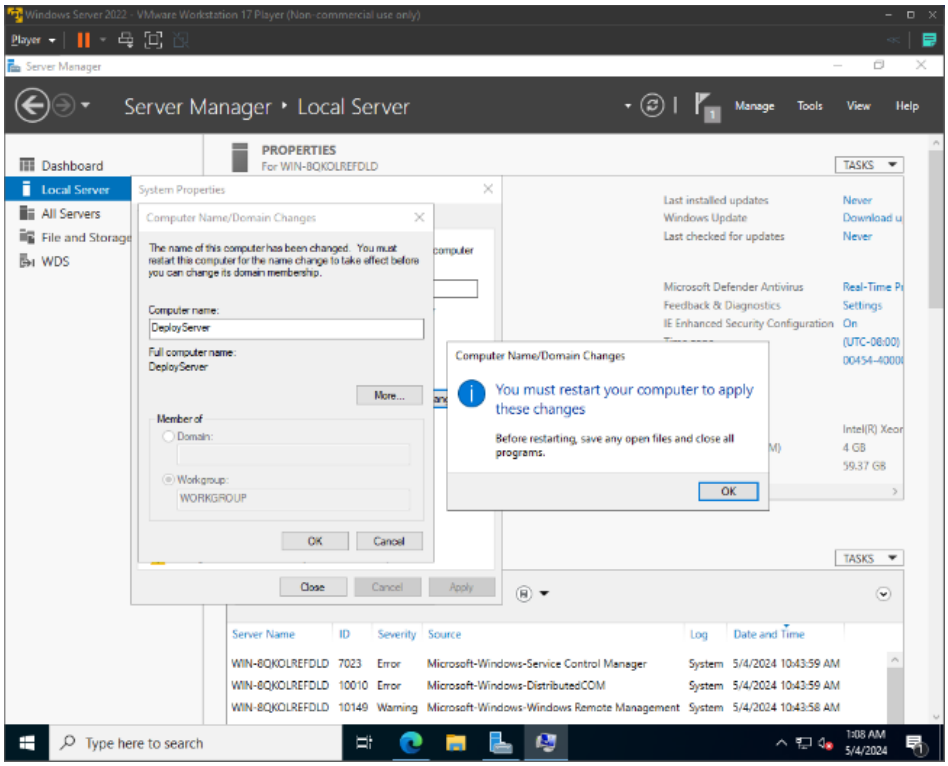


Рис. 2.2 Змінення ім’я ПК-Сервера на DeployServer

Після цього було налаштовано статичну IP-адресу для сервера з наступними параметрами (рис. 2.3):

IP адреса: 192.168.92.100

Маска: 255.255.255.0

Шлюз: 192.168.92.2

DNS: 1.1.1.1

Альтернативний DNS: 1.0.0.1

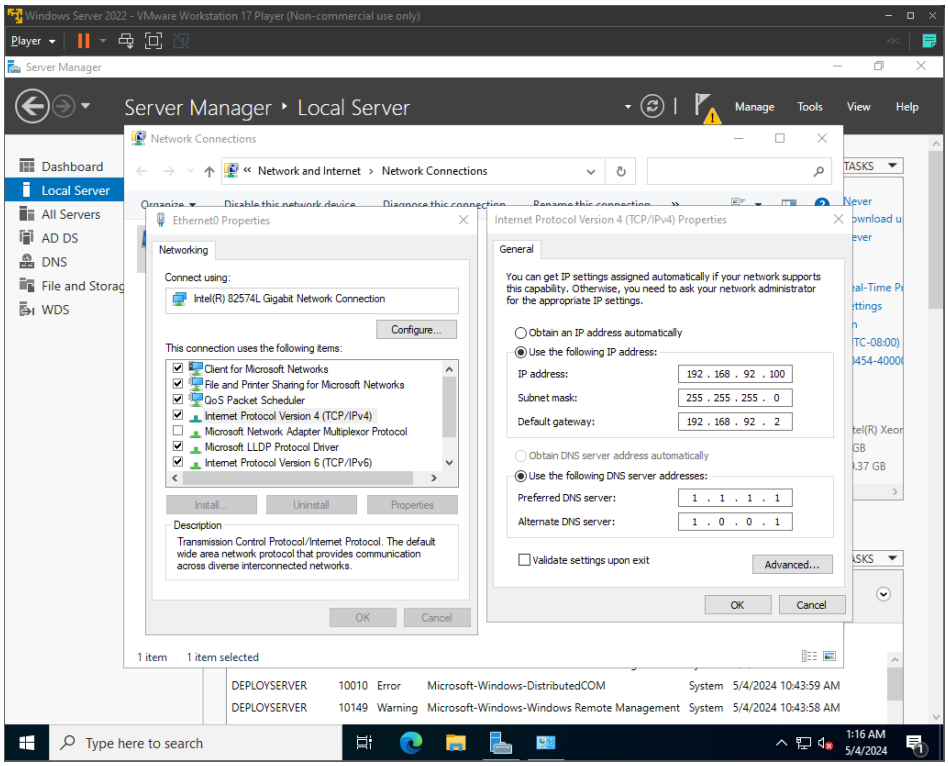


Рис. 2.3 Змінення конфігурації мережевого адаптера

Ці налаштування були виконані з використанням інструментів управління мережею в опціях конфігурації сервера. Застосування статичного IP-адресу дозволить забезпечити стале підключення до сервера та ефективну роботу мережі в цілому.

Після перезавантаження сервера, крок за кроком була встановлена доменна система Active Directory для управління мережею та ресурсами. Спочатку, в Server Manager, у розділі 'Manage' було обрано опцію 'Add Roles and Features', де були вибрані серверні ролі 'Active Directory Domain Services' та 'DNS Server' (рис. 2.4).

Після цього, в процесі конфігурації цих ролей, було встановлено параметри, відповідні конкретним потребам системи.

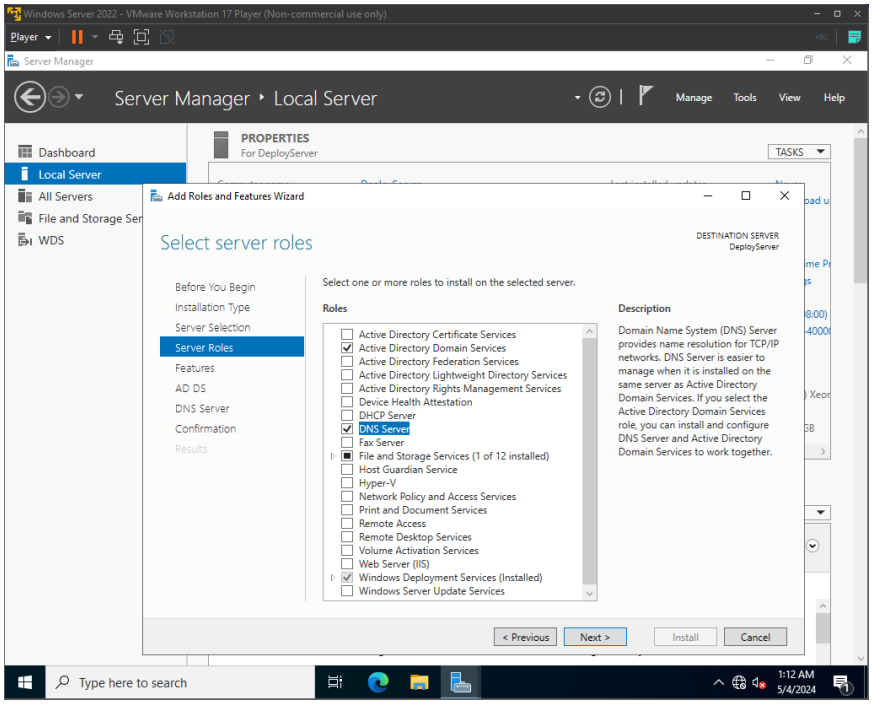


Рис. 2.4 Додавання ролей AD та DNS Server

Для створення нового дерева каталогів була використана опція 'Deployment Configuration', де був створений новий ліс з ім'ям 'Voskolup.Organization' (рис. 2.5). Це ліс є високорівневим контейнером для усіх об'єктів Active Directory в мережі.

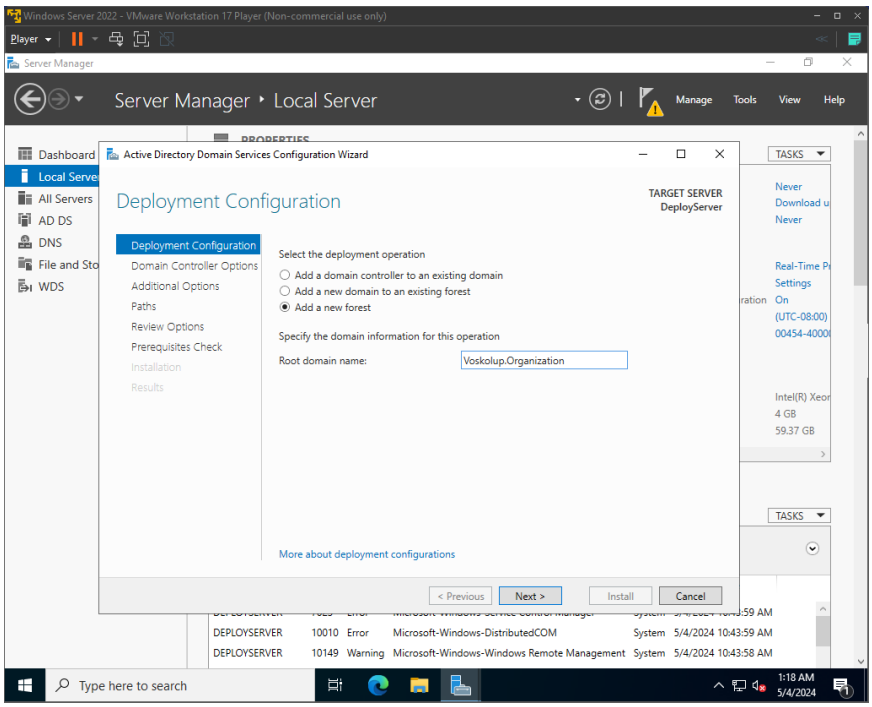


Рис. 2.5 Створення лісу з ім’ям Voskolup.Organization

Після вказання імені кореневого домену, було встановлено DSRM (Directory Services Restore Mode) пароль, який використовується для відновлення служби каталогів в разі потреби (рис. 2.6).

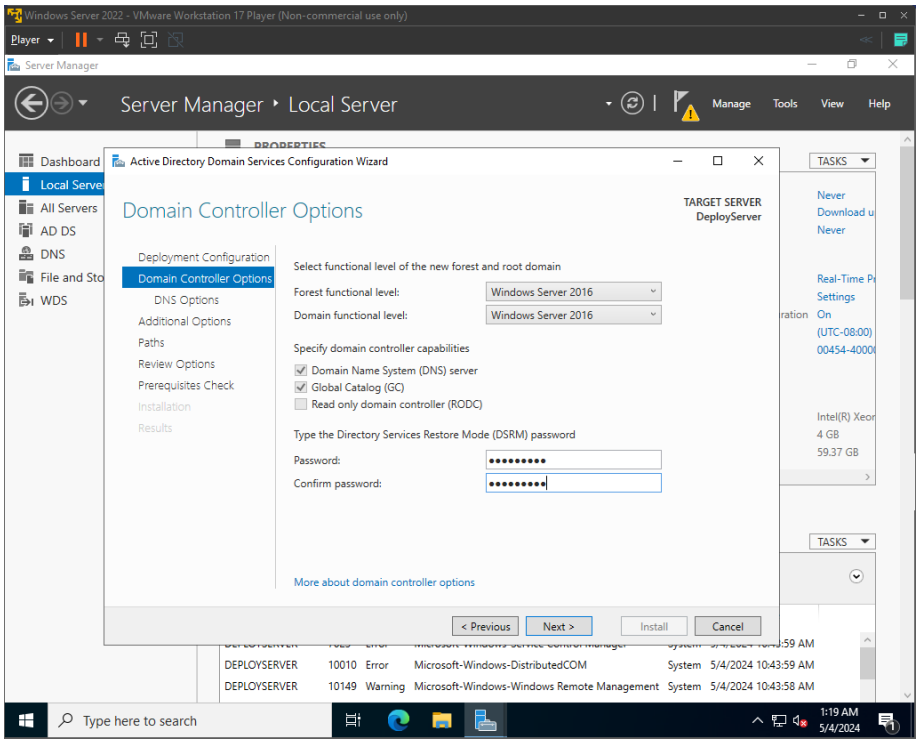


Рис. 2.6 Встановлення паролю DSRM

Також було вказано ім'я NetBIOS для домену - 'VOSKOLUP' (рис. 2.7).

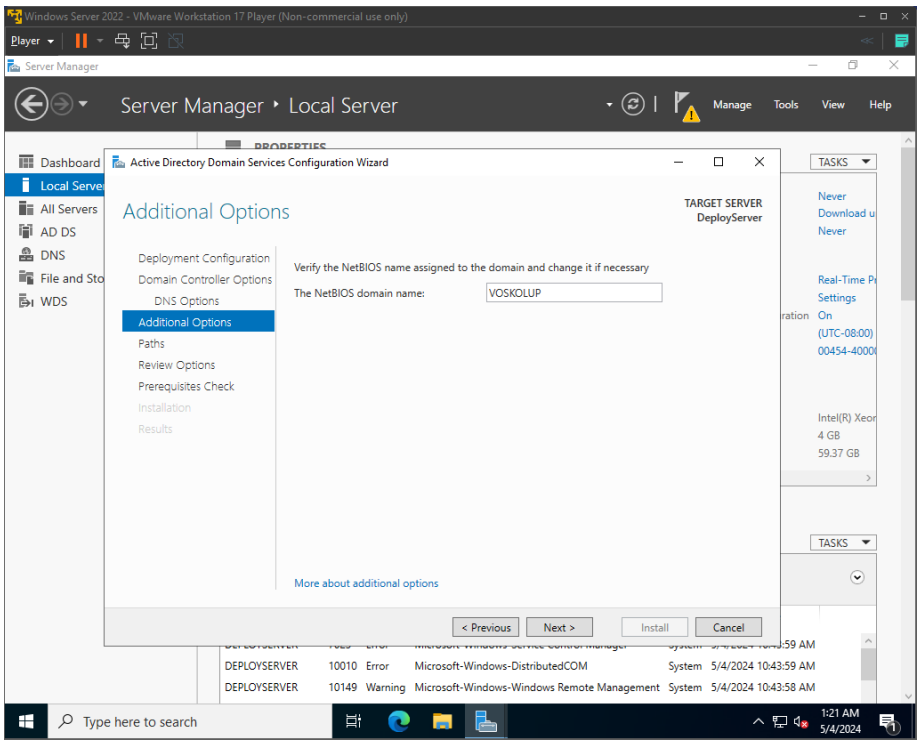


Рис. 2.7 Задання імені NetBIOS

Після завершення установки Active Directory та DNS Server ролей, система була перезавантажена для застосування змін. Це дозволило активувати нову конфігурацію та забезпечити правильне функціонування доменної системи Active Directory з урахуванням зазначених параметрів. Тепер система готова до додавання користувачів, груп, ресурсів та інших об'єктів для подальшого управління мережею та обміном ресурсами в рамках доменної структури 'Voskolup.Organization'.

Після успішної установки та налаштування Active Directory та DNS Server, треба додати ще один важливий компонент - Windows Deployment Services (WDS). Цей інструмент і буде надавати можливість розгортання операційних систем через мережу.

Для цього, в Server Manager, було вибрано опцію 'Add Roles and Features', а потім обрано роль 'Windows Deployment Services' (рис. 2.8).

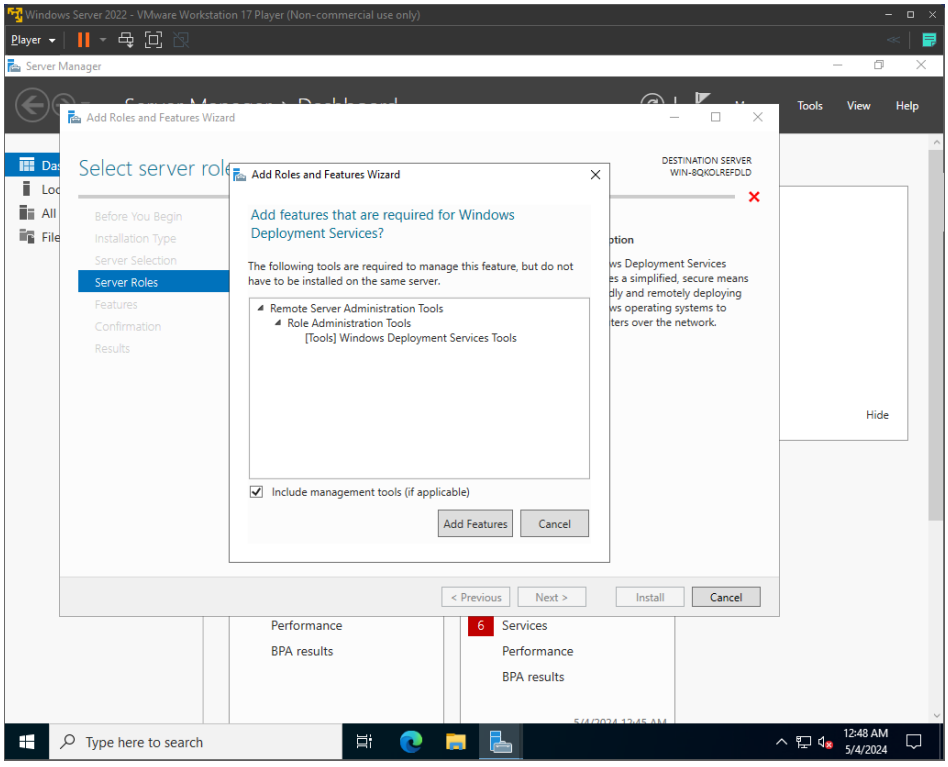


Рис. 2.8 Додавання ролі WDS

Після вибору ролі, в процесі конфігурації були встановлені галочки напроти опцій 'Deployment Server' та 'Transport Server' (рис. 2.9).

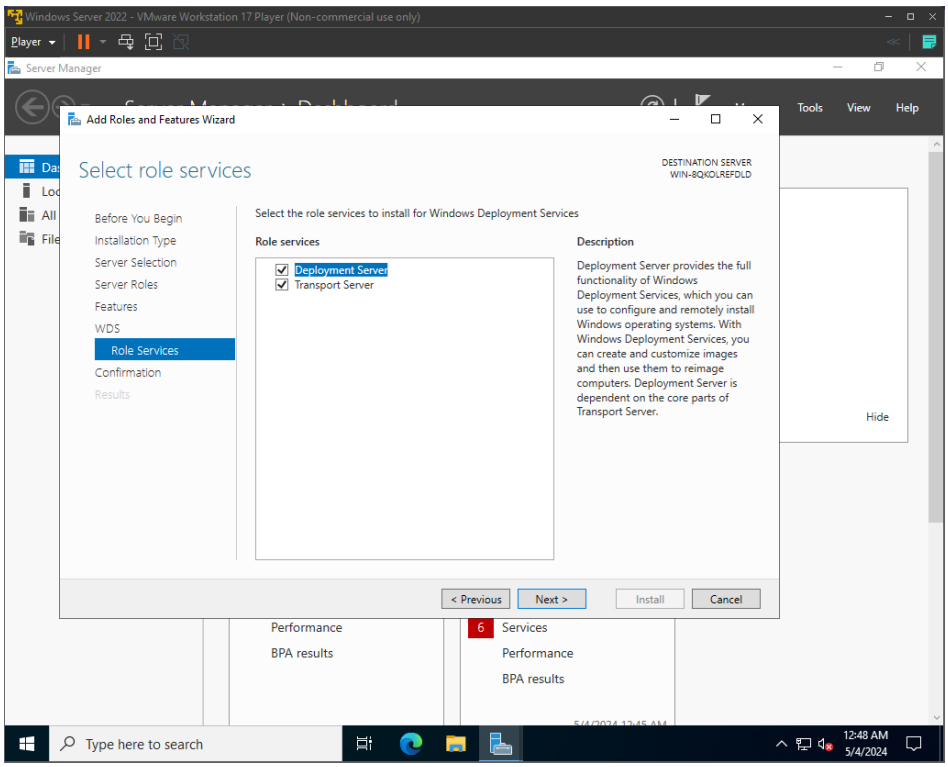


Рис. 2.9 Активація Deployment та Transport серверів

Deployment Server відповідає за розгортання образів операційних систем та інших компонентів через мережу, в той час як Transport Server забезпечує передачу даних між сервером та клієнтськими комп'ютерами під час розгортання.

Після налаштування ролі Windows Deployment Services на сервері, потрібно додатково встановити Microsoft Deployment Toolkit (MDT) та необхідні компоненти, щоб забезпечити більш гнучке та ефективне управління розгортанням операційних систем через мережу.

Для цього, з сайту Microsoft було завантажено та встановлено Microsoft Deployment Toolkit. MDT є інструментом для автоматизації та спрощення розгортання операційних систем, додатків та налаштувань на комп'ютерах. Встановлення MDT дозволяє забезпечити централізоване управління розгортанням, створювати та налаштовувати образи операційних систем та додаткові параметри для розгортання, серед них можуть бути драйвери, оновлення та програмне забезпечення (рис. 2.10). MDT легко інтегрується з іншими інструментами Microsoft, серед них – Windows Deployment Services, що і був завантажений раніше.

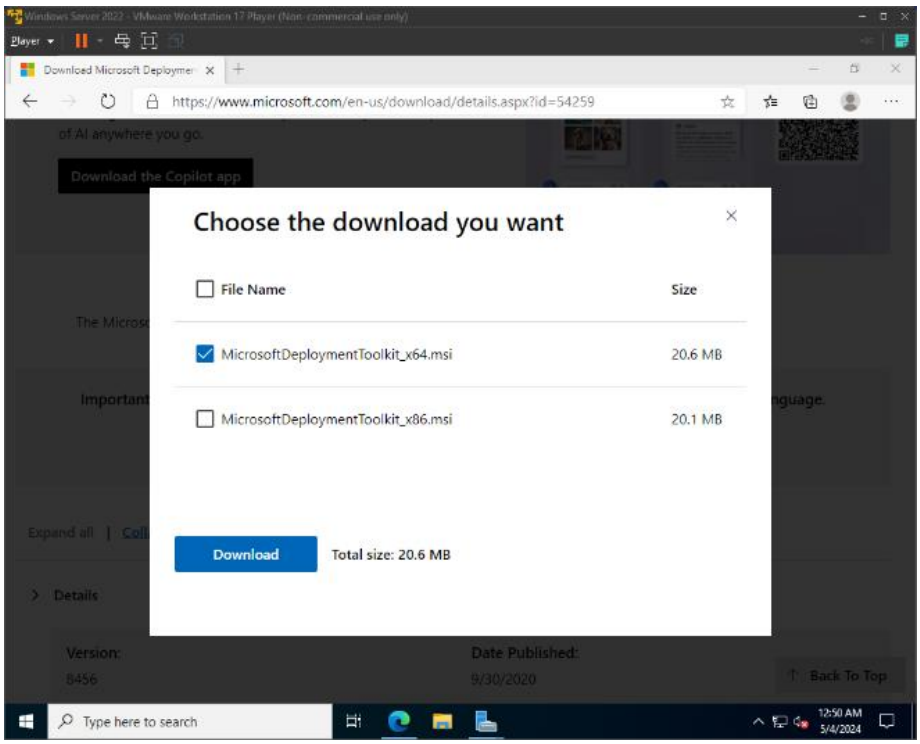


Рис. 2.10 Завантаження Microsoft Deployment Toolkit

Також було встановлено Windows Assessment and Deployment Kit (ADK) версії September 2023, яке містить інструменти та ресурси для автоматизованого розгортання Windows, включаючи інструменти для створення та налаштування образів Windows та Windows PE (рис. 2.11).

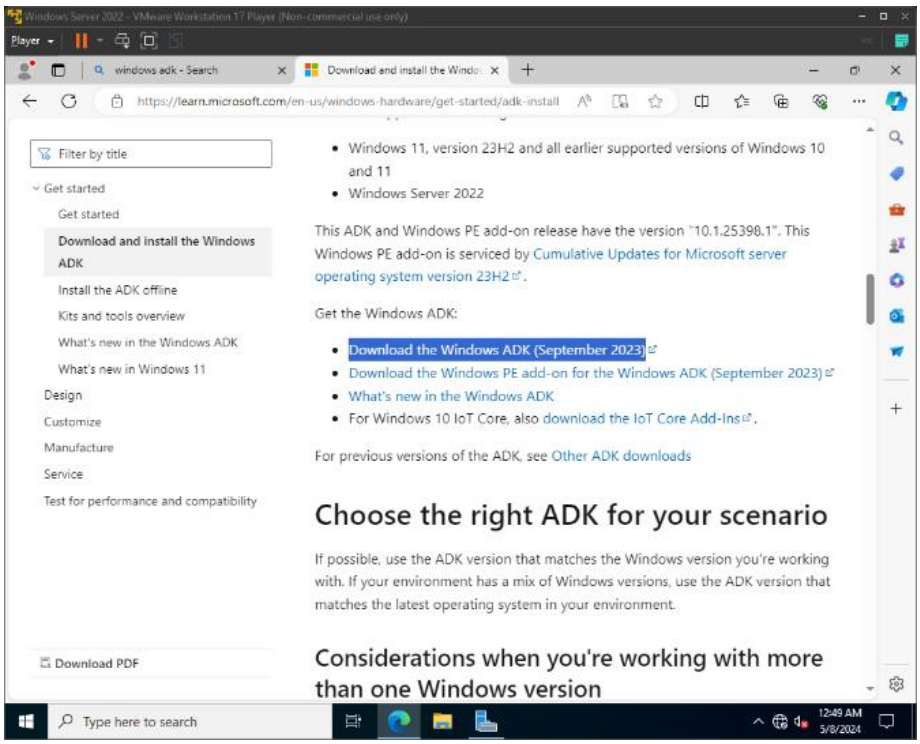


Рис. 2.11 Завантаження Windows ADK

Оскільки нова версія аддону Windows PE не має підтримки 32-бітних систем, було встановлено Windows PE add-on для Windows ADK для Windows 10 версії 2004 (рис. 2.12). Це забезпечить підтримку 32-бітних систем для конфігурації та розгортання образів операційних систем через мережу.

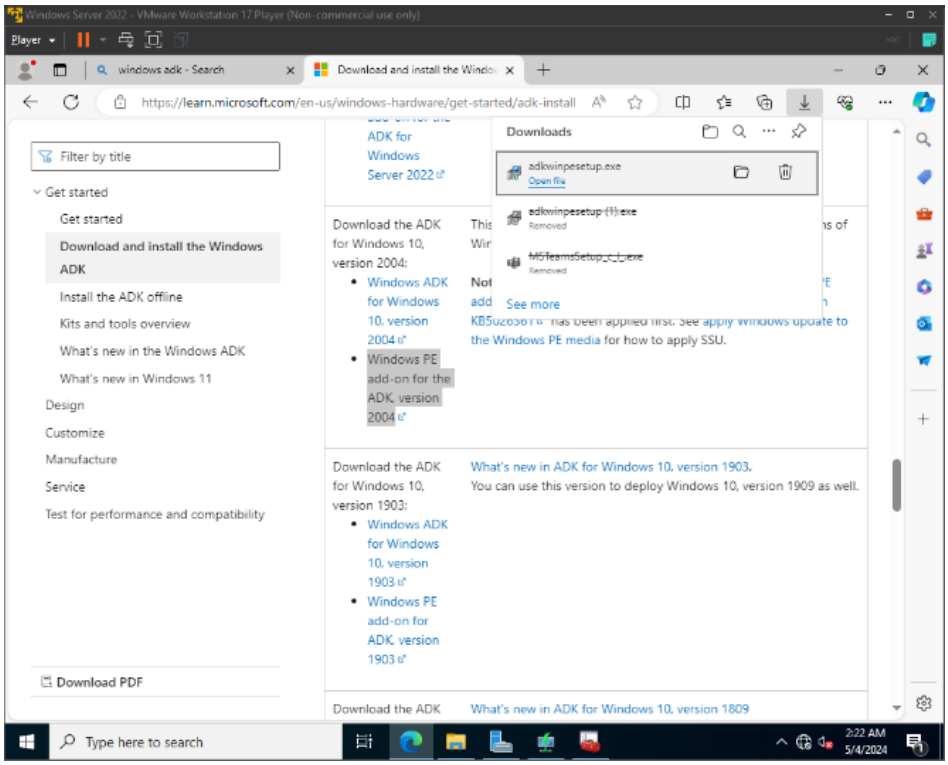


Рис. 2.12 Завантаження Windows PE add-on

2.3 Налаштування служби розгортання Windows

У конфігурації сервера Windows Deployment Services були здійснені деякі важливі кроки, щоб забезпечити правильну роботу служби розгортання операційних систем через мережу.

Спочатку була обрана опція інсталяції "Integrated with Active Directory" (рис. 2.13). Це означає, що Windows Deployment Services буде інтегровано зі службою каталогів Active Directory, що дозволить управляти розгортанням операційних систем через мережу з використанням доменної аутентифікації та авторизації.

Політики безпеки, які налаштовуються у домені Active Directory, можуть бути застосовані до комп'ютерів, які розгортані за допомогою WDS. Це дозволяє стандартизувати налаштування безпеки та забезпечити дотримання корпоративних стандартів безпеки для всіх комп'ютерів у мережі.

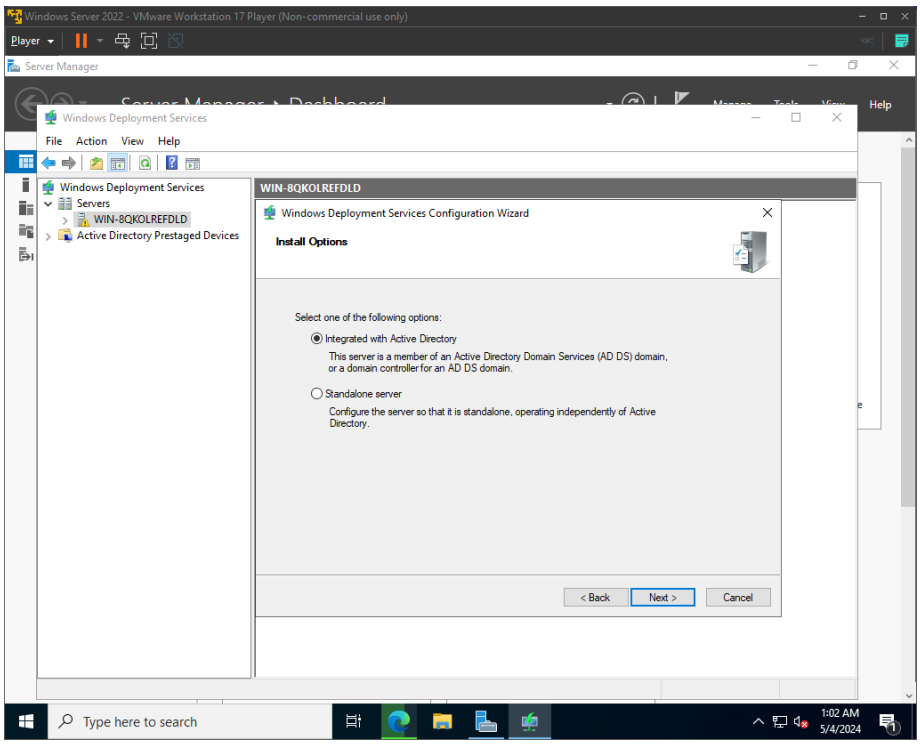


Рис. 2.13 Увімкнення інтеграції з AD

Шлях до папки інсталяції залишено за замовчуванням, тобто C:\RemoteInstall (рис. 2.14). Це стандартне місце розташування, де зберігаються файли та налаштування для розгортання операційних систем через мережу за допомогою Windows Deployment Services.

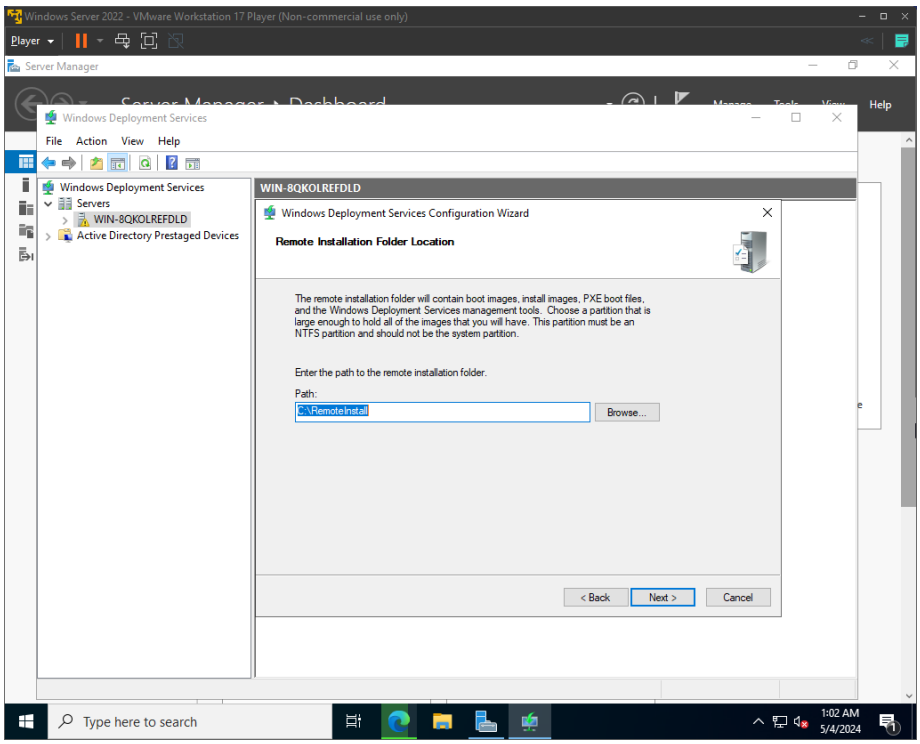


Рис. 2.14 Задання шляху для віддаленої інсталяції

У розділі PXE Server Initial Settings була вибрана опція "Respond to all client computers (known and unknown)" (рис. 2.15). Це означає, що служба буде реагувати на запити PXE від усіх клієнтських комп'ютерів, незалежно від того, чи вони відомі системі (зареєстровані в Active Directory) чи невідомі. Це дає можливість розгортати операційні системи на будь-які комп'ютери у мережі, що робить процес розгортання більш гнучким та універсальним.

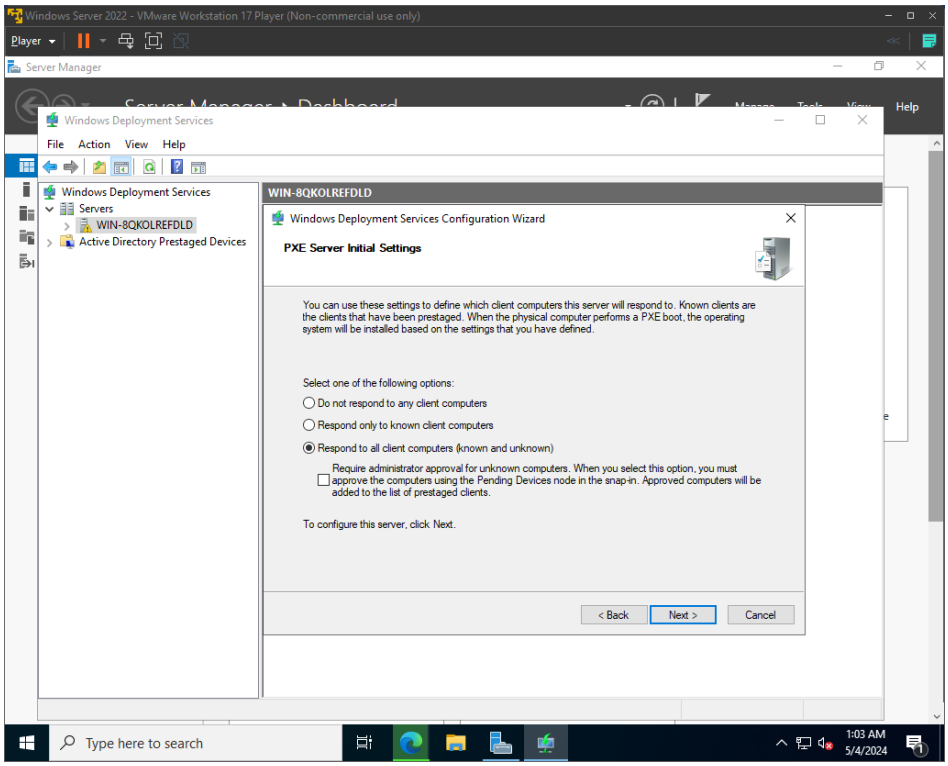


Рис. 2.15 Увімкнення реагування на всі запити PXE

У DeploymentWorkbench був налаштований новий Deployment Share для забезпечення доступу до ресурсів, необхідних для розгортання операційних систем та інших компонентів у мережевому середовищі.

Шлях до Deployment Share був вказаний як C:\DeploymentShare (рис. 2.16), що є стандартним місцем розташування для Deployment Shares в Microsoft Deployment Toolkit (MDT). Вказана папка на сервері або на локальному комп'ютері буде використовуватися для зберігання образів операційних систем, драйверів, сценаріїв автоматизації та інших компонентів, необхідних для розгортання.

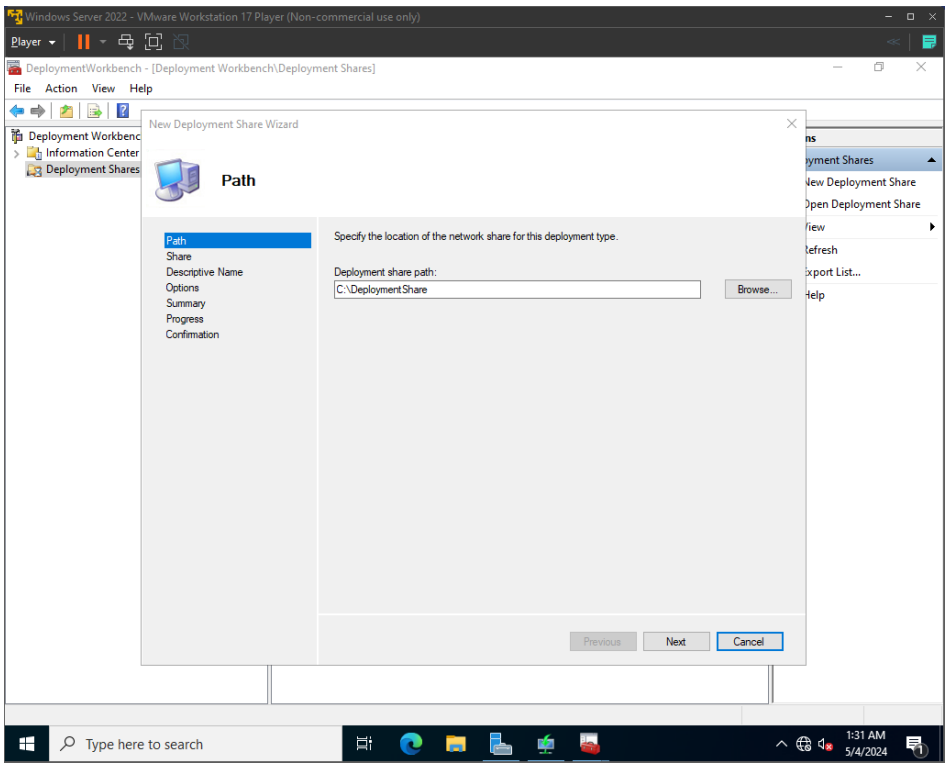


Рис. 2.16 Задання шляху для Deployment Share

Share name було задано як DeploymentShare$ (рис. 2.17), що дозволить доступ до ресурсів за допомогою мережі, використовуючи шлях \\DEPLOYSERVER\DeploymentShare$.

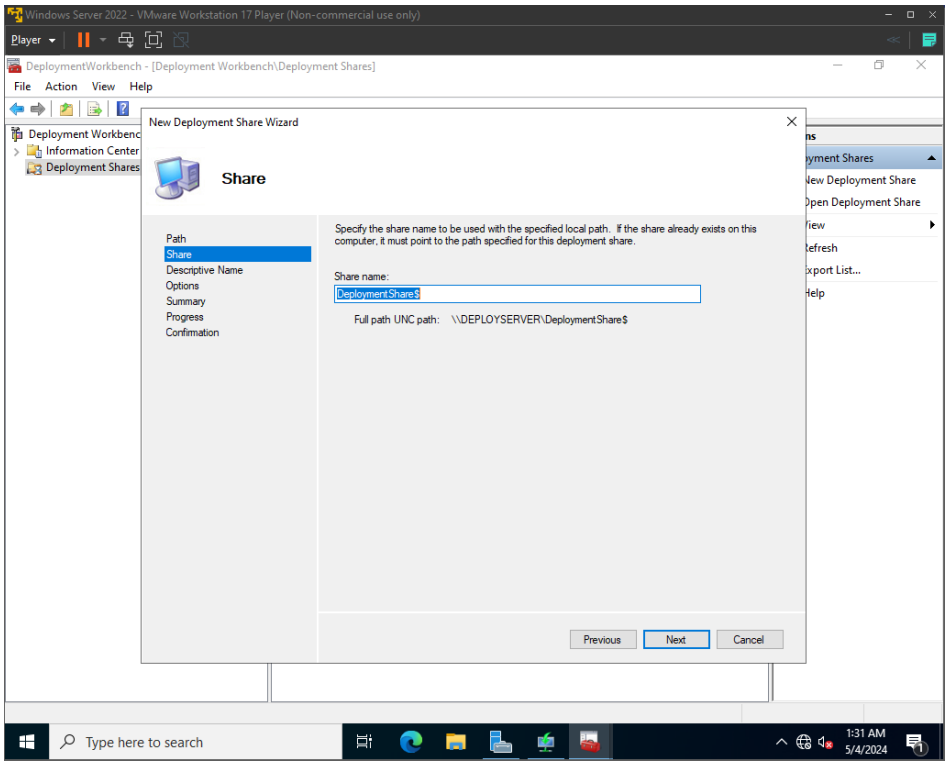


Рис. 2.17 Задання ім’я для Deployment Share

Додатково, для підвищення зручності та доступності ресурсів, Deployment share description було встановлено як "MDT Deployment Share" (рис. 2.18), що дозволить легко ідентифікувати цей ресурс в мережі.

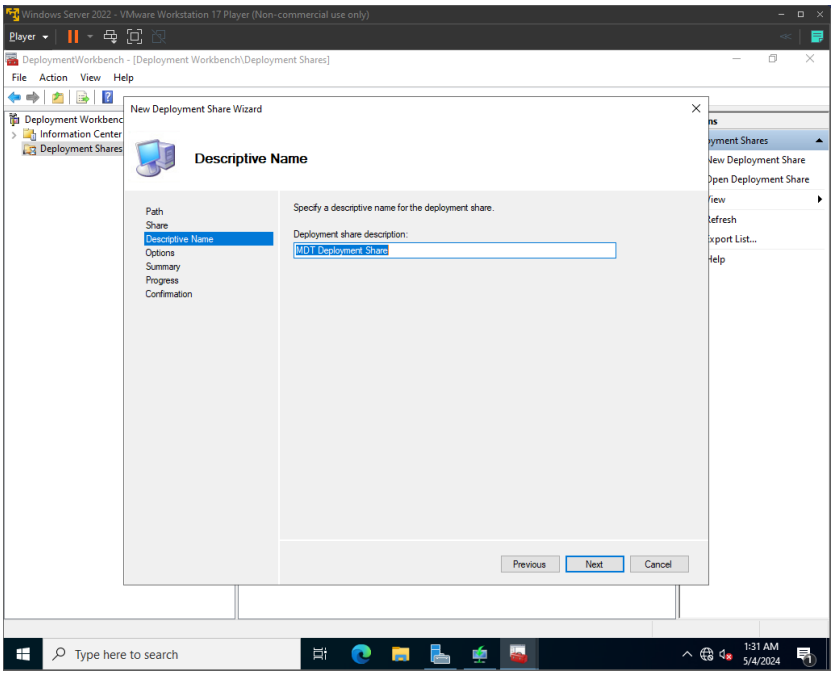


Рис. 2.18 Задання опису для Deployment Share

У конфігурації Deployment Share були залишені галочки, які стояли по замовчуванню, що відповідають базовим налаштуванням (рис. 2.19). Проте ця конфігурація буде змінена та доповнена пізніше.

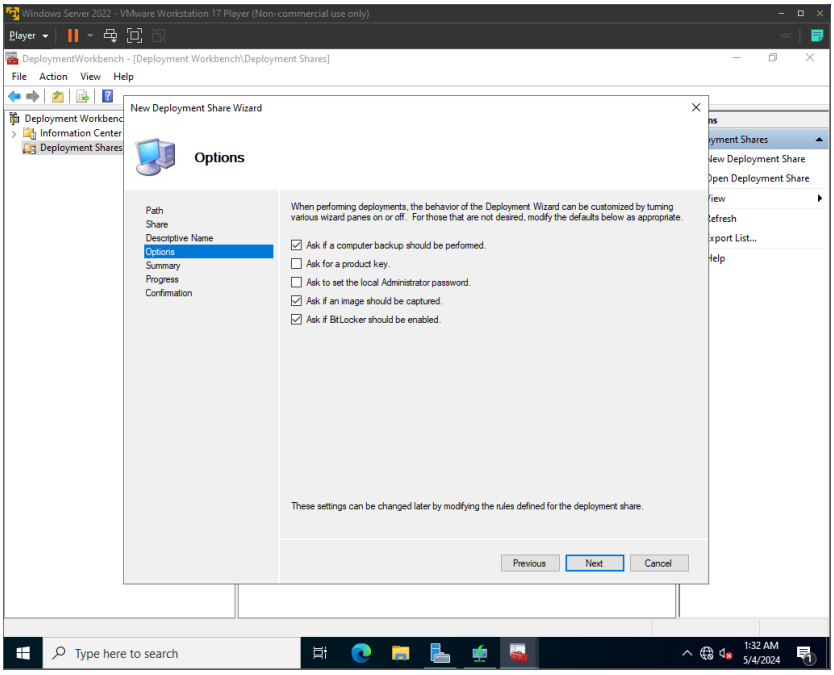


Рис. 2.19 Редагування стандартних опцій для образу

Тепер для розгортання операційної системи необхідний відповідний образ, тому було завантажено та змонтовано образ Windows 11 Enterprise з офіційного веб-сайту Microsoft (рис. 2.20).

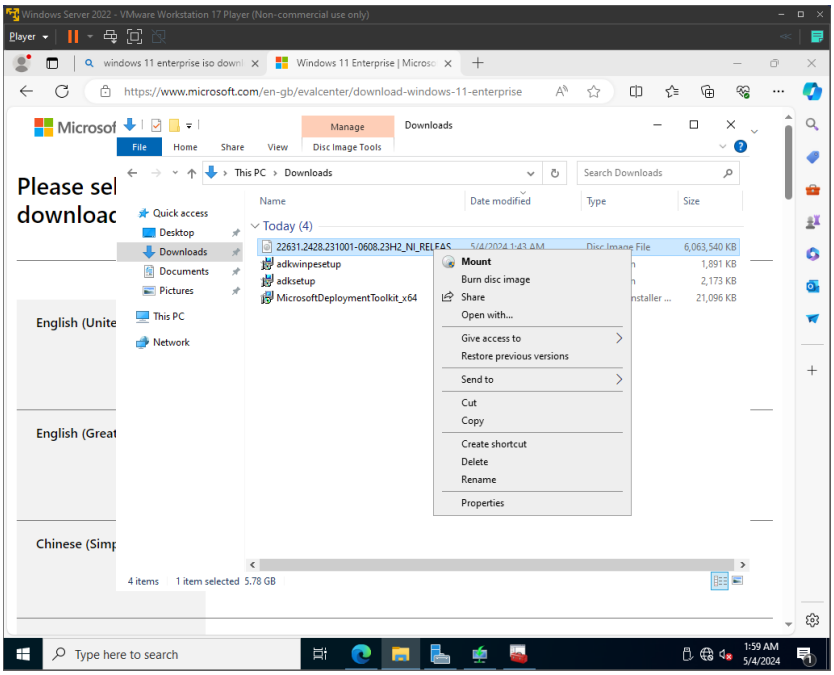


Рис. 2.20 Монтування завантаженого образу

У налаштуваннях імпортованої операційної системи було вибрано тип "Full set of source files" (рис. 2.21), що дозволить імпортувати всі необхідні файли та компоненти для розгортання.

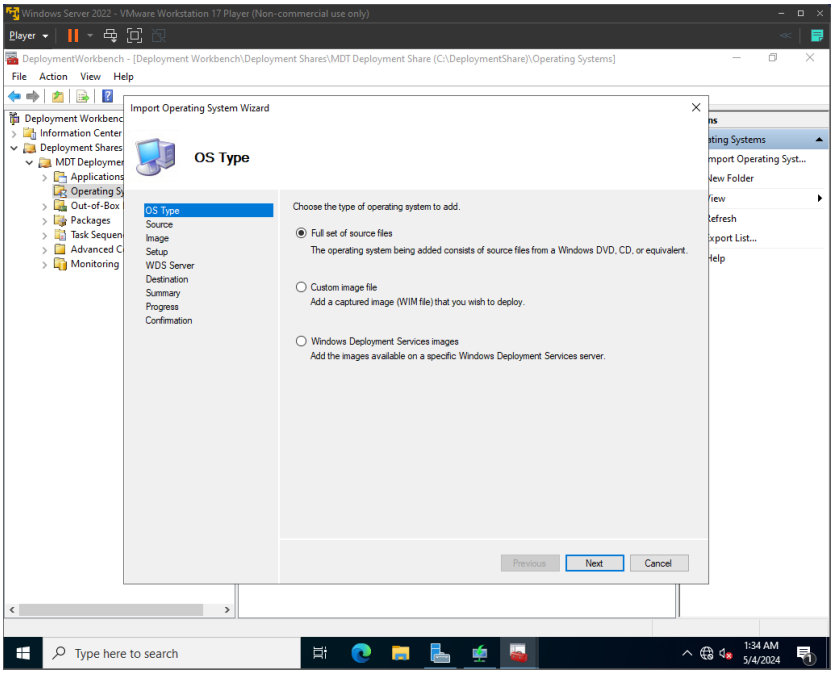


Рис. 2.21 Вибір типу імпортованого образу

У полі "Source directory" був вибраний шлях до змонтованого образу Windows 11 Enterprise, в моєму випадку – це диск E:\ (рис. 2.22).

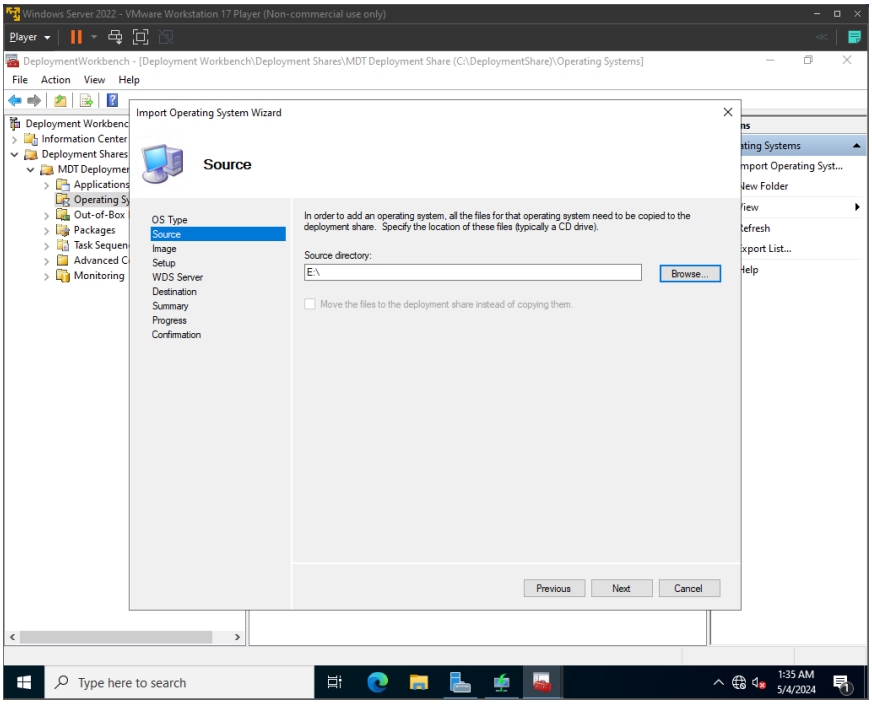


Рис. 2.22 Вибір шляху до змонтованого образу

Також, в полі "Destination Directory Name" була залишена назва за замовчуванням, що вказує на версію та архітектуру операційної системи - "Windows 11 Enterprise Evaluation x64" (рис. 2.23).

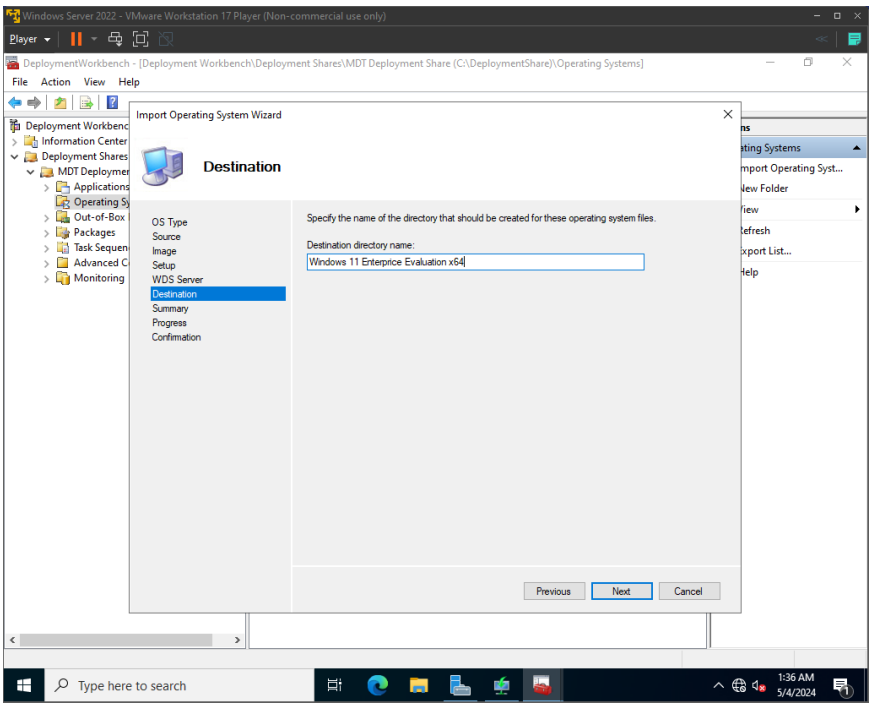


Рис. 2.23 Задання імені ОС, що імпортується

Додатково до розгортання операційної системи, я хочу розгортати додаток 7-zip. Для цього, встановлювальний файл 7-zip у форматі MSI був завантажений з офіційного веб-сайту.

Далі, в DeploymentWorkbench додаємо новий додаток - 7-zip. У налаштуваннях цього додатку, було вибрано тип "Application with source files", що дозволить включити всі необхідні файли для розгортання (рис. 2.24).

Інший тип додатку «Application without source file» означає, що він не включає вихідні файли програми у Deployment Share, але можна надати посилання на виконавчий файл або інсталяційний пакет програми, який може бути розташований у будь-якому доступному місці у мережі.

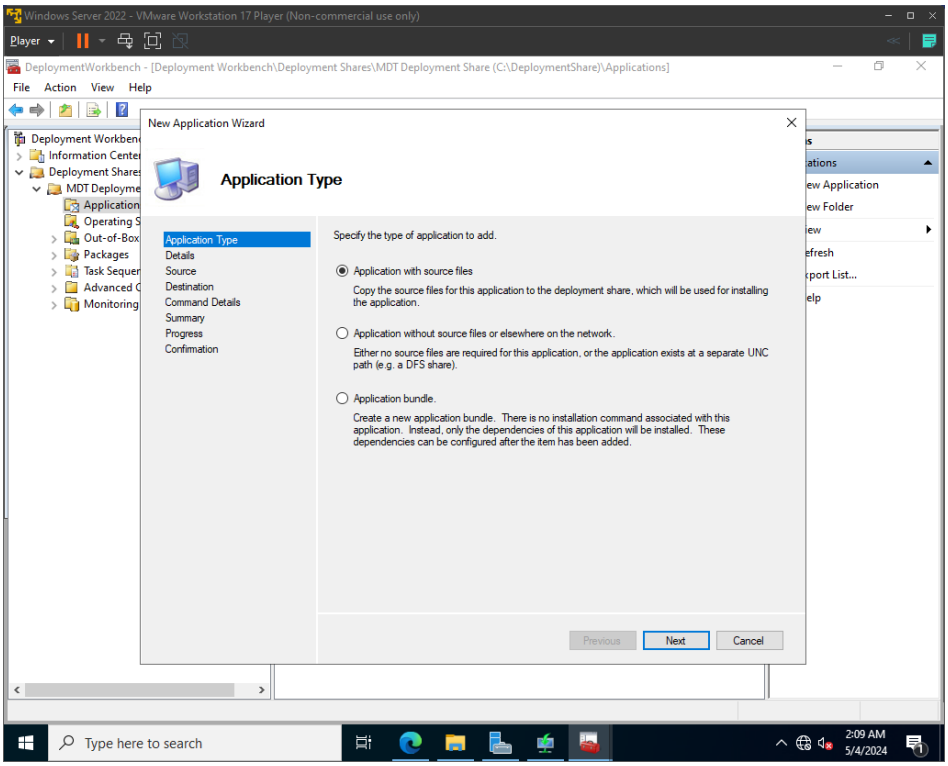


Рис. 2.24 Вибір типу додатку

У деталях додатка вказав назву програмного забезпечення - 7-zip (рис. 2.25), а також було можливо вказати виробника, версію та мову, проте це не є обов'язковим.

Заповнення цих пунктів може дозволити комп’ютерам розуміту, яка версія програмного забезпечення є самою

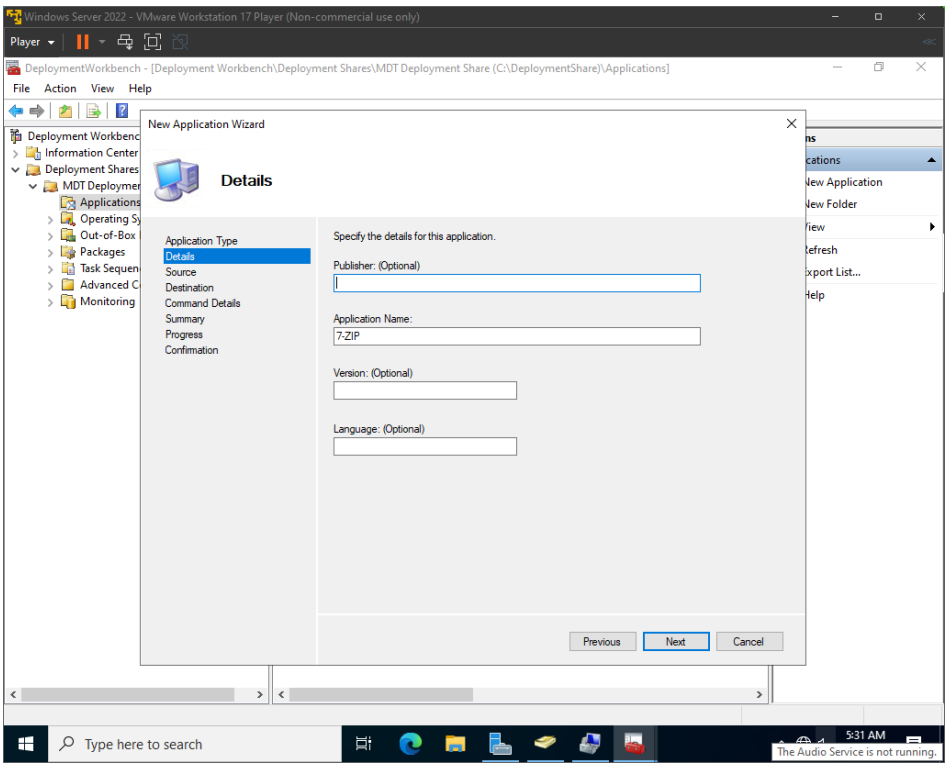


Рис. 2.25 Вказання деталей про додаток

В полі "Source directory" вказано місцезнаходження папки з встановлювальним файлом MSI (рис. 2.26).

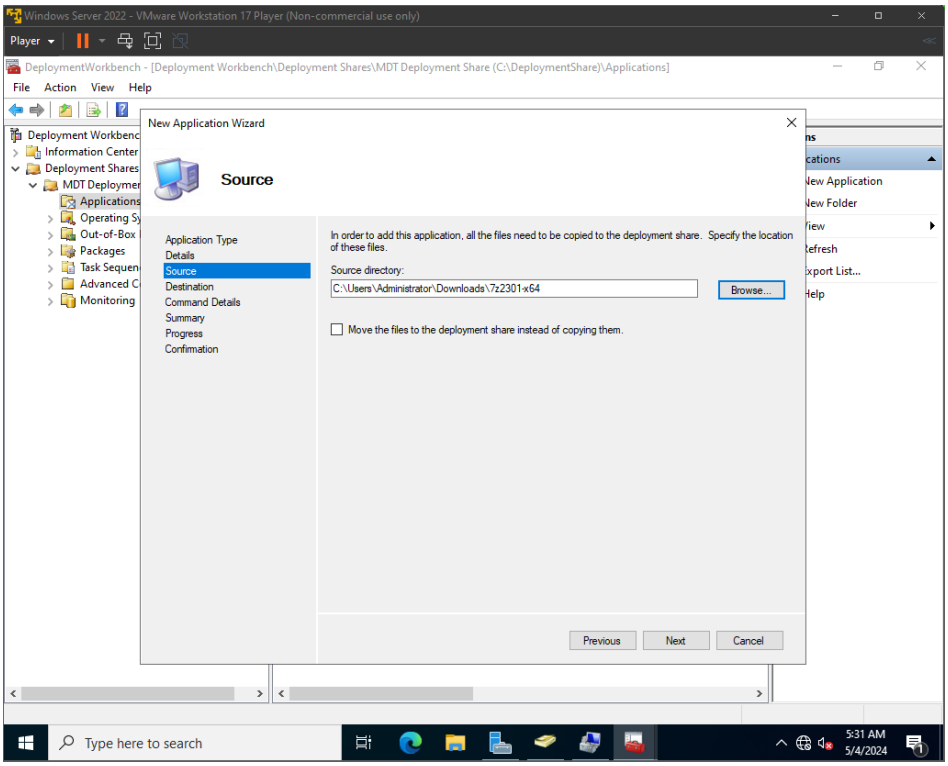


Рис. 2.26 Задання папки, де знаходить інсталятор 7-zip

У полі "Command line" вказано команду для тихої розгортки програми: msiexe.exe /i 7z2404-x64.msi /q (рис. 2.27). Це дозволить встановлювати програму без участі користувача, у тихому режимі.

В розділі "Working Directory" вказано шлях до робочого каталогу, де буде встановлено програмне забезпечення, в моєму випадку - це .\Applications\7-ZIP.

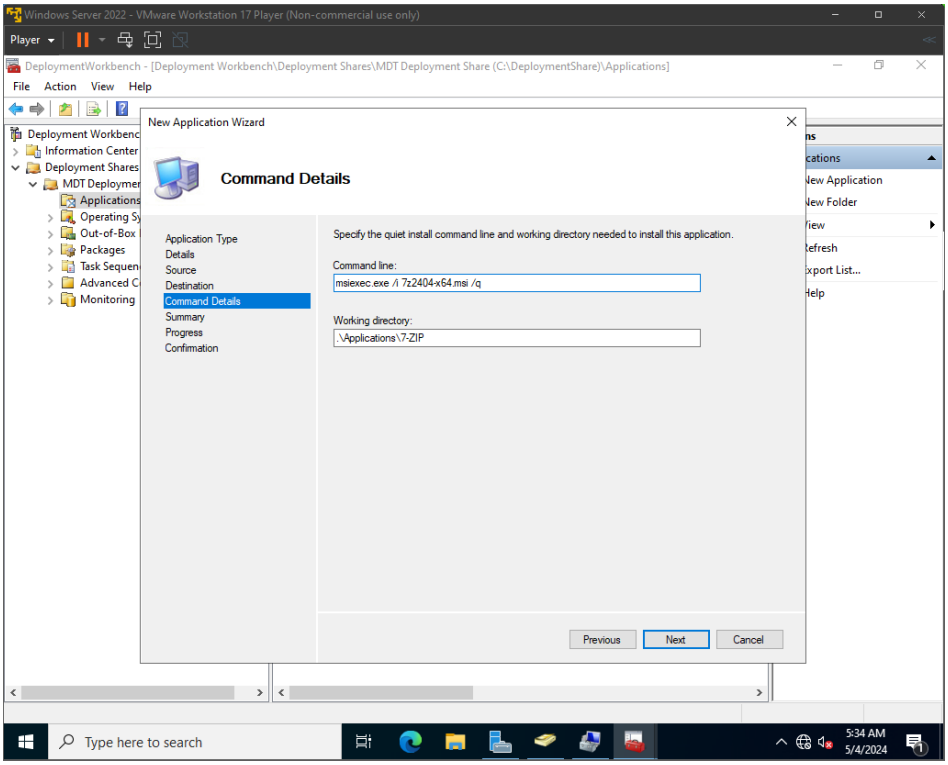


Рис. 2.27 Задання команди для інсталятора

Після налаштування цього додатку, його можна буде додати до Deployment Share та використовувати разом з іншими програмами, що будуть додані за цим же принципом, під час розгортання операційних систем на цільові комп'ютери у мережевому середовищі.

Зараз треба створити послідовність завдань для розгортання операційної системи Windows 11. У розділі "General Settings" був вказаний ідентифікатор послідовності завдань (Task Sequence ID) як "win-11-deploy". Для самої дії було обрано назву "Windows 11 Enterprise Deploy" (рис. 2.28).

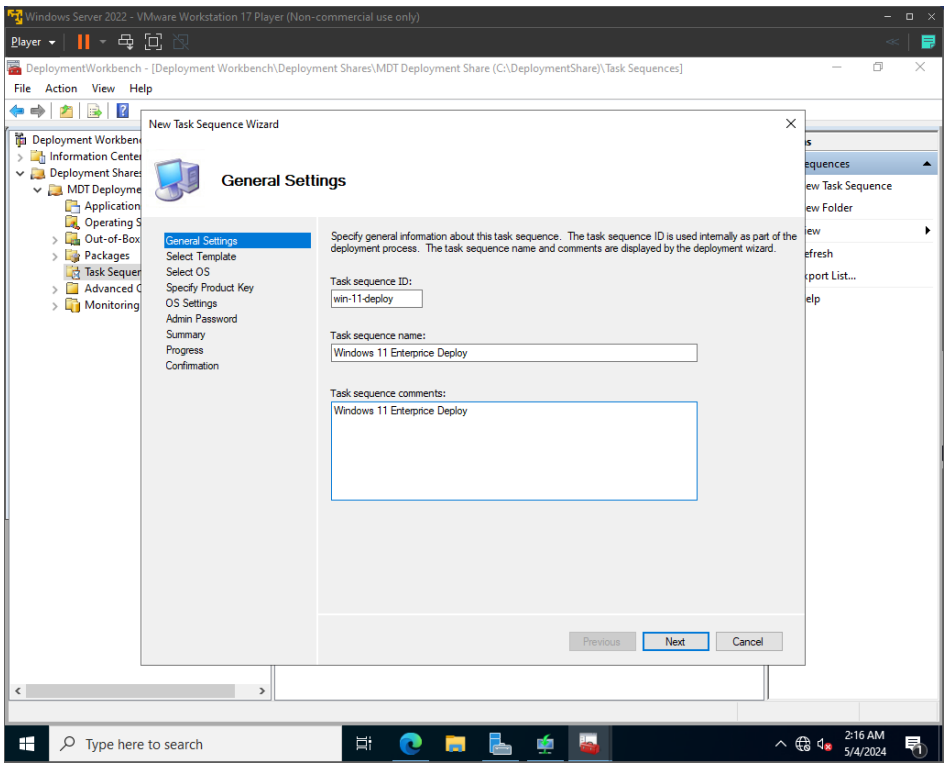


Рис. 2.28 Встановлення основних налаштувань для сценарію

У розділі шаблонів був вибраний "Standard Client Task Sequence" (рис. 2.29), проте інші шаблони також можуть бути цікавими для використання.

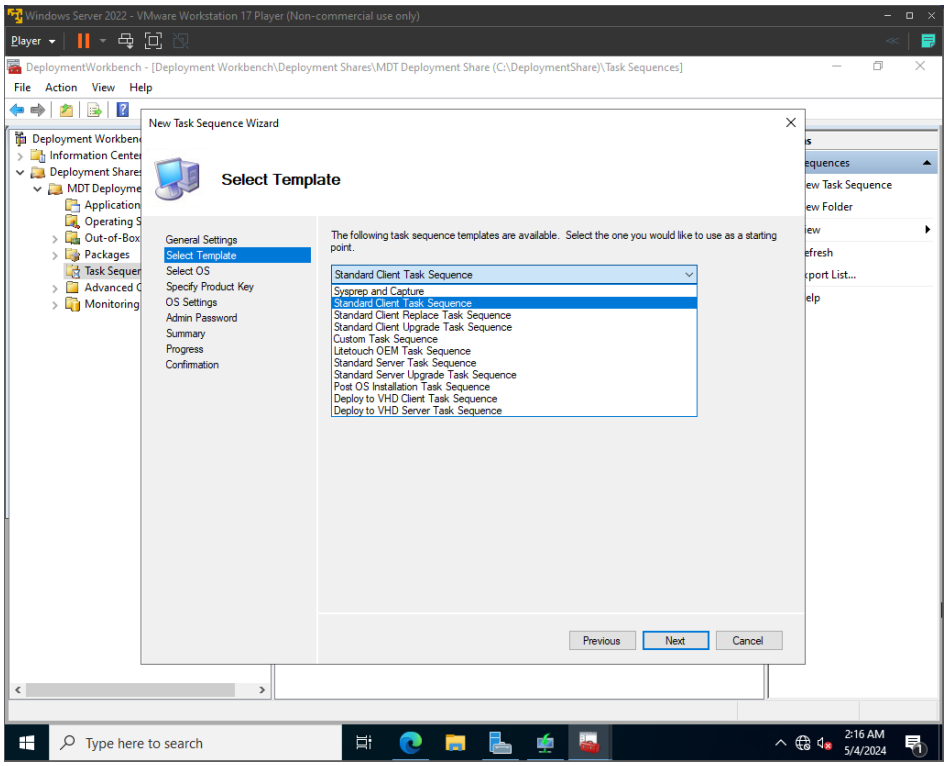


Рис. 2.29 Вибір шаблону послідовності процесу встановлення

У налаштуваннях операційної системи була обрана раніше імпортована операційна система Windows 11 Enterprise (рис. 2.30).

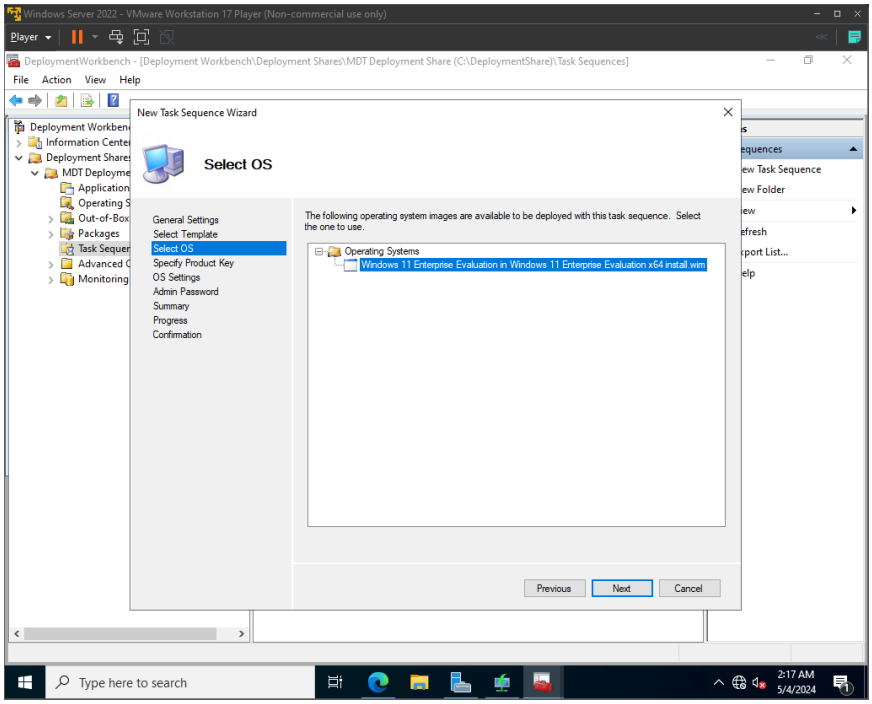


Рис. 2.30 Вибір образу ОС, що буде розгортатись

Для ліцензійного ключа була залишена можливість вставити корпоративний ключ, який дозволить уникнути подальших турбот щодо активації системи (рис. 2.31). У моєму випадку, ліцензійний ключ був відсутній.

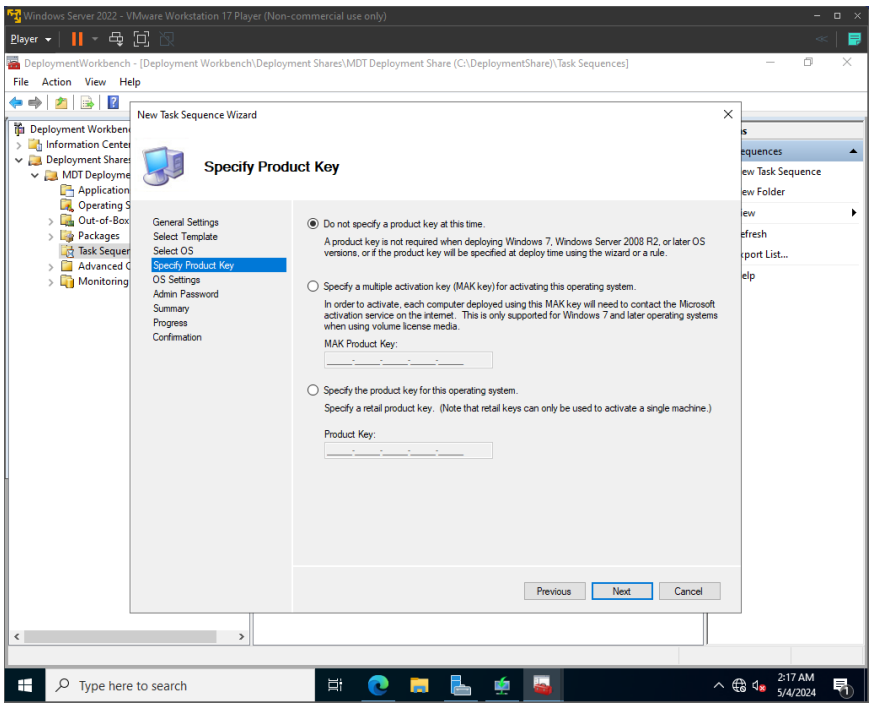


Рис. 2.31 Вікно задання ключа активації системи

У налаштуваннях операційної системи також можна було зазначити локальне ім'я користувача, домен та веб-сайт за замовчуванням, у моєму випадку я вказав ці дані: Windows User, Voskolup.Organization, google.com (рис. 2.32).

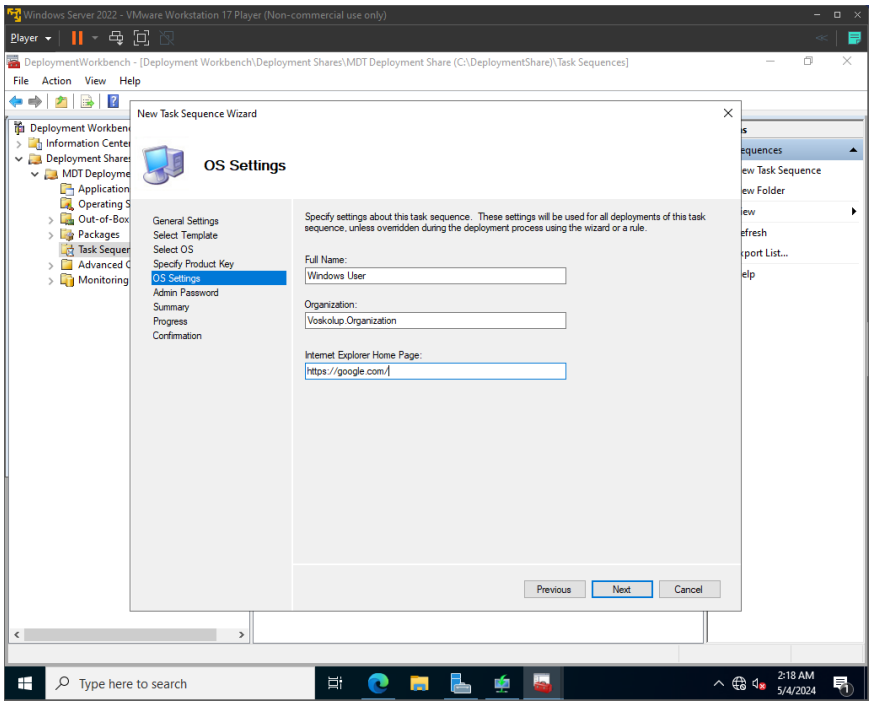


Рис. 2.32 Задання типових параметрів ОС

Також був вказаний пароль для локального запису адміністратора (рис. 2.33), проте цей крок можна пропустити, якщо це необхідно.

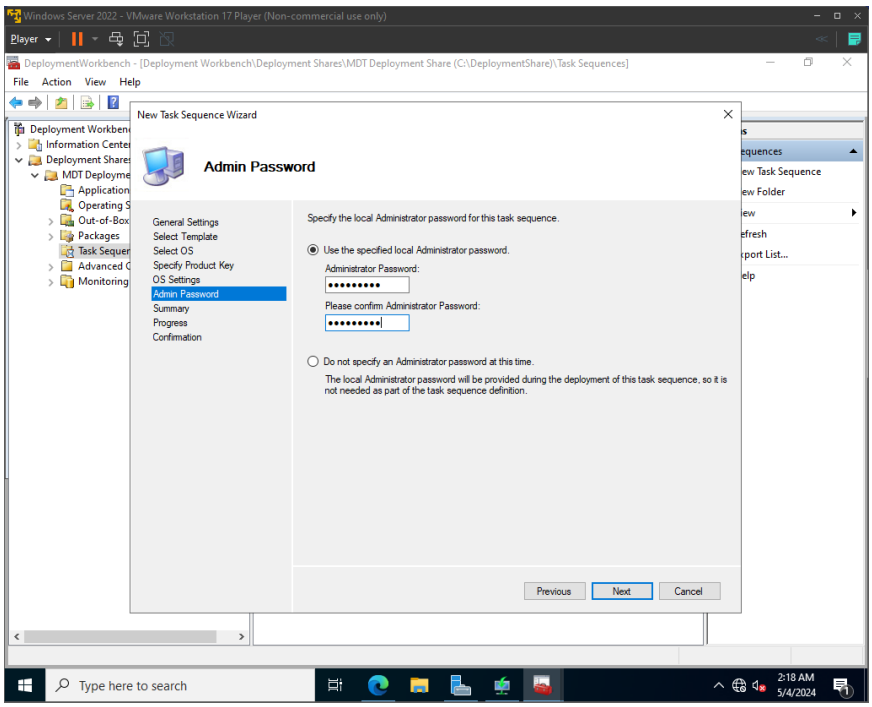


Рис. 2.33 Встановлення паролю адміністратора

Додаткові вимоги та налаштування послідовності завдань можна відредагувати, натиснувши праву кнопку миші на створеному сценарії, далі обрати "Властивості", а потім перейти до розділу "Послідовність завдань" (рис. 2.34). Тут можна змінити або додати нові задачі, встановити їх послідовність та параметри виконання.

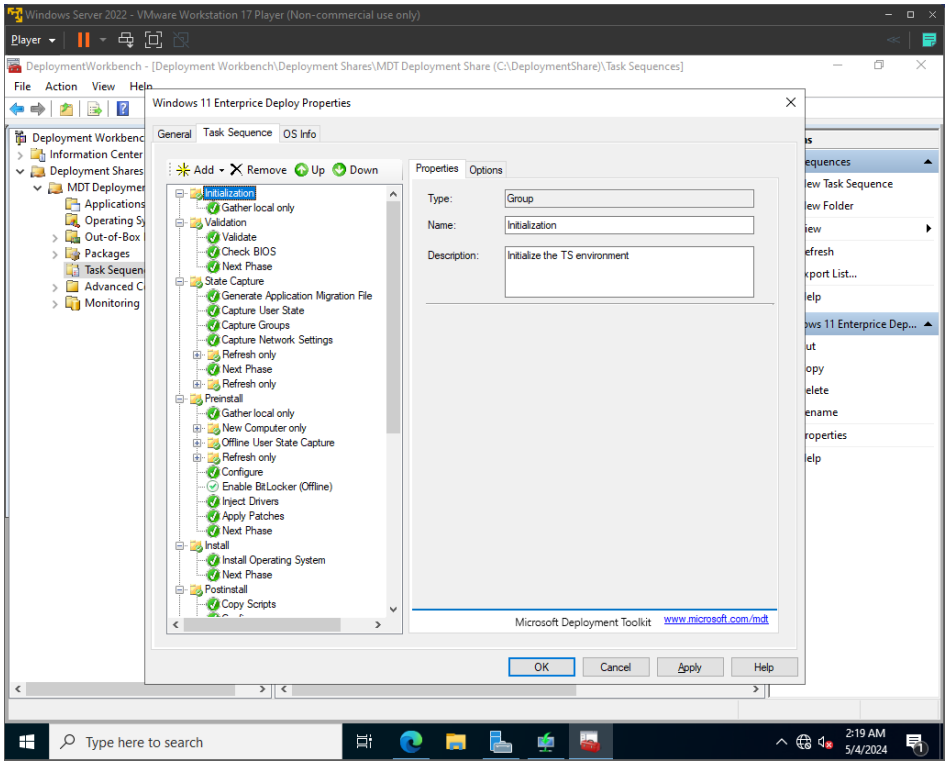


Рис. 2.34 Вікно з додатковими налаштуваннями ОС

Додатково, можна встановити драйвери від виробника у розділі "Out-of-Box Drivers". Це особливо корисно для забезпечення сумісності пристроїв з операційною системою. Також можна прив'язати драйвери до кожної окремої моделі ноутбуку або ПК, щоб забезпечити оптимальну роботу системи на конкретних пристроях.

Проте, якщо використовується віртуальна машина, як у моєму випадку, то цей крок можна пропустити, бо віртуальна машина вже має вбудовані драйвери, яких зазвичай вистачає для нормальної роботи.

Тепер необхідно налаштувати Deployment Share в Microsoft Deployment Toolkit (MDT). У властивостях Deployment Share було вимкнуто підтримку платформ x86, що означає, що тільки 64-бітні системи будуть підтримуватись для

розгортання (рис. 2.35). Проте, завантажений раніше Windows Assessment and Deployment Kit (ADK) все ще дозволить використання 32-бітної архітектури, якщо це буде потрібно.

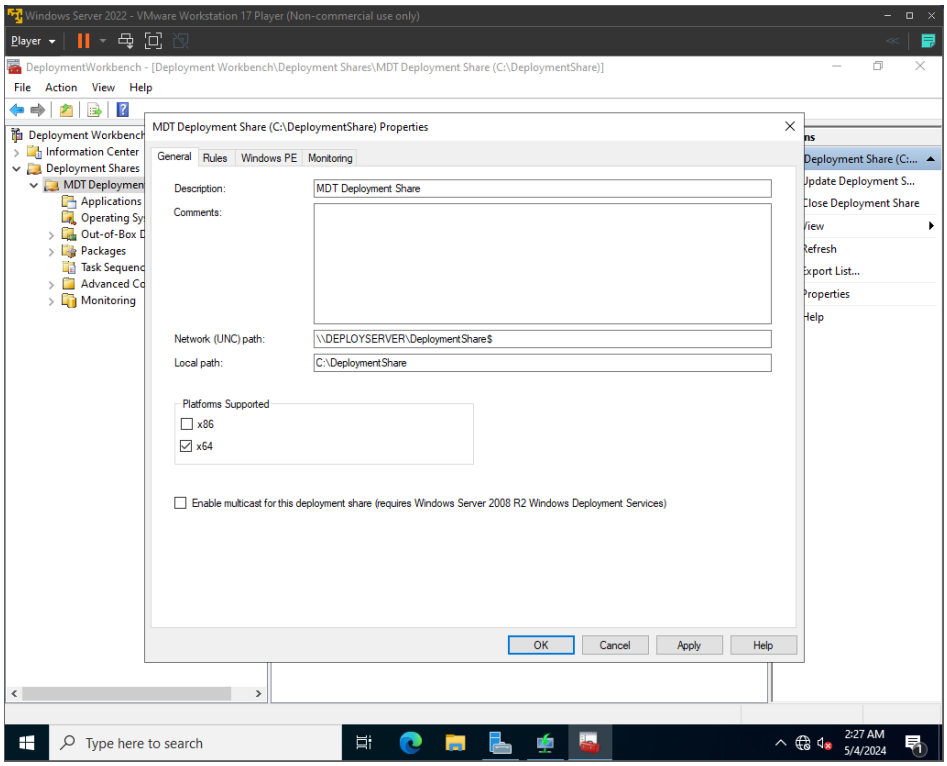


Рис. 2.35 Вказання основних властивостей для Deployment Share

Параметри налаштувань в MDT Deployment Share відповідають за конфігурацію різних аспектів розгортання операційної системи. У правилах Deployment Share мною було вказано наступні налаштування (рис. 2.36):

[Settings]

Priority=Default

Properties=MyCustom Property

[Default]

OSInstall=Y

Skip BDDWelcome=YES

SkipCapture=YES

Skip Admin Password=YES

Skip Product Key=YES

SkipComputerBackup=YES

Skip BitLocker=YES

Skip UserData=YES

Skip TimeZone=YES

Skip Locale Selection=YES

Join Domain=Voskolup.Organization

MachineObjectOU=OU=Computers,DC=Voskolup,DC=Organization

Keyboard Locale=en-US

Event Service http://DeployServer:9800

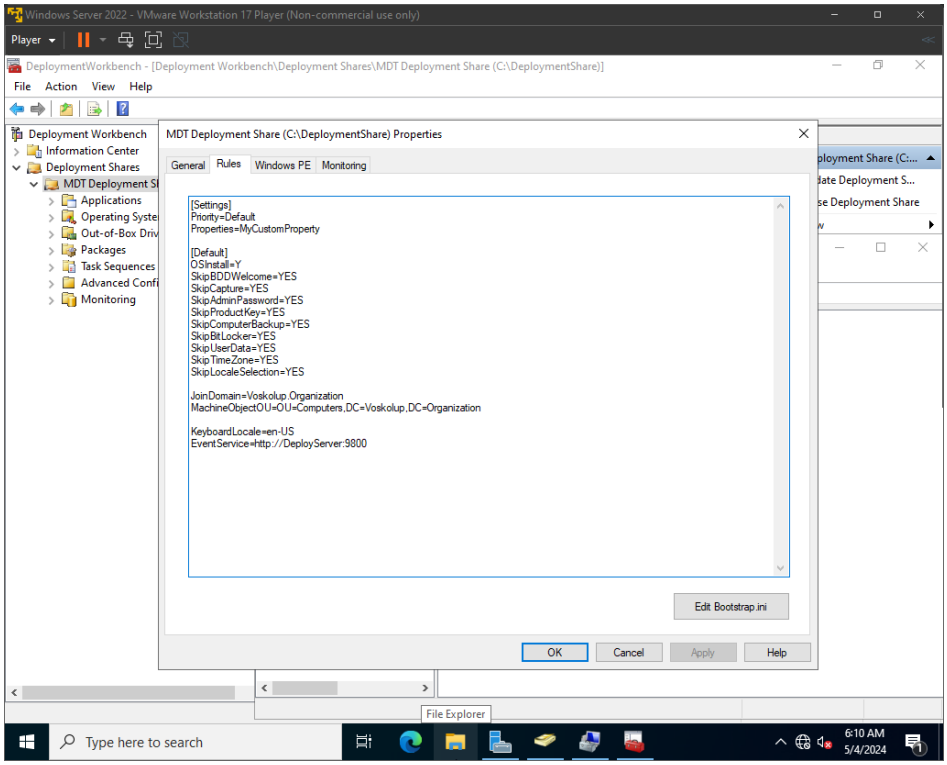


Рис. 2.36 Задання правил ОС

У bootstrap.ini були вказані наступні дані (рис. 2.37):

[Settings]

Priority=Default

[Default]

DeployRoot=\\DEPLOYSERVER\DeploymentShare$

UserID=Administrator

UserDomain=Voskolup.Organization

UserPassword=Voskolup1

SkipBDDWelcome=YES

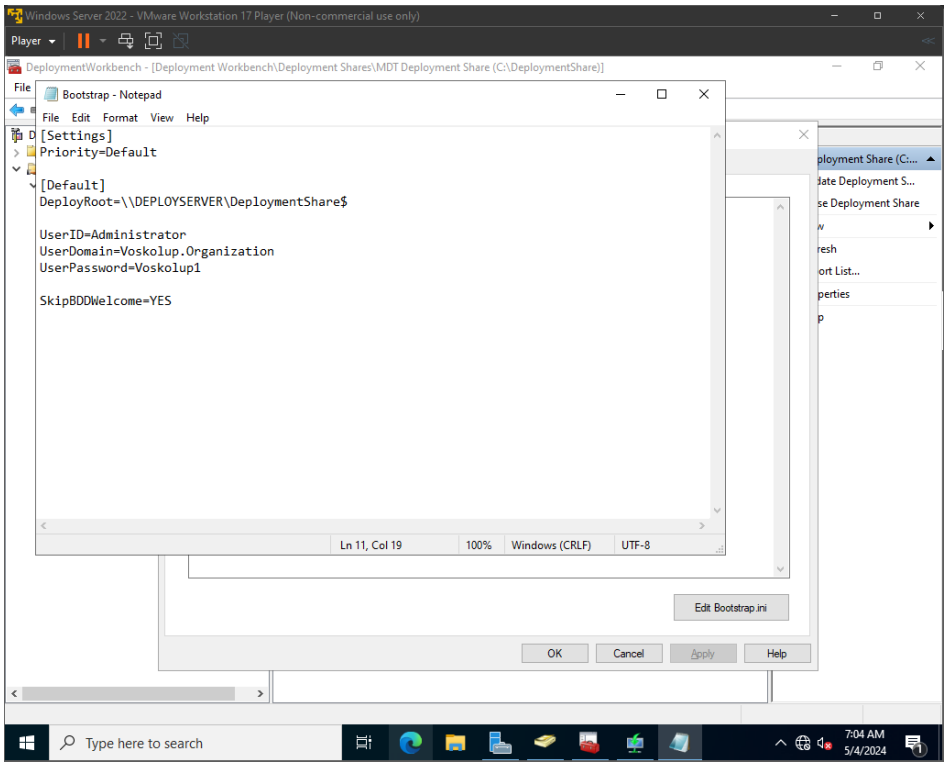


Рис. 2.37 Задання правил запуску

Ось детальний розбір кожного параметра, що були вказані:

Priority - визначає пріоритет використання налаштувань для різних компонентів. У даному випадку, значення "Default" вказує на те, що будуть використані налаштування, визначені в розділі [Default].

Properties - визначає властивості, які будуть доступні для використання під час розгортання.

OSInstall - параметр вказує, що необхідно встановлювати операційну систему.

SkipBDDWelcome - вказує на пропуск екрану вітання MDT.

SkipCapture - вказує на пропуск процесу захоплення (збереження) образу операційної системи.

SkipAdminPassword - дозволяє пропустити введення пароля адміністратора під час встановлення.

SkipProductKey - дозволяє пропустити введення ключа продукту під час встановлення.

SkipComputerBackup - вказує на пропуск резервного копіювання комп'ютера перед розгортанням.

SkipBitLocker - дозволяє пропустити налаштування BitLocker під час встановлення.

SkipUserData - вказує на пропуск налаштування даних користувача під час встановлення.

SkipTimeZone - дозволяє пропустити вибір часового поясу під час встановлення.

SkipLocaleSelection - вказує на пропуск вибору мови під час встановлення.

JoinDomain - визначає домен, до якого комп'ютер буде доданий під час розгортання.

MachineObjectOU - вказує на організаційну одиницю (OU), в яку буде доданий об'єкт комп'ютера під час додавання до домену.

KeyboardLocale - визначає мову клавіатури, що буде встановлена за замовчуванням.

EventService - визначає URL-адресу служби подій, яка використовується для повідомлення сервера розгортання про стан розгортання.

У файлі bootstrap.ini такі налаштування:

Priority - аналогічно до налаштувань у файлі Settings.ini, вказуємо пріоритет "Default".

DeployRoot - визначає шлях до Deployment Share, де знаходяться файли для розгортання.

UserID - вказує ім'я користувача, яке буде використовуватися під час розгортання.

UserDomain - визначає домен користувача, який буде використовується під час входу в домен.

UserPassword - вказує пароль користувача для аутентифікації під час встановлення.

SkipBDDWelcome - дозволяє пропустити екран вітання MDT під час запуску.

У налаштуваннях WinPE також була вибрана платформа x64 (рис. 2.38), щоб забезпечити сумісність із використовуваними операційними системами та зменшити можливі проблеми сумісності під час розгортання.

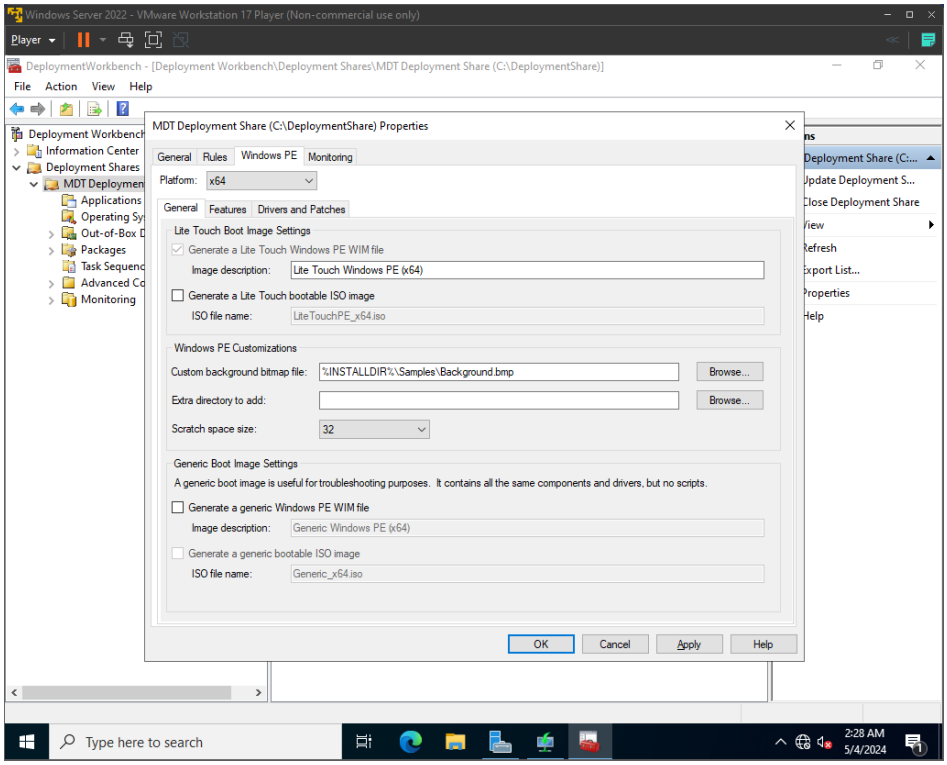


Рис. 2.38 Змінення налаштувань для Windows PE

У розділі моніторингу було увімкнуто моніторинг (рис. 2.39). MDT зберігає детальні журнали процесу розгортання для кожного комп'ютера, на якому відбувається розгортання. Ці журнали містять інформацію про кожен крок у процесі розгортання, включаючи інформацію про успішні та невдачні операції, помилки, відомості про встановлене програмне забезпечення тощо. Адміністратори можуть звернутися до централізованої консолі моніторингу, щоб переглянути журнали розгортання з різних комп'ютерів у мережі

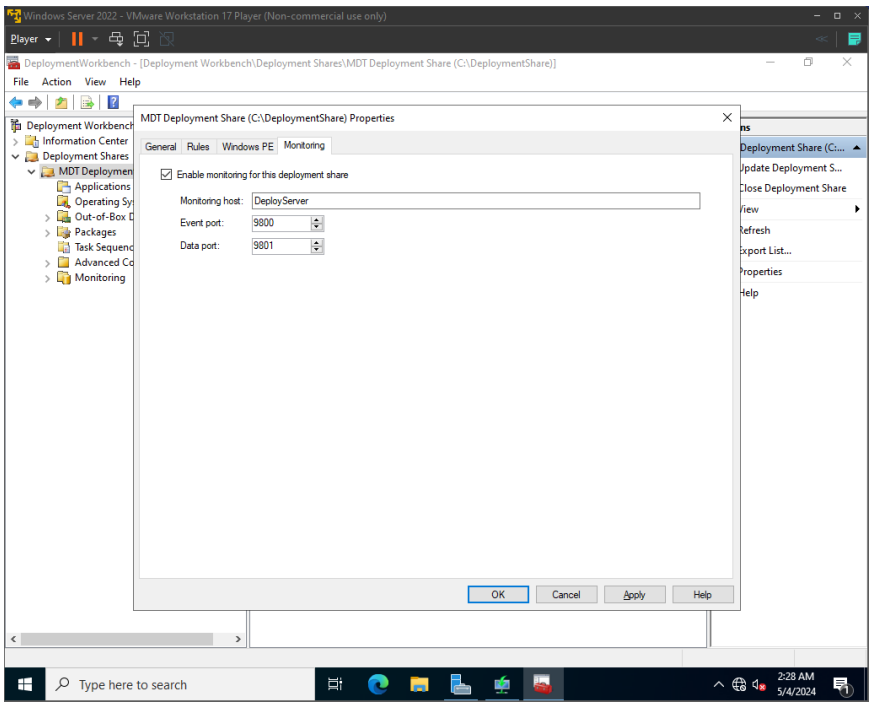


Рис. 2.39 Увімкнення функції моніторингу

Тепер необхідно створити загрузочний образ, що використовуватиметься для розгортання операційних систем. Це можна зробити, натиснувши праву кнопку миші на MDT Deployment Share, а потім обрати "Update Deployment Share". У вікні, що відкрилось, було обрано повну регенерацію загрузочного образу, і розпочато процес (рис. 2.40).

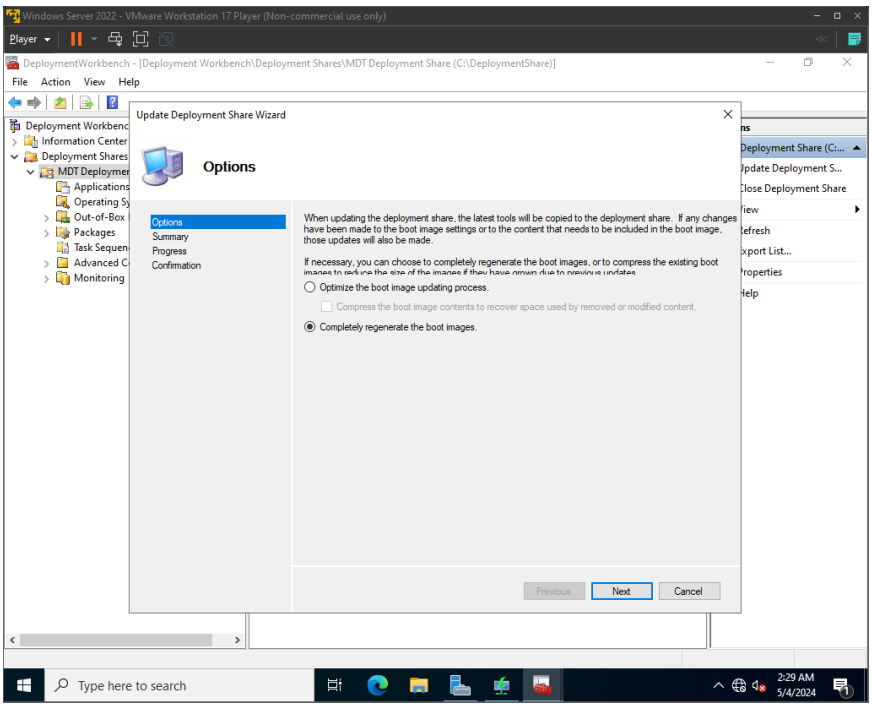


Рис. 2.40 Регенерація boot образу

Варто відзначити, що цей процес може зайняти деякий час. Після завершення процесу, готовий файл .wim можна знайти за шляхом C:\DeploymentShare\Boot (рис. 2.41).

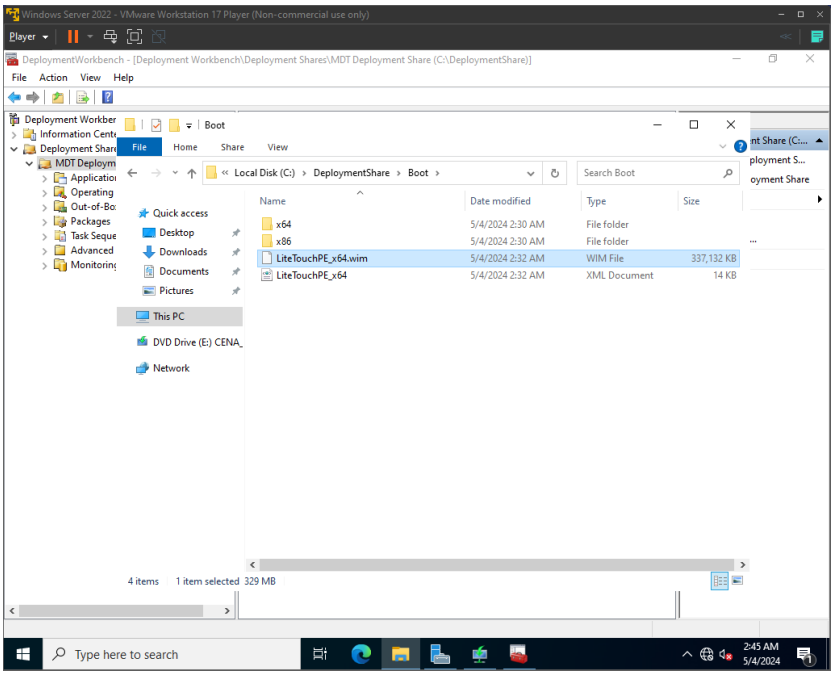


Рис. 2.41 Демонстрація згенерованого .wim файлу

Далі, отриманий .wim файл необхідно додати у Windows Deployment Services у розділі "Boot Images". У налаштуваннях шляху до файлу слід вказати шлях до цього .wim файлу (рис. 2.42).

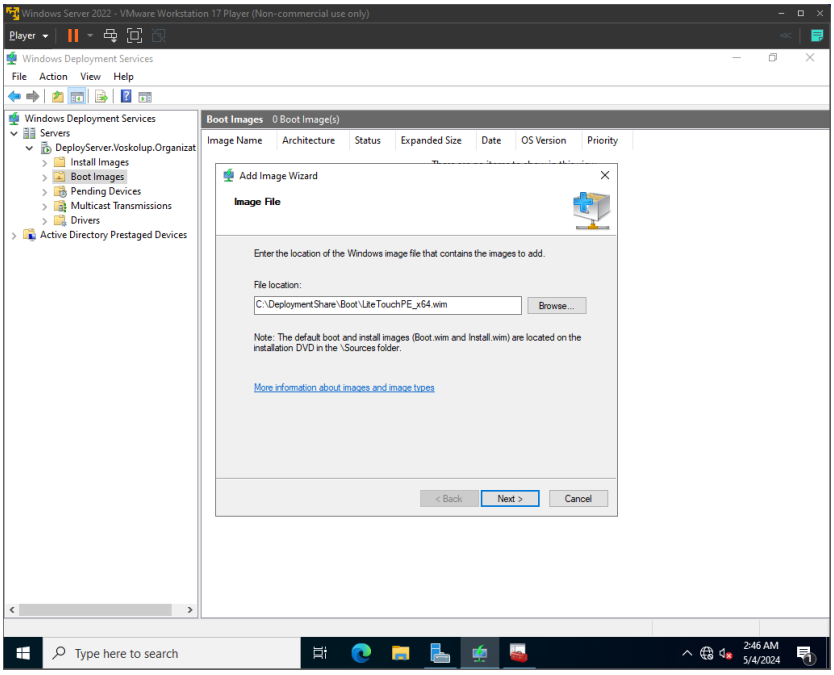


Рис. 2.42 Вказання розташування .wim файлу

В наступному кроці можна також надати ім'я та опис для образу, проте я залишив все по замовчуванню (рис. 2.43).

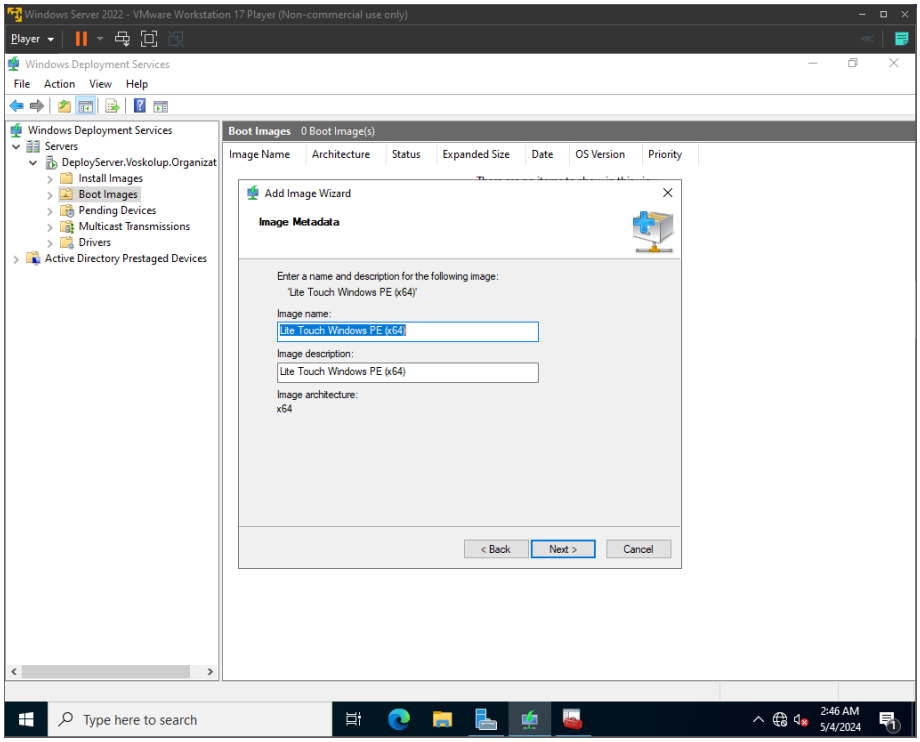


Рис. 2.43 Задання імені та опису для образа

3 НАЛАШТУВАННЯ ТА КЕРУВАННЯ КЛІЄНТСЬКОЇ ОС

3.1 Розгортання клієнтської ОС

Тепер, коли було підготовлено всі необхідні кроки, можемо створити клієнтську віртуальну машину, я надав такі характеристиками: 6 ядер і 4 гб ОЗП (рис. 3.1).

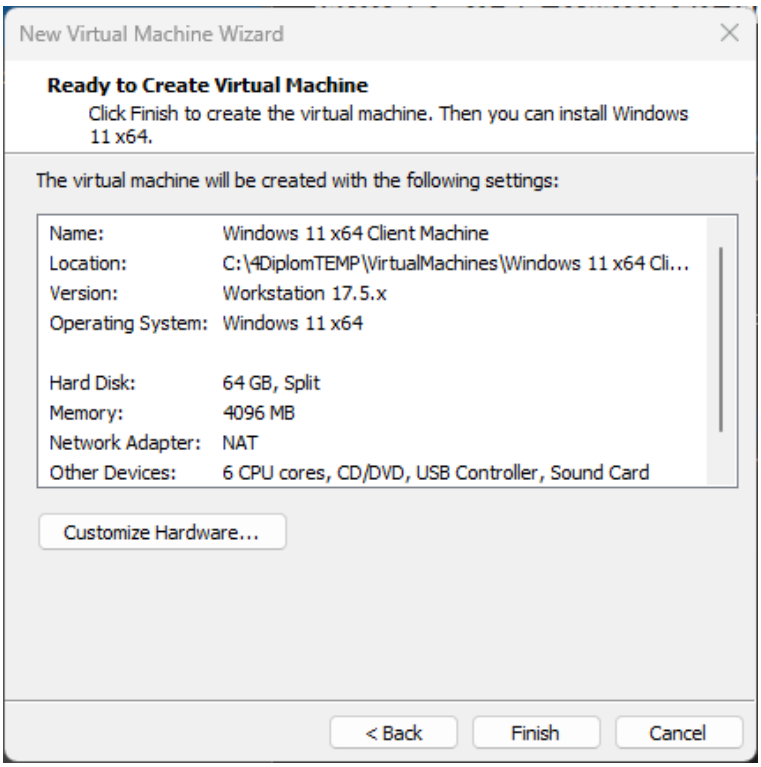


Рис. 3.1 Створення клієнтської віртуальної машини

При виборі варіанту завантаження, обираємо завантаження через мережу. При виборі сервера PXE комп'ютер намагається встановити з'єднання з сервером PXE за допомогою мережевого протоколу DHCP (Dynamic Host Configuration Protocol) та TFTP (Trivial File Transfer Protocol). Після цього, ми бачимо перед собою Windows Boot Manager з сервером, який має IP-адресу 192.168.92.100 (рис. 3.2). Після вибору образу та підтвердження завантаження, комп'ютер почне процес завантаження образу з сервера, що може зайняти деякий час залежно від розміру образу та швидкості мережі.

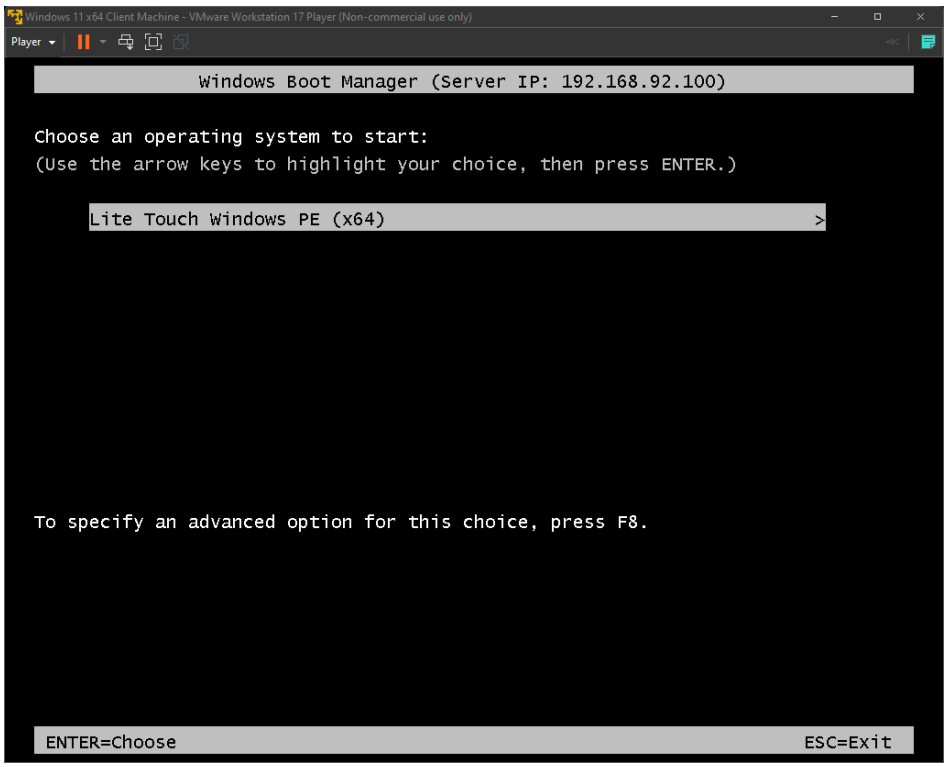


Рис. 3.2 Вікно Windows Boot Manager

Після завантаження відкривається вікно, де обираємо задачу "Windows 11 Enterprise Deploy" (рис. 3.3).

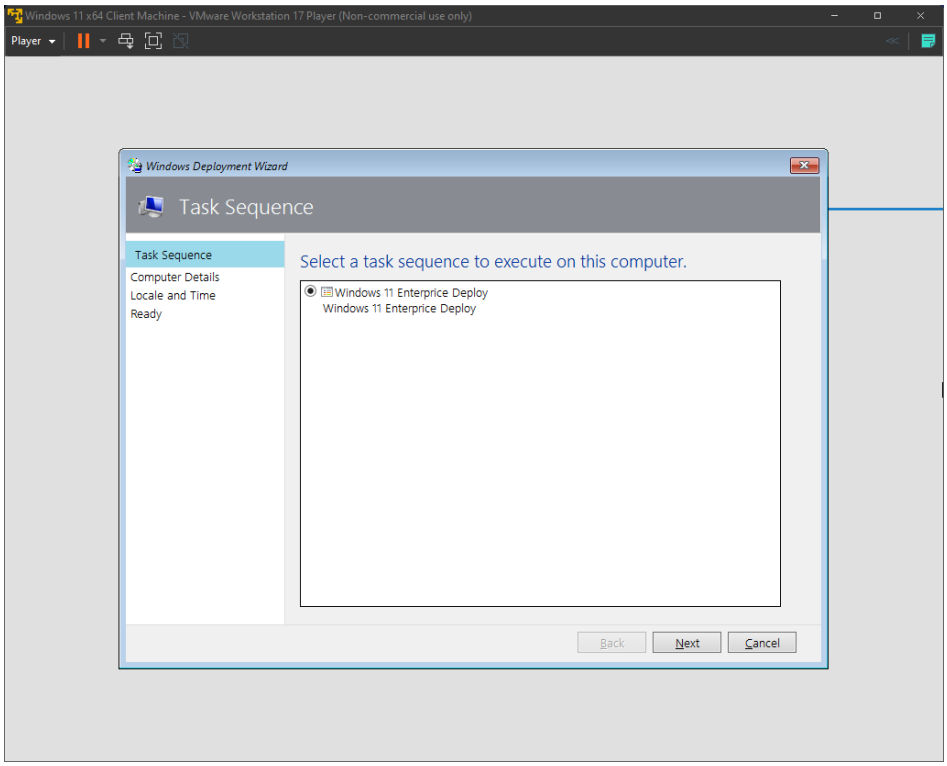


Рис. 3.3 Вибір сценарію розгортки

Далі, в розділі про комп'ютер, дані вже введені (рис. 3.4), ім'я було обрано випадково, а дані для входу в домен - ті, що були вказані в правилах.

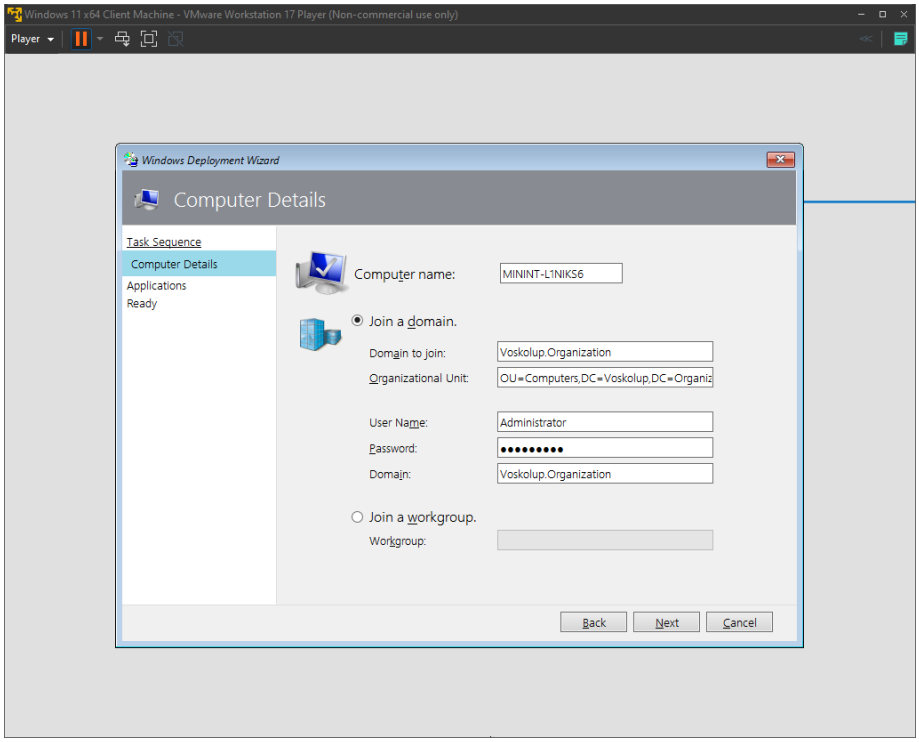


Рис. 3.4 Налаштування деталей ОС

В розділі додатків, які я хочу встановити - поставив галочку напроти 7-ZIP (рис. 3.5).

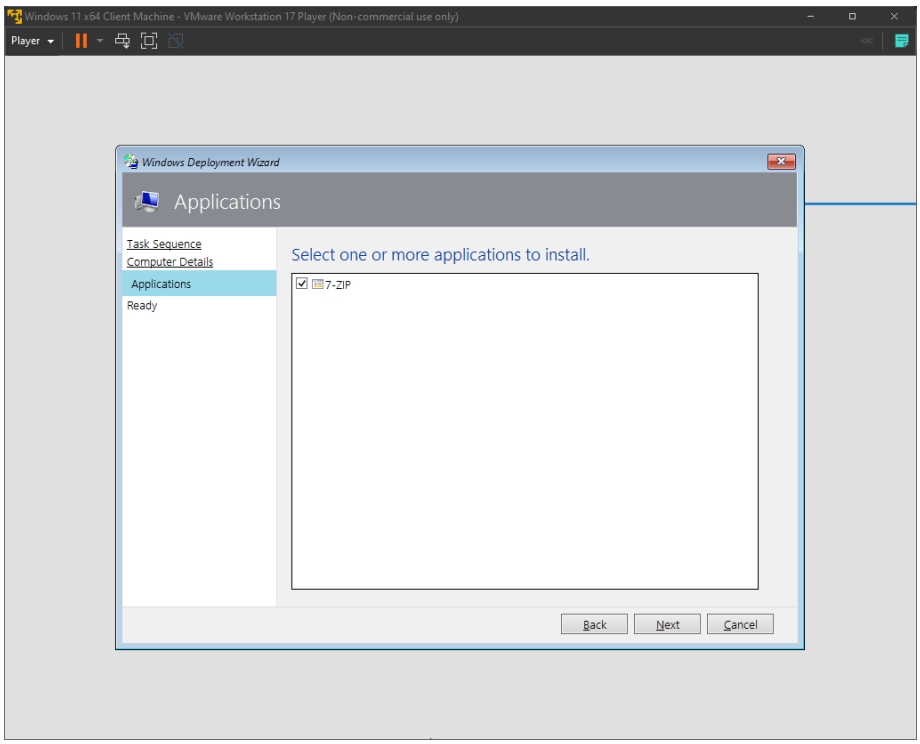


Рис. 3.5 Вибір програми для інсталяції разом з ОС

Тепер у розділі "Ready" показується інформація та дії, що будуть виконані (рис. 3.6).

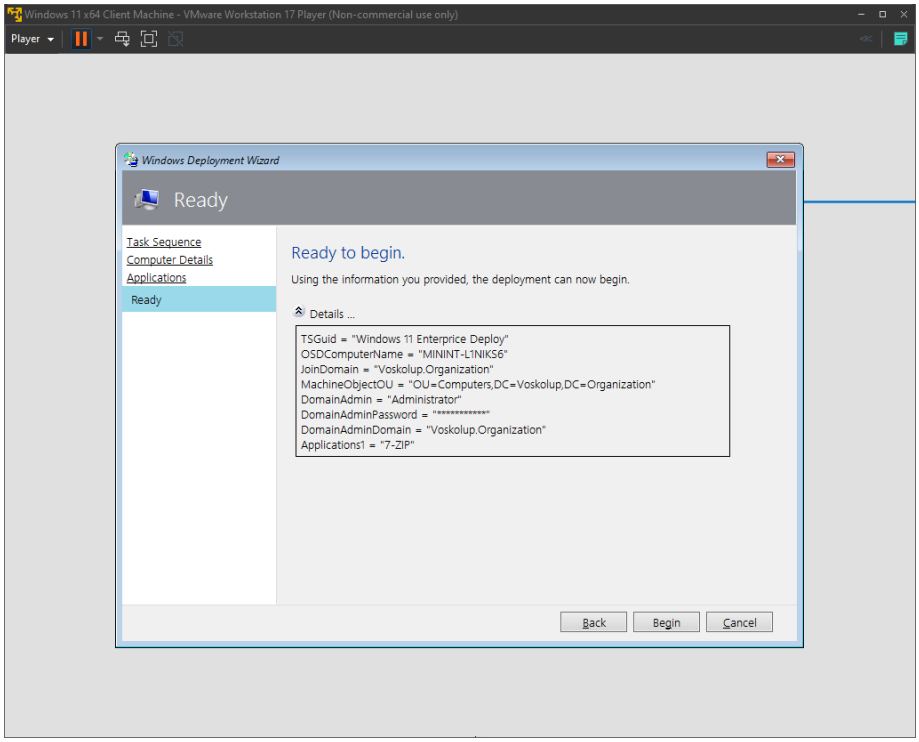


Рис. 3.6 Детальна інформація про ОС, що буде встановлена

Після натискання на кнопку "Почати", просто чекаємо процес встановлення (рис. 3.7).

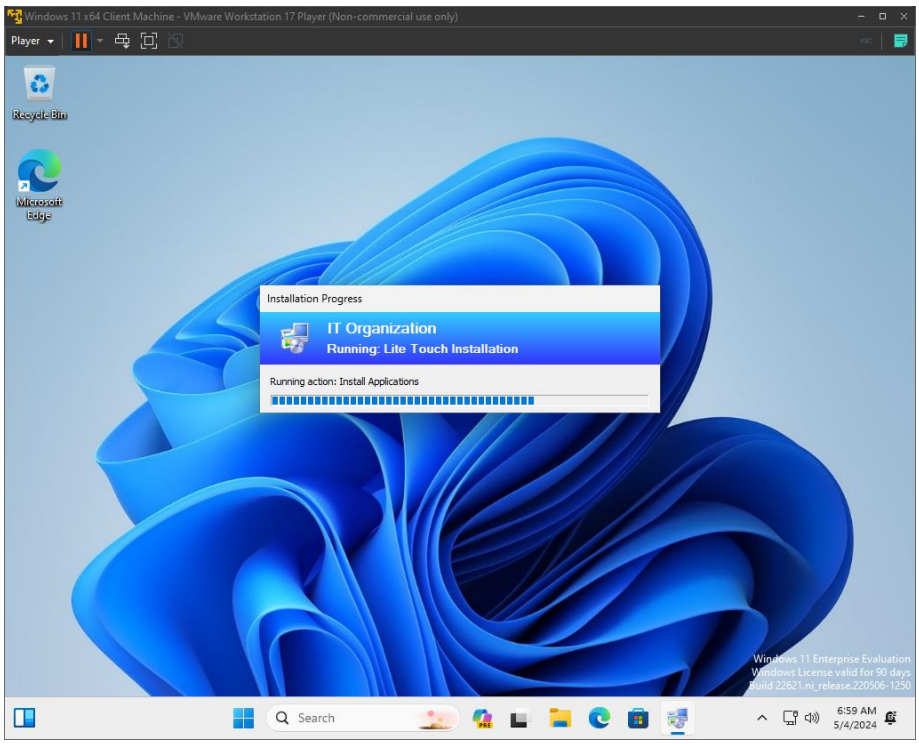


Рис. 3.7 Автоматизований процес встановлення ПЗ

По завершенню на клієнтській машині можна побачити, що у нас є програма 7-ZIP та комп'ютер було введено в домен (рис. 3.8).

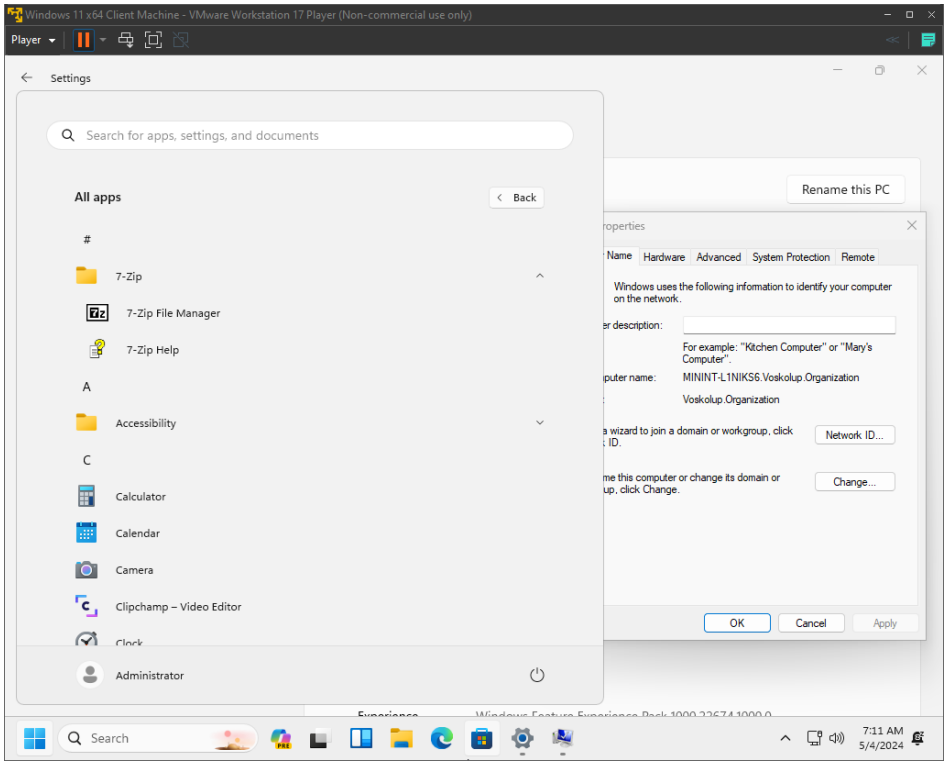


Рис. 3.8 Перевірка наявності 7-zip та підключення до домену

Сам ПК відображається в списку робочих станцій (Workstations) в Active Directory Users and Computers (рис. 3.9). Це означає, що вона успішно додана до домену і готова до використання у мережевому середовищі.

Тепер замість того, щоб налаштовувати кожен ПК окремо, адміністратори можуть керувати всіма налаштуваннями з однієї консолі Active Directory. Це значно економить час і ресурси, роблячи адміністрування мережі значно ефективнішим.

Active Directory дозволяє легко створювати та застосовувати комплексні політики безпеки до всіх комп'ютерів в домені. Ці політики можуть включати:

1. Налаштування брандмауера та антивірусного програмного забезпечення
2. Контроль доступу до користувачів та груп
3. Шифрування даних
4. Обов'язкове використання складних паролів
5. Регулярне оновлення програмного забезпечення

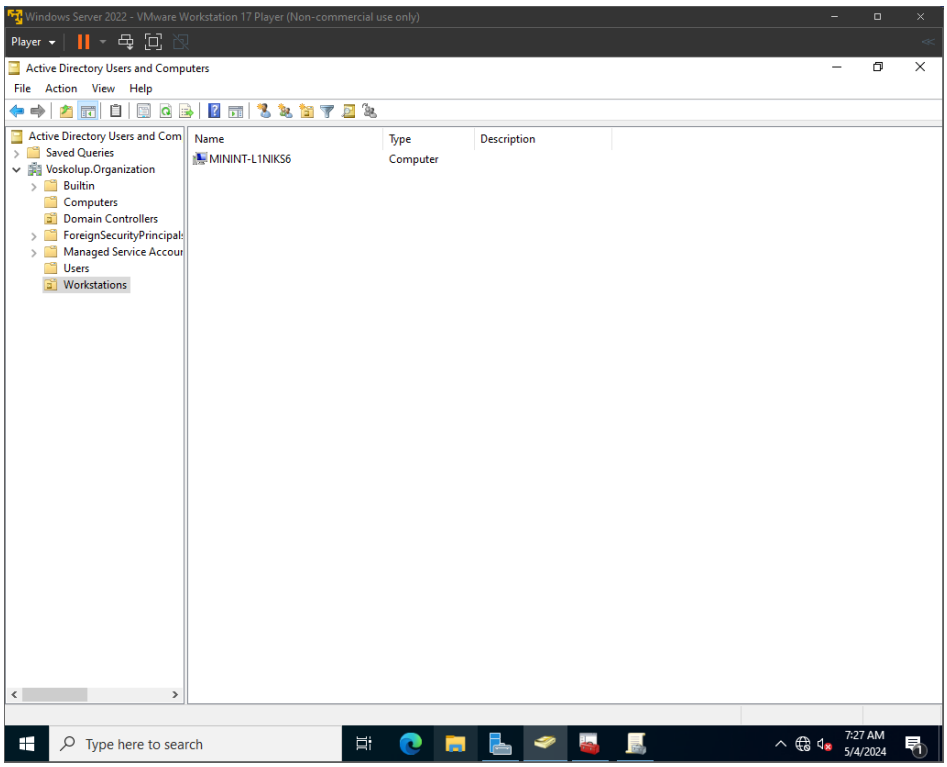


Рис. 3.9 Перевірка наявності комп'ютера в AD

3.2 Змінення налаштувань віддаленного доступу

Тепер комп'ютери, що є у списку робочих станцій в Active Directory можна додатково налаштовувати. Для цього я покажу приклад налаштування віддаленого робочого столу (RDP) та доступу до програми допомоги віддаленого доступу (msra).

Спочатку на серверній машині через Server Manager заходимо у консоль керування груповими політиками (Group Policy Management Console), розкриваємо список домену, в ньому буде знаходитись розділ «Group Policy Object», в ньому і зберігаються всі політики, що будуть вноситись. Хоча і в одну політику можна внести одразу всі налаштування, проте я рекомендую на кожну функцію створювати свою політику з окремою назвою, якщо з часом якась функція не буде потрібна, то її можна буде вимкнути через контекстне меню, яке відкривається при натисканні правою кнопкою миші по політиці. В цьому розділі створюємо нову групову політику, я її назвав "Allow RDP" (рис. 3.10).

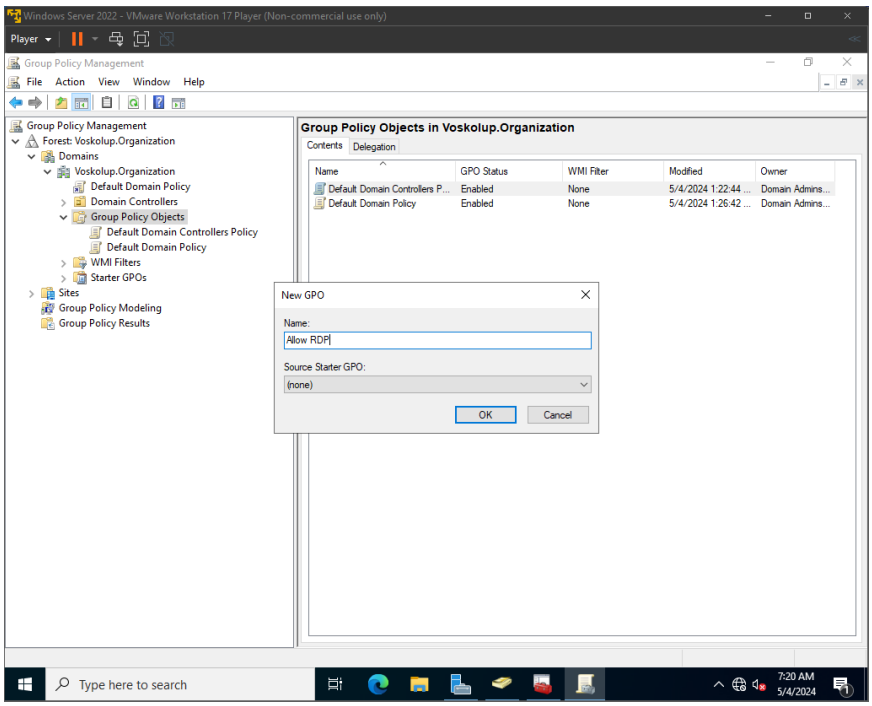


Рис. 3.10 Створення політики під назвою Allow GPO

Потім відкриваємо редагування політики та переходимо за шляхом Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections. Тут ми можемо побачити правило "Allow users to connect remotely using Remote Desktop Services", яке ми переводимо в статус "Enabled" (рис. 3.11).

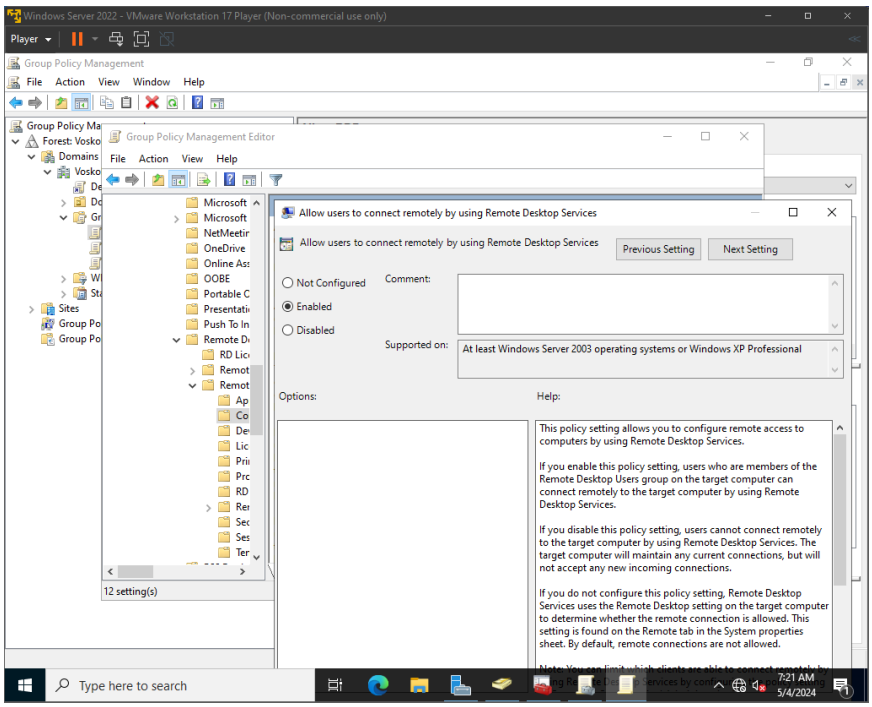


Рис. 3.11 Увімкнення правила Allow users to connect remotely

У сусідньому розділі "Security" вимикаємо опцію "Require user authentication for remote connections by using Network Level Authentications" (рис. 3.12).

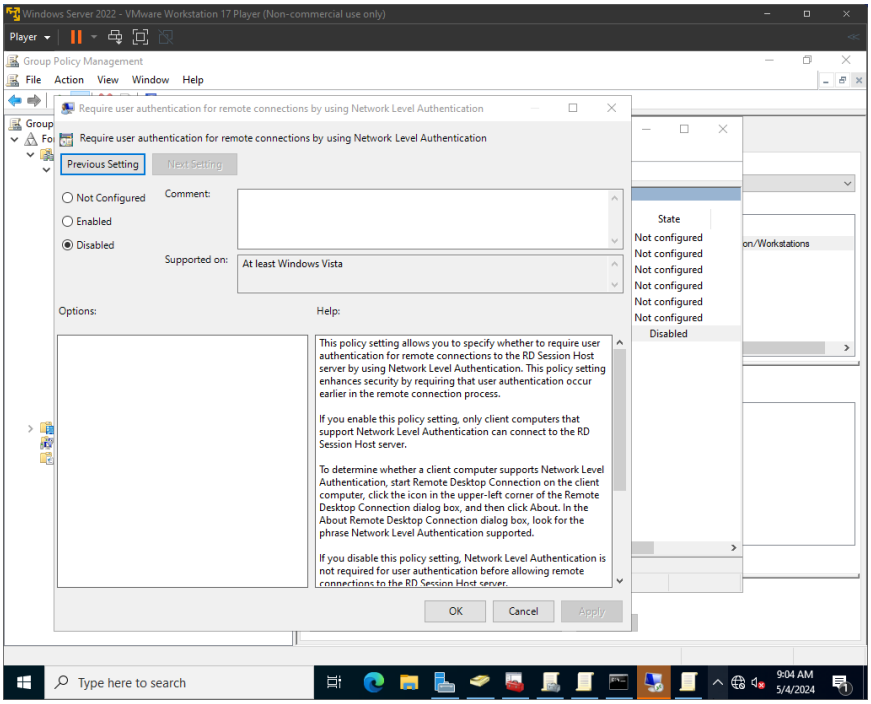


Рис. 3.12 Вимкнення правила Require user authentication for remote connections

Далі повертаємось назад, у Windows Settings > Security Settings > Windows Firewall Settings заходимо в "Inbound Rules" та створюємо нове правило на основі шаблону "Remote Desktop", дозволяючи підключення (рис. 3.13, рис. 3.14).

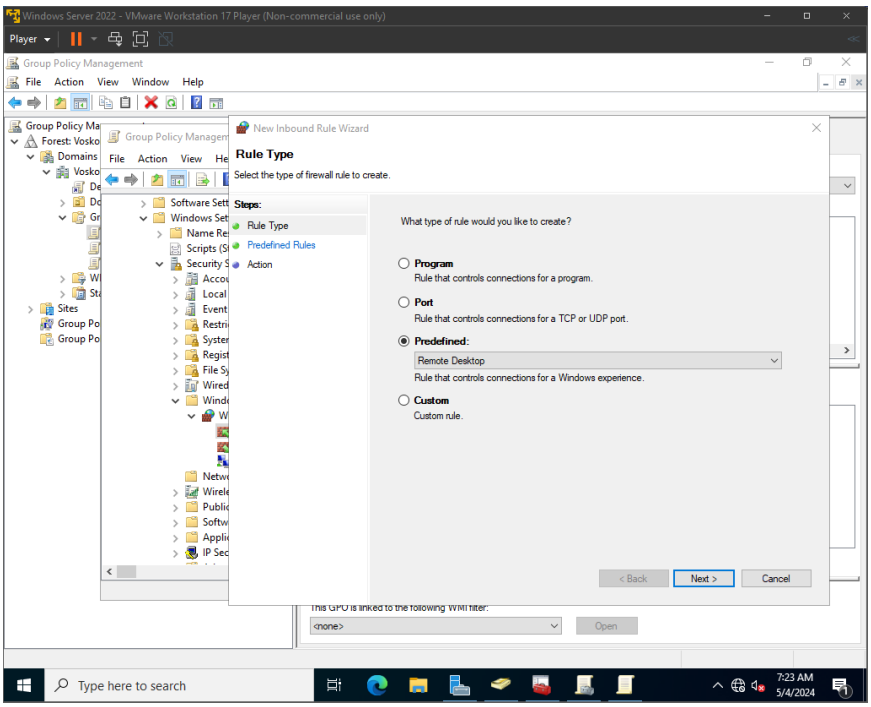


Рис. 3.13 Вибір шаблону Remote Desktop для вхідних підключень

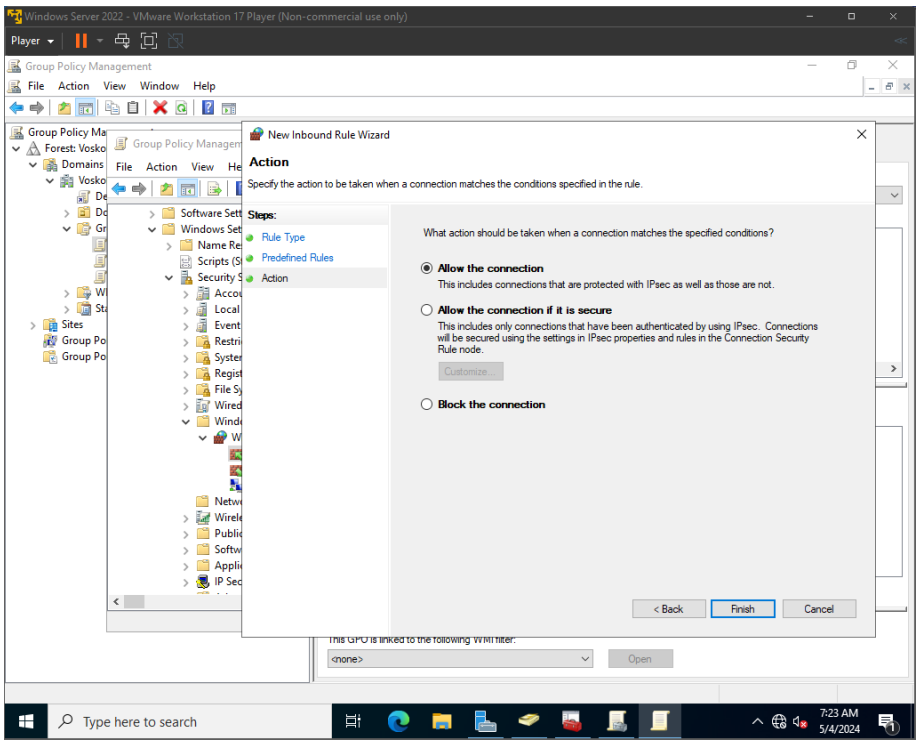


Рис. 3.14 Надання дозволу підключення на основі шаблону RDP

Додатково до налаштування віддаленого підключення важливо налаштувати Network Discovery, оскільки комп'ютер зараз просто не надає дані про себе у мережі. Для цього я створив нову політику з наступною назвою - "Enable Network Discovery" (рис. 3.15).

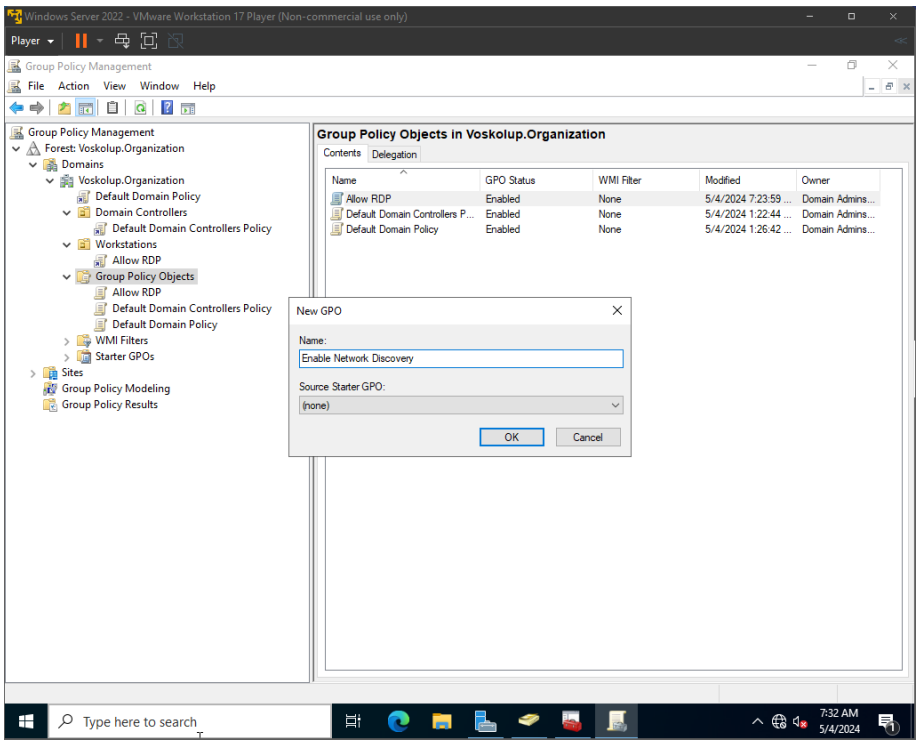


Рис. 3.15 Створення політики Enable Network Discovery

Далі, я перейшов у Windows Settings > Security Settings > Windows Firewall Settings і увійшов у "Inbound Rules". Там я створив нове правило на основі шаблону "File and Printer Sharing", вибрав тільки File and Printer Sharing (Echo Request - ICMPv4-In), та дозволив підключення (рис. 3.16).

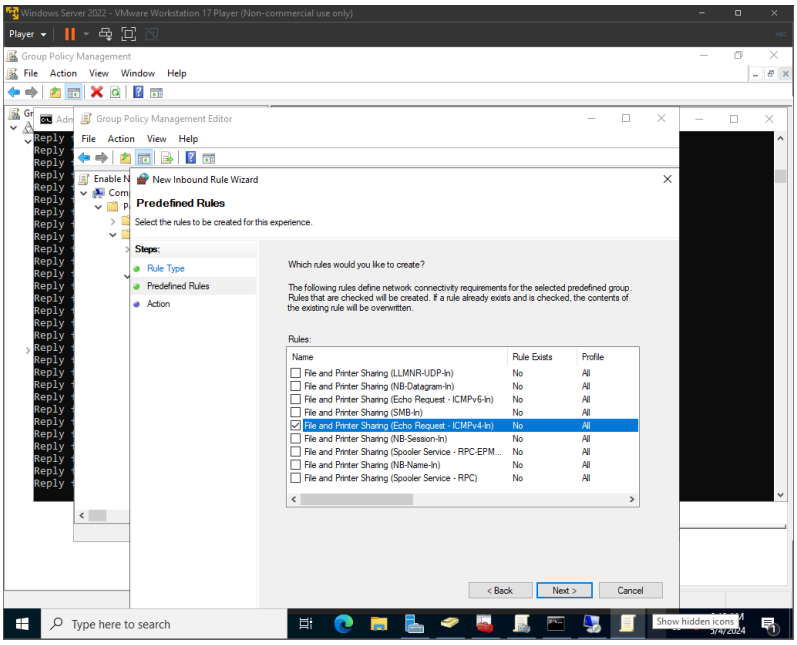


Рис. 3.16 Увімкнення правила File and Printer Sharing

Поруч, у розділі "Outbound Rules", я також створив правило на основі шаблону "Network Discovery" та дозволив підключення для всього (рис. 3.17, рис. 3.18).

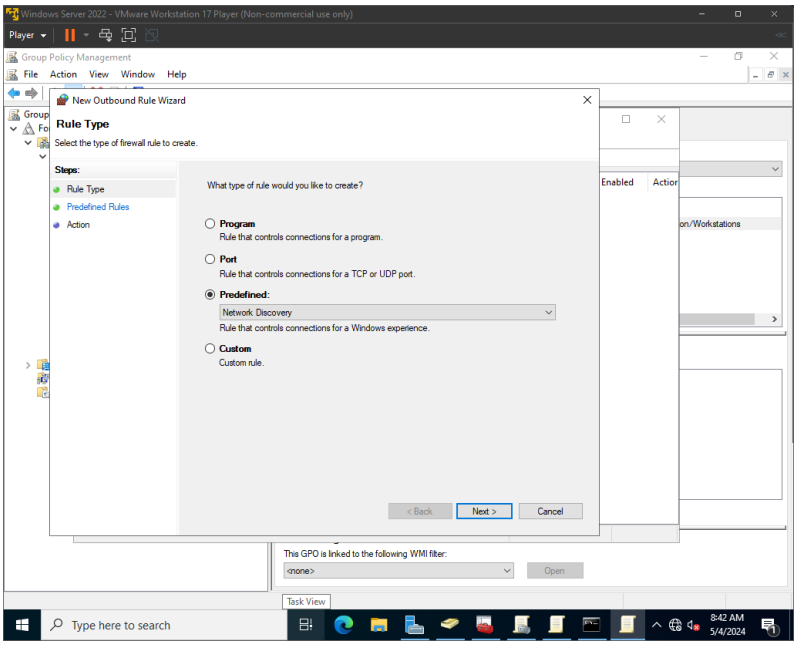


Рис. 3.17 Використання шаблону Network Discovery в вихідних підключеннях

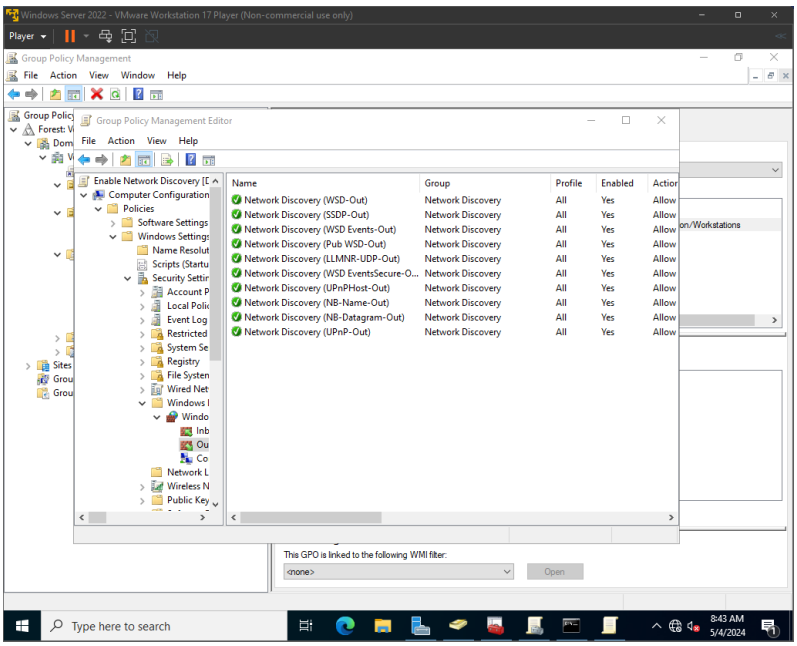


Рис. 3.18 Вікно Windows Firewall з списком дозволених вихідних підключень

Тепер, коли налаштовано необхідні політики для клієнтських машин, можна прив'язати ці політики до групової одиниці "Workstation". Це дозволить автоматично застосовувати ці налаштування до всіх комп'ютерів у цій групі.

Після прив'язки політик зроблено примусове оновлення політик на клієнтській машині, використовуючи команду "gpupdate /force" (рис. 3.19). Ці політики можуть оновитися на ПК самостійно, зазвичай оновлення іде один раз на 15 хвилин або після перезавантаження ПК.

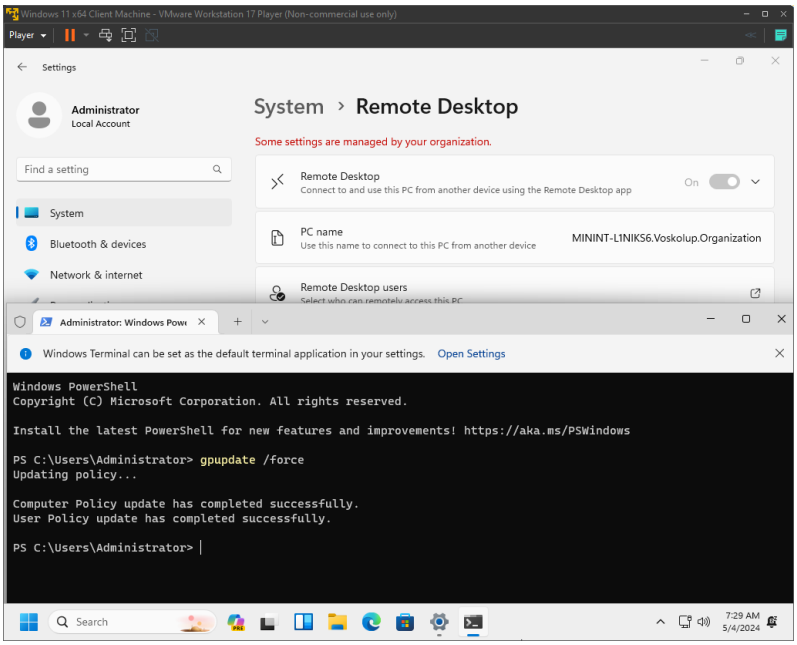


Рис. 3.19 Примусове оновлення політик

Тепер перевіримо, чи застосувались налаштування RDP, а також чи є можливість підключитись за допомогою віддаленого робочого столу. Це можна зробити шляхом спроби підключення до комп'ютера за допомогою RDP. Як можна побачити на скріншотах – все працює (рис. 3.20, рис. 3.21).

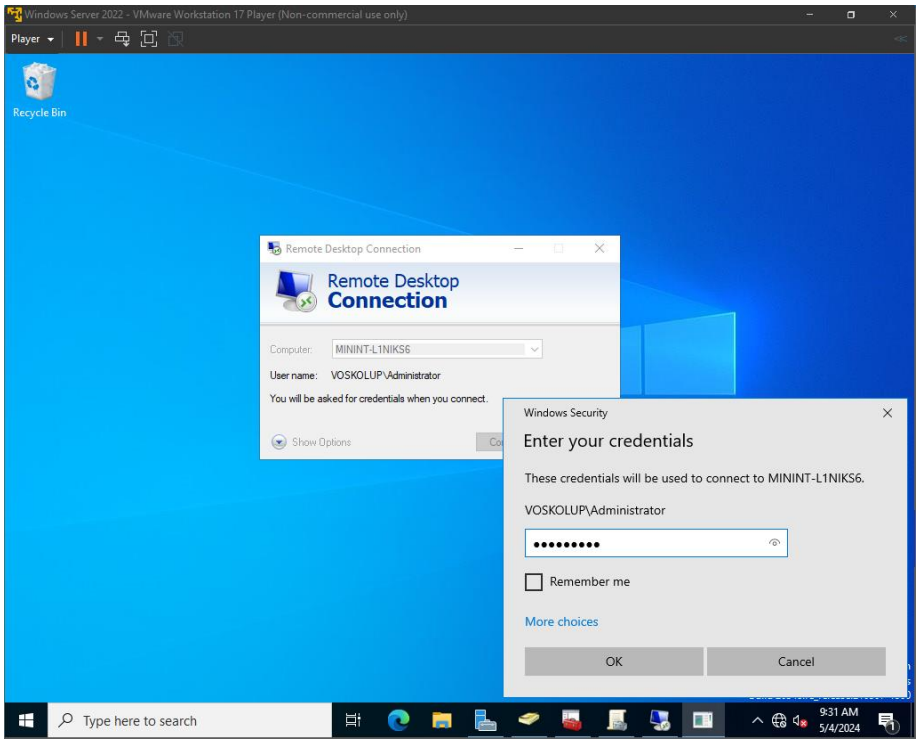


Рис. 3.20 Перевірка працездатності RDP

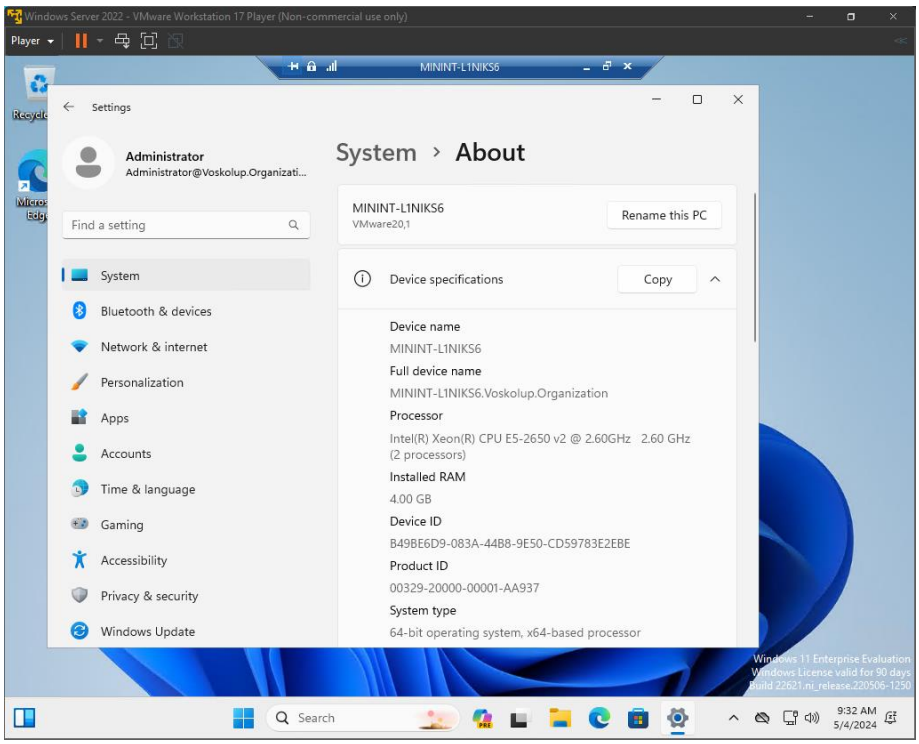


Рис. 3.21 Режим віддаленого підключення по RDP

Після успішного налаштування віддаленого підключення за допомогою RDP, ми переходимо до налаштування програми допомоги віддаленого доступу (msra). Для цього на серверному комп'ютері ми додаємо функції під назвою "Remote Assistance" (рис. 3.22).

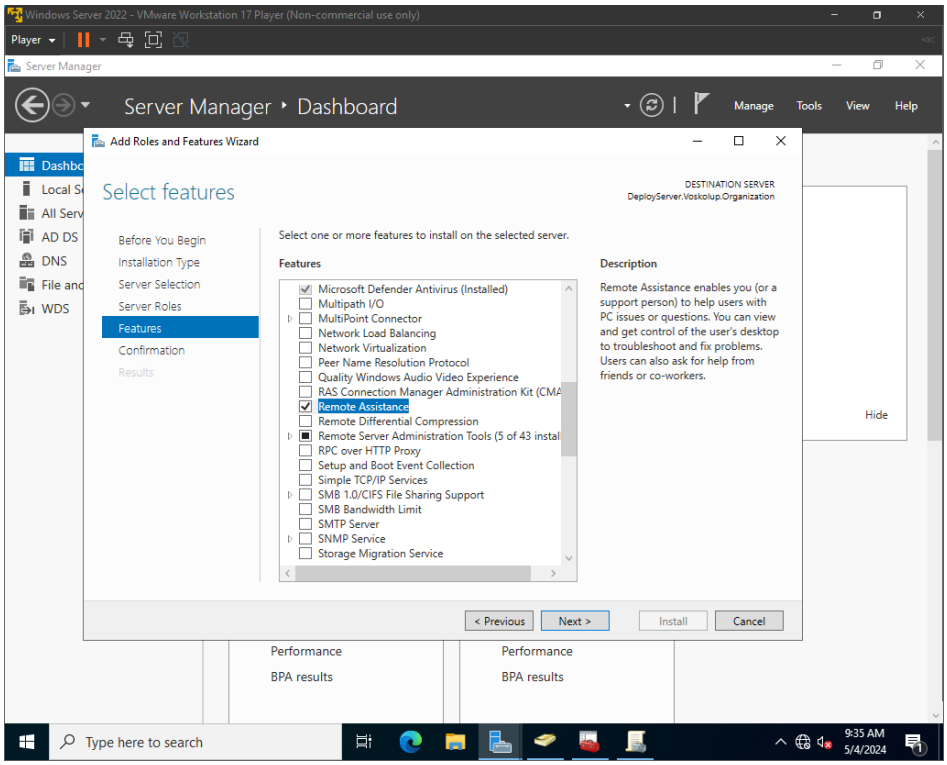


Рис. 3.22 Додавання функції Remote Assistance на серверну машину

Далі, у редакторі групових політик створюємо нову політику, я назвав її "Allow Remote Assistance".

У редакторі політик переходимо за шляхом Windows Settings > Security Settings > Windows Firewall Settings та у Inbound Rules створюємо правило, цього разу шаблона не буде, тому у майстрі створення правил вибираю Port і натискаю "Next", вказую протокол TCP для порту 135, у наступному розділі дозволяю всі підключення натискаючи Allow the connection (рис. 3.23). За замовчуванням всі вказані правила використовуються для всіх типів мереж, але якщо потрібно, то можна зайти у властивості правил, тільки для доменної та приватних мереж.

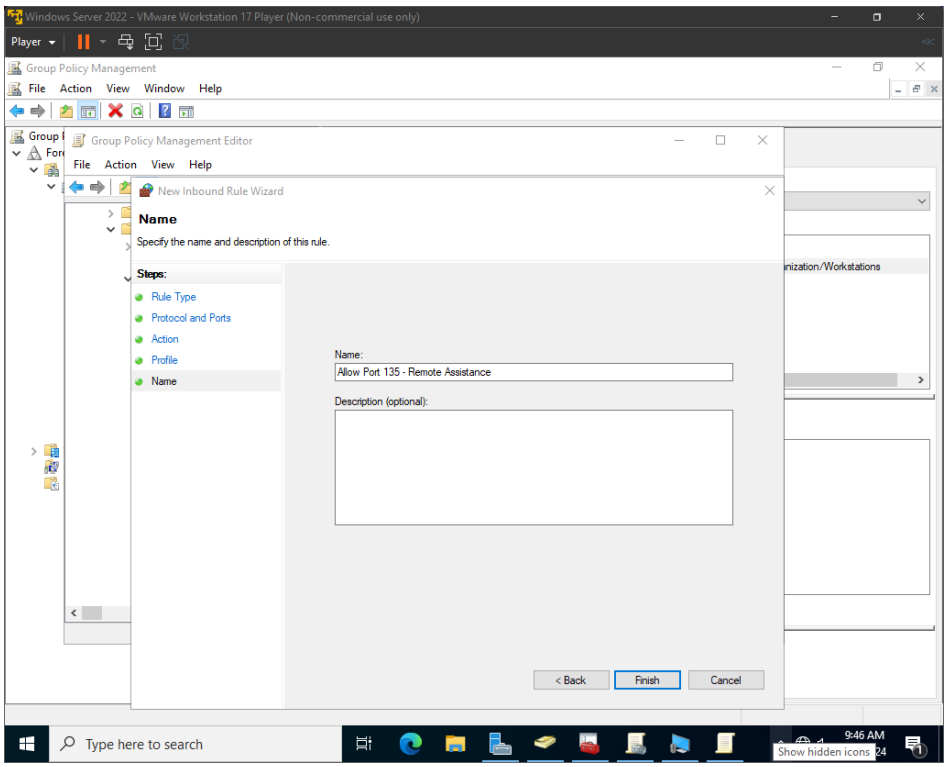


Рис. 3.23 Встановлення правила на підключення по 135 порту

Також, у Computer Configuration > Policies > Administrative Templates > System > Remote Assistance, у правилі "Configure Offer Remote Assistance", дозволяємо підключення для користувачів рівня адміністратора (рис. 3.24).

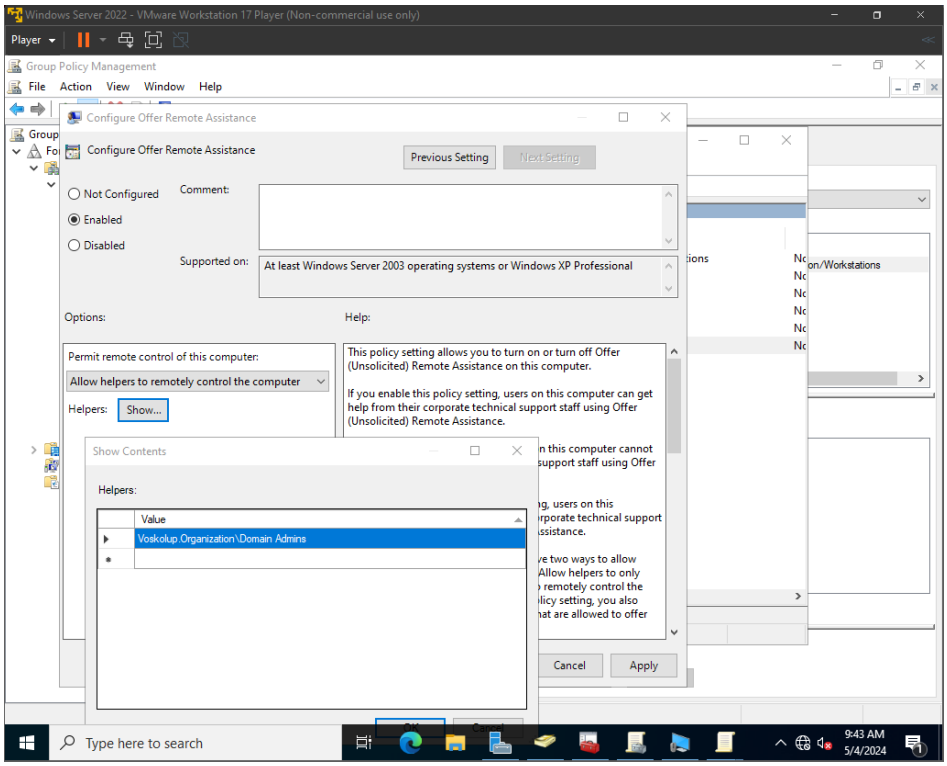


Рис. 3.24 Встановлення дозволу на підключення для групи адміністраторів

Після цього ми прив'язуємо правило для групової одиниці "Workstations", оновлюємо налаштування на клієнтській машині і перевіряємо можливість підключення (рис. 3.25). Як можна побачити по скріншотам, підключення працює успішно (рис. 3.26).

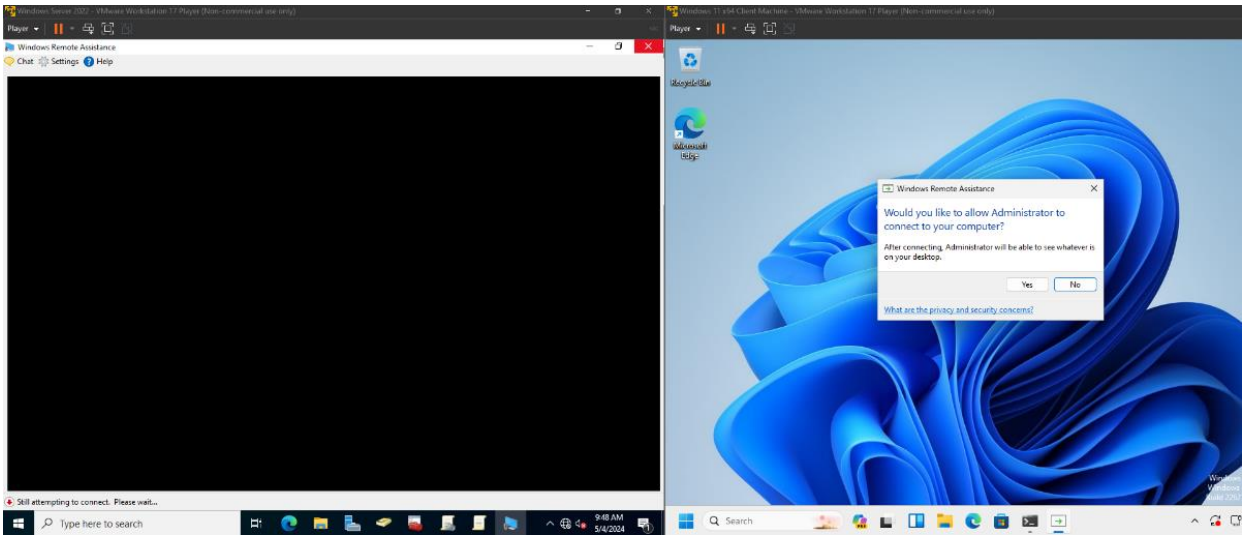


Рис. 3.25 Перевірка запиту та підключення MSRA

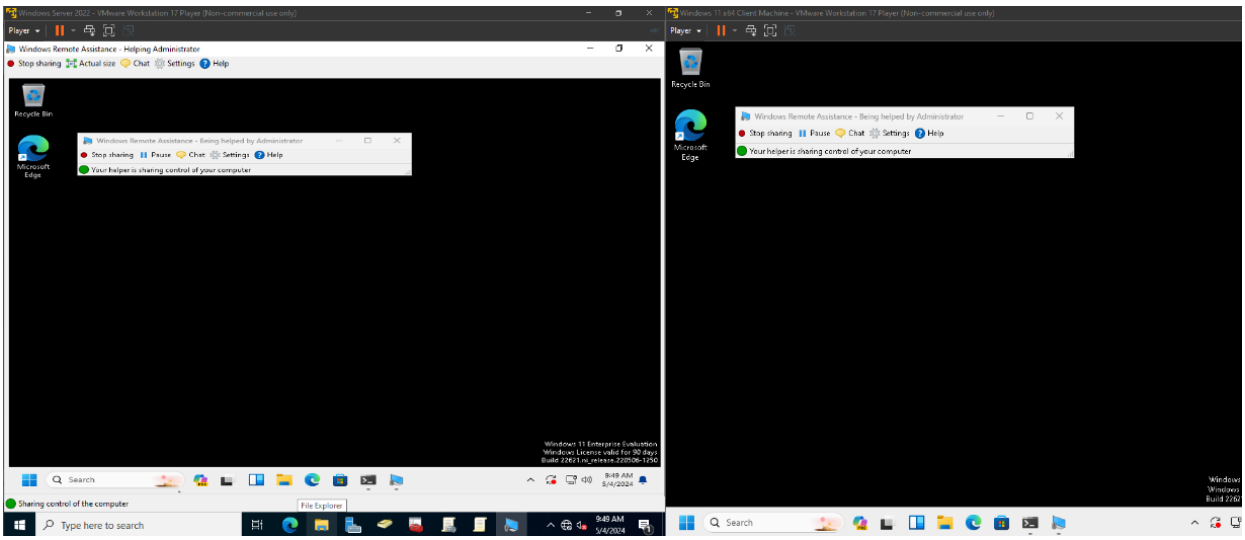


Рис. 3.26 Успішне підключення по MSRA

3.3 Керування програмним забезпеченням на клієнтському ПК

Тепер, коли успішно налаштовано віддалене підключення, можна розглянути процес розгортання додаткової програми на комп'ютери через групові політики.

Спочатку на серверній машині були створені папки Share/Install, а доступ до них було надано через мережу для всіх на читання (рис. 3.27).

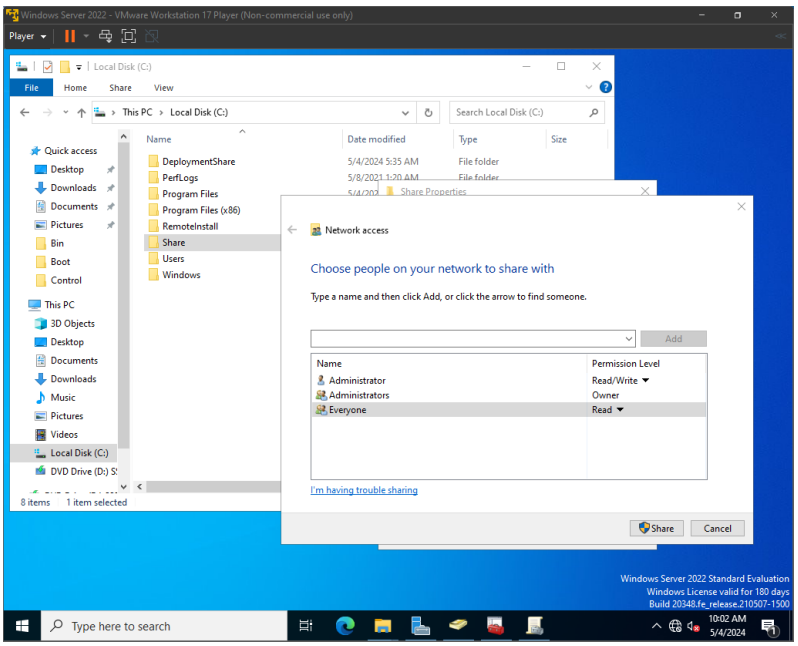


Рис. 3.27 Надання мережевого доступу до папки Share

Як приклад програми - я взяв Microsoft Teams у форматі msi, завантаживши його до нещодавно створеної папки.

Потім було створено нову політику в менеджері політик під назвою "Deploy Teams". У редакторі політик ми перейшли за шляхом Computer Configuration > Polices > Software Settings, вибрали опцію встановлення ПЗ та вказали мережевий шлях до нашого файлу, у моєму випадку - \\DEPLOYSERVER\Share\Install\Teams_windows_x64.msi (рис. 3.28, рис. 3.29).

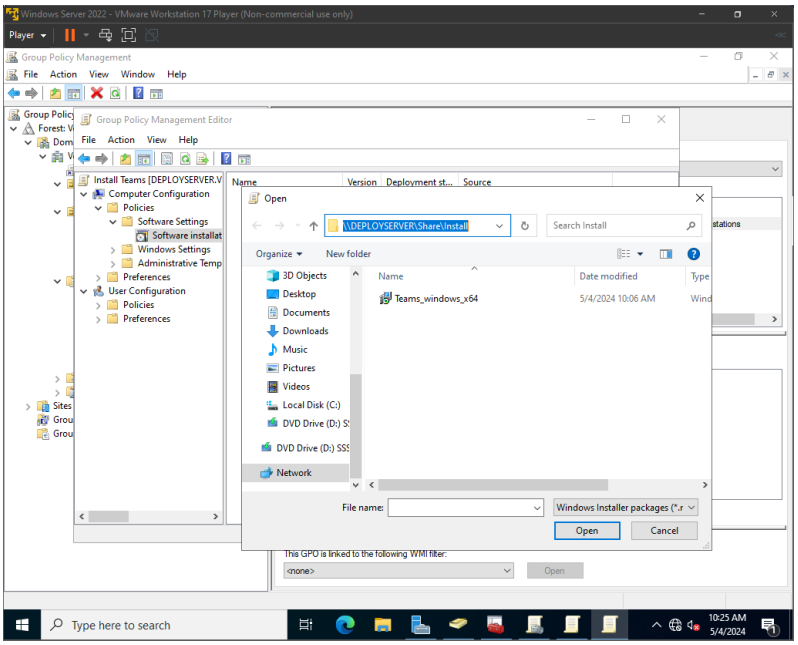


Рис. 3.28 Вказання мережевого шляху до інсталятора

Важливо зазначити, що вибір файлу через провідник без вказання мережевого шляху не призведе до нічого, і редактор додатково попередить, що сталася помилка.

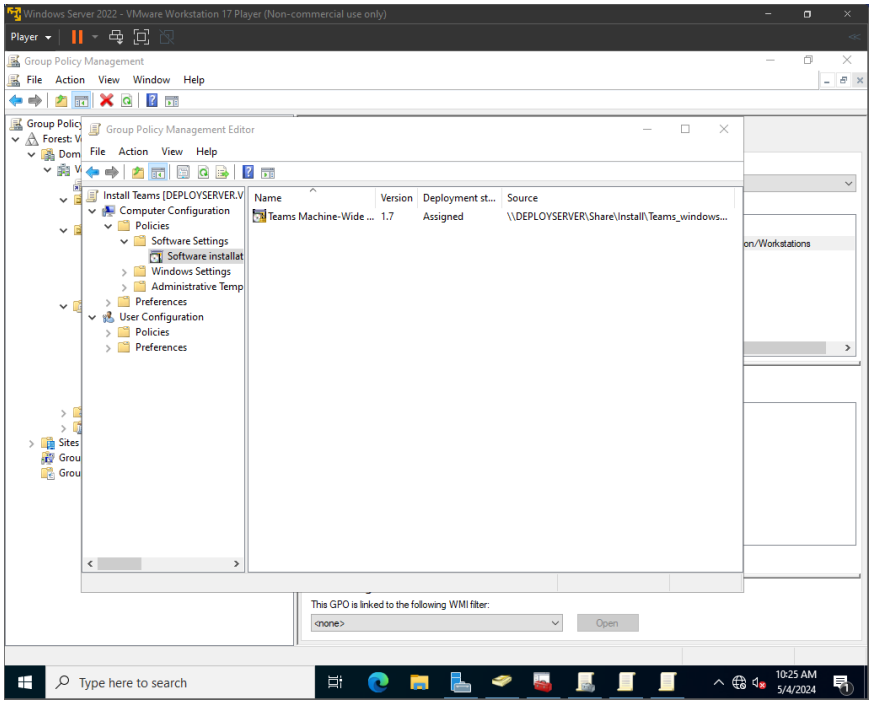


Рис. 3.29 Вікно з програмами, що повинні бути інстальовані

Після цього знову прив'язано політику до групової одиниці "Workstations" та клієнтський комп'ютер було відправлено на перезавантаження. Після завантаження одразу з’явилось вітання Teams, що свідчить про успішне розгортання (рис. 3.30).

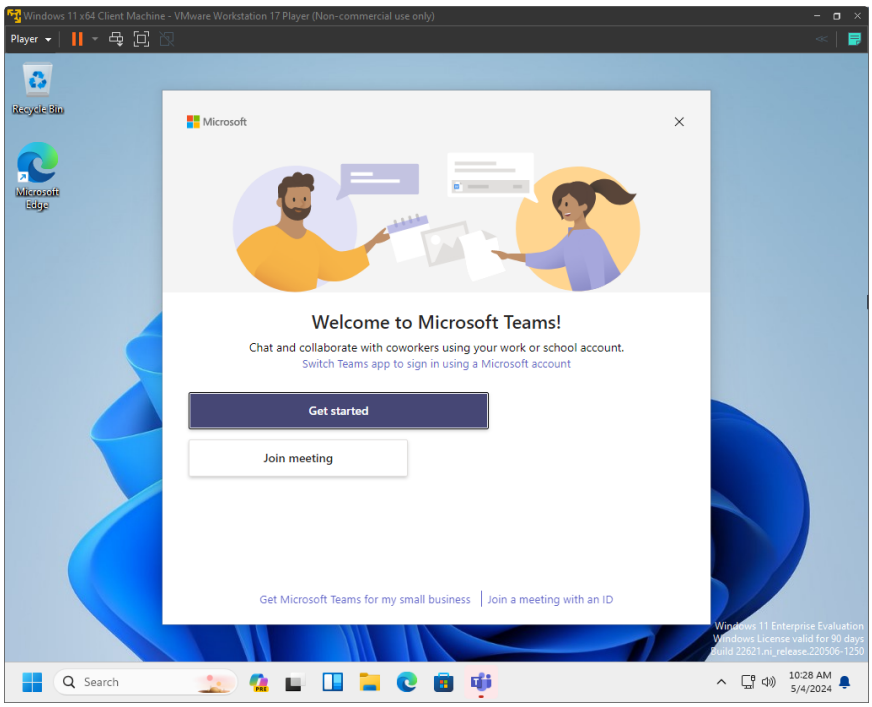


Рис. 3.30 Вікно вітання Teams на клієнтському ПК

Щоб видалити програму, можна скористатися тією ж груповою політикою, вибравши опцію видалення на всіх ПК (рис. 3.31), де вона була встановлена, щоб пришвидшити процес знову перезавантажую комп’ютер та перевіряю наявність програми (рис. 3.32).

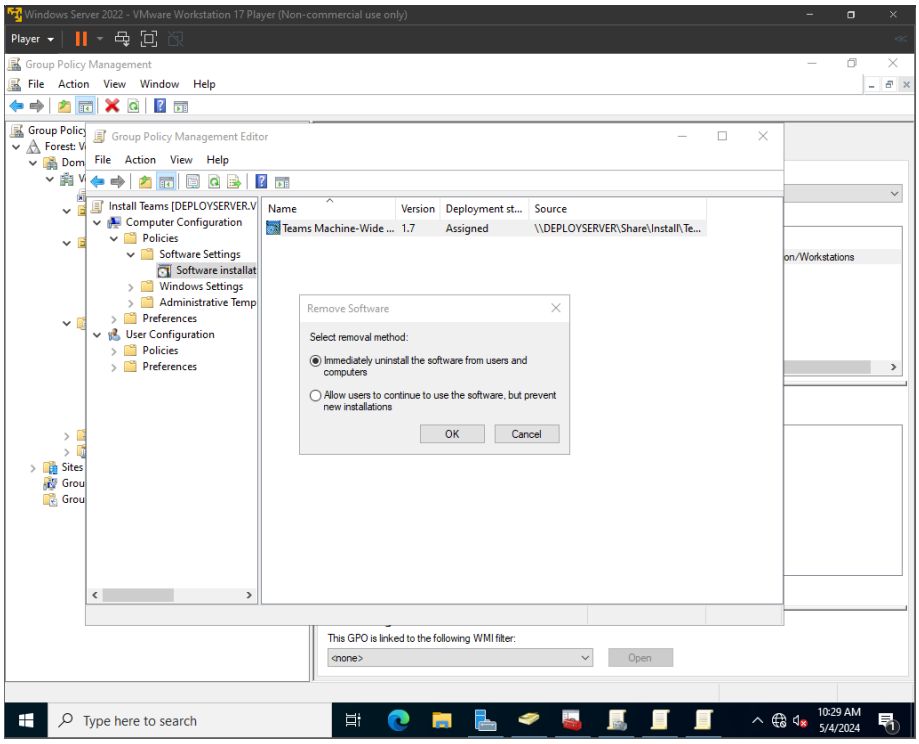


Рис. 3.31 Видалення ПЗ Teams через політики

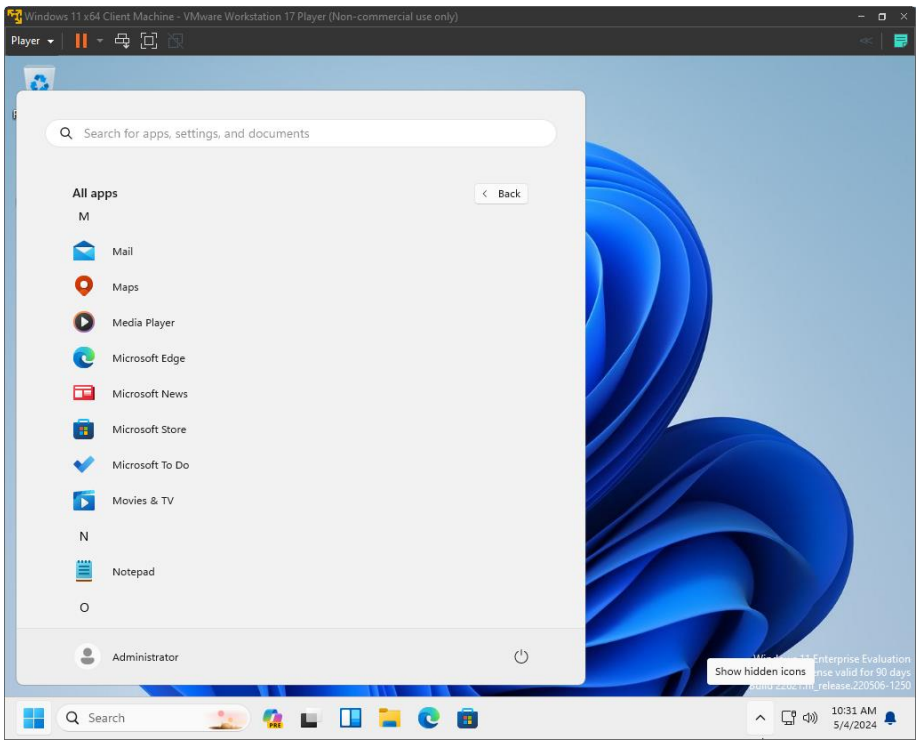


Рис. 3.32 Демонстрація відсутності ПЗ Teams на клієнтському ПК

ВИСНОВКИ

Було розглянуто процес створення та налаштування інфраструктури віртуалізації та автоматизованого розгортання операційних систем та програмного забезпечення за допомогою різних інструментів, зокрема VMware Workstation, Windows Deployment Services (WDS), Microsoft Deployment Toolkit (MDT), а також групових політик Active Directory.

Більшість інструментів можна використовувати напряму встановивши їх з Server Manager, що постачається в Windows Server 2022 Standard Evaluation (Desktop Experience), робота продовжилася налаштуванням серверних ролей, встановленням та конфігуруванням служб, таких як Active Directory, DNS, та Windows Deployment Services.

За допомогою Microsoft Deployment Toolkit було автоматизовано розгортання операційних систем та додаткового програмного забезпечення на клієнтські машини. Додатково було налаштовано різні аспекти віддаленого управління, такі як віддалений робочий стіл (RDP) та допомога віддаленого доступу (msra), а також налаштовано правила мережевого фаєрволу для забезпечення безпеки.

Завершальним етапом було розгортання додаткових програм на клієнтські машини через групові політики, зокрема за допомогою Microsoft Teams. Це дозволило створити повністю автоматизовану систему управління інфраструктурою та програмним забезпеченням у корпоративному середовищі.

Важливо також зазначити, що система може бути модифікована для отримання більшої кількості можливостей для керування клієнтськими системами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Server Manager [Електронний ресурс] / Microsoft Learn - Режим доступу: https://learn.microsoft.com/en-us/windows-server/administration/server-manager/server-manager
2. Using the Microsoft Deployment Toolkit [Електронний ресурс] / Microsoft Learn - Режим доступу: https://learn.microsoft.com/en-us/mem/configmgr/mdt/use-the-mdt
3. Working with the Administrative Template policy settings using the Local Group Policy Editor [Електронний ресурс] / Microsoft Learn - Режим доступу: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789184(v=ws.11)
4. Windows Deployment Services Overview Manager [Електронний ресурс] / Microsoft Learn - Режим доступу: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764(v=ws.11)
5. Download VMware Workstation Player [Електронний ресурс] / VMware by Broadcom. - Режим доступу: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
6. Windows Server 2022 download [Електронний ресурс] / Microsoft Evaluation Center - Режим доступу: https://www.microsoft.com/en-us/evalcenter/download-windows-server-2022
7. Microsoft Deployment Toolkit [Електронний ресурс] / Microsoft Download Center - Режим доступу: https://www.microsoft.com/en-us/download/details.aspx?id=54259
8. Download and install the Windows ADK [Електронний ресурс] / Microsoft Learn - Режим доступу: https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install
9. Windows 11 Enterprise download [Електронний ресурс] / Microsoft Evaluation Center - Режим доступу: https://www.microsoft.com/en-us/evalcenter/download-windows-11-enterprise

10. Bulk install classic Teams using Windows Installer (MSI) [Електронний ресурс] / Microsoft Learn - Режим доступу: https://learn.microsoft.com/en-us/microsoftteams/msi-deployment
11. Download 7-Zip [Електронний ресурс] / 7-ZIP - Режим доступу: https://www.7-zip.org/download.html

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація
до кваліфікаційної роботи на здобуття освітнього ступеня бакалавра
на тему: **«Управління корпоративною інфраструктурою в середовищі Windows: використання доменних функцій для оптимізації розгортання та налаштування техніки»**

Виконав: здобувач вищої освіти
гр. КНД-41 Євген ВОСКОЛУП

Керівник: Микола ГНІДЕНКО

Мета роботи, об’єкт та предмет дослідження

- **Мета роботи** – вивчення методів розгортання операційних систем, розробка та реалізація ефективного процесу автоматизованого налаштування інфраструктури мережевого середовища з використанням різноманітних інструментів.
- **Предмет дослідження** – інструменти для розгортання операційних систем, групові політики, налаштування віддаленого доступу, процеси автоматизації у сфері інформаційних технологій.
- **Об`єкт дослідження** – процеси автоматизації розгортання та налаштування серверних та клієнтських операційних систем.

Методи розгортання

Ручне розгортання - передбачає встановлення операційної системи на кожному ПК індивідуально.

Цей метод включає:

- Встановлення ОС з носія (наприклад, USB-накопичувача або DVD).
- Налаштування системи та встановлення необхідних драйверів і програмного забезпечення.

Недоліки:

- Трудомісткість: потребує багато часу та зусиль.
- Непослідовність: можливі варіації в налаштуваннях між ПК.

Масове розгортання за допомогою Windows Deployment Services (WDS) - дозволяє одночасно встановлювати операційну систему на велику кількість ПК через мережу.

Основні етапи цього методу включають:

- Налаштування WDS-сервера.
- Створення образів ОС і їх збереження на сервері.
- Розгортання образів на клієнтських ПК через мережу за допомогою PXE-завантаження.

Переваги:

- Ефективність: швидке одночасне розгортання на багатьох ПК.
- Консистентність: всі ПК отримують однакову конфігурацію і програмне забезпечення.
- Автоматизація: мінімізація ручної роботи та можливість планування автоматичного розгортання.

Опис основного функціоналу

Windows Deployment Services (WDS) забезпечує мережеве розгортання операційних систем Windows, дозволяючи встановлювати ОС на комп’ютери без використання фізичних носіїв.

Group Policy Manager (GPM) керує груповими політиками в доменах Active Directory, автоматизуючи управління та конфігурацію комп'ютерів і користувачів.

Remote Desktop Protocol (RDP) дозволяє віддалене підключення до комп'ютерів, забезпечуючи доступ до робочого столу та ресурсів комп'ютера через мережу.

Microsoft Remote Assistance (MSRA) надає можливість дистанційної підтримки, дозволяючи одному користувачу запрошувати іншого для надання допомоги через спільний доступ до екрана.

Середовище використання автоматизованої системи

У рамках інфраструктури офісу повинна бути наявна локальна мережа (LAN), яка є ключовим елементом забезпечення зв'язку між комп'ютерами, принтерами та іншими мережевими пристроями в офісі. Ця мережа дозволяє спільний доступ до ресурсів, обмін даними та забезпечує комунікацію між співробітниками.

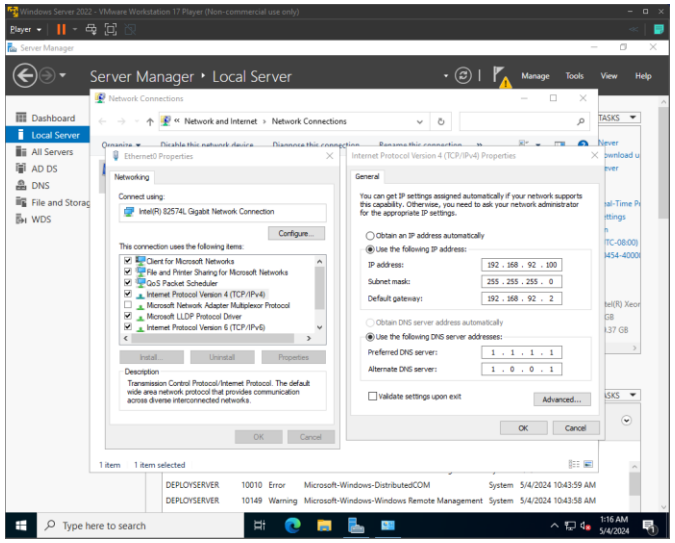
В мережі можуть бути реалізовані заходи безпеки, такі як використання паролів, шифрування даних, фаєрвол та інші методи захисту для забезпечення конфіденційності та цілісності інформації, що передається через мережу, тому слід заздалегідь розблокувати порти, які використовує Microsoft Deployment Toolkit, а саме:

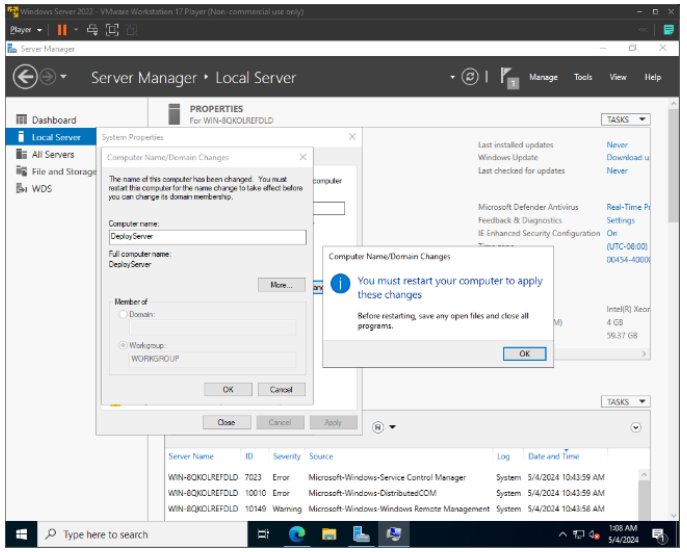
- TCP порт 139 - для доступу до файлового сервера або розподіленого сховища, де знаходяться образи операційних систем та програм.
- TCP порт 445 - аналогічно, для доступу до файлового сервера або сховища.
- TCP порт 3389 - для віддаленого доступу до серверів, де розміщені засоби MDT.

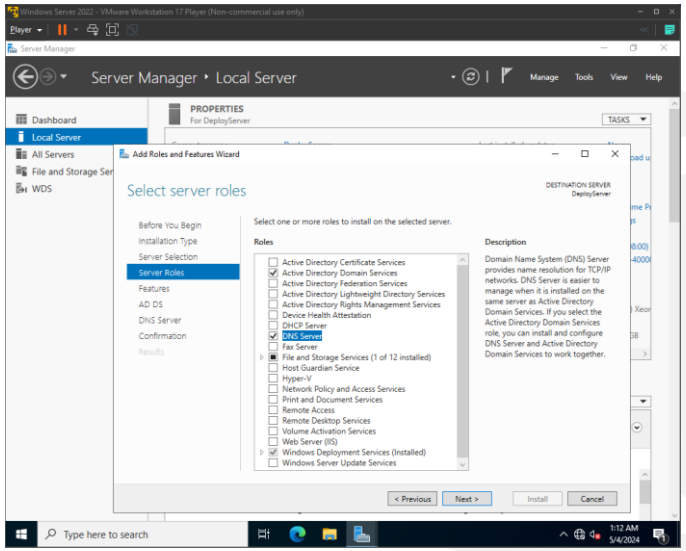
Для реалізації серверного середовища був використаний образ операційної системи Windows Server 2022

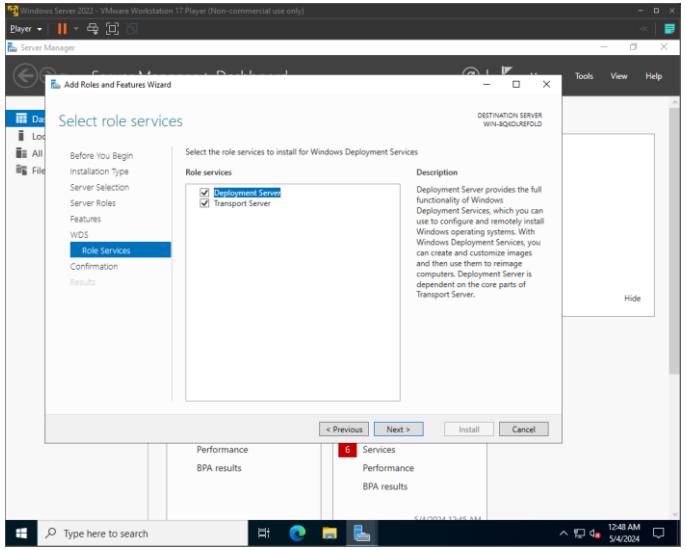
Підготовка ПК-Сервера

ПК-Сервер було створено, а на ньому встановлено операційну систему Windows Server 2022. Після встановлення було змінено його ім'я на DeployServer для відображення його призначення в мережі. Також були змінені мережеві налаштування з метою надання серверу статичної IP-адреси, забезпечуючи стабільну та надійну комунікацію у мережі.









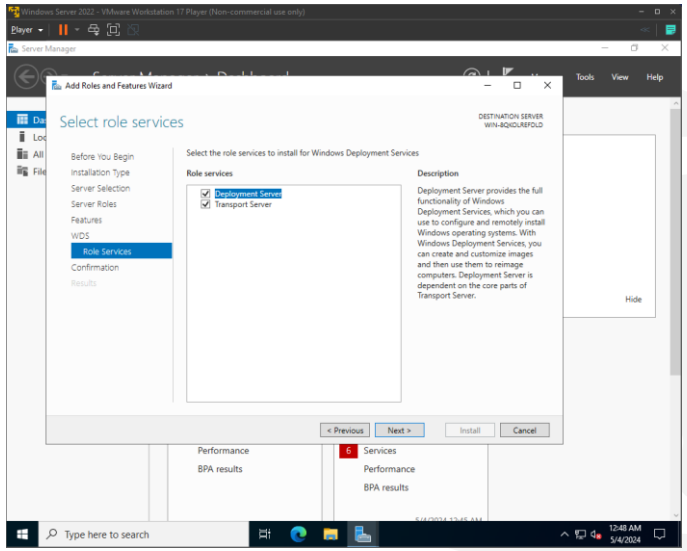
Первинні налаштування

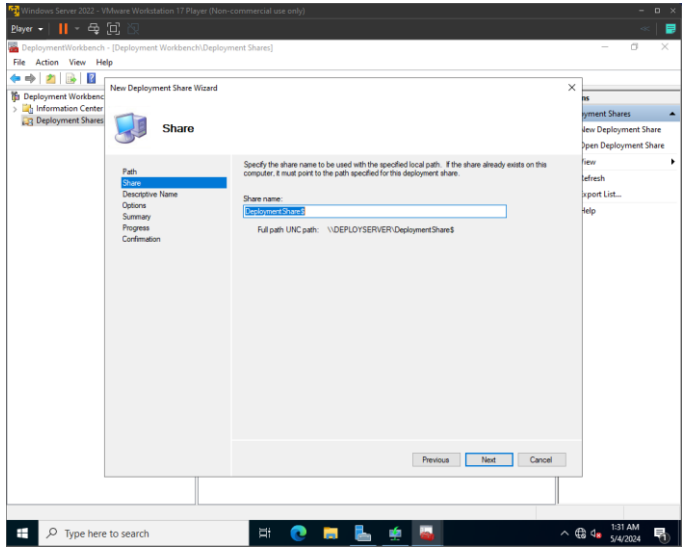
У Server Manager було додано та первинно налаштовано наступні елементи:

- Active Directory (AD) - дозволяє налаштовувати та керувати доменами, організаційними одиницями, об'єктами користувачів та групами в мережевому середовищі.
- Інтеграція DNS Server - дозволяє забезпечити розподіл та перетворення імен доменів в IP-адреси, що необхідно для правильної роботи мережевого середовища.
- Windows Deployment Services (WDS) - надає можливість розгортання операційних систем Windows через мережу. Вона дозволяє встановлювати Windows на багато комп'ютерів одночасно з централізованого сервера.

Після цього з Інтернету було завантажено та встановлено додаткові компоненти:

- Microsoft Deployment Toolkit (MDT) - інструмент для автоматизованого розгортання операційних систем Windows та додаткових програм на комп'ютерах. Використовується для створення образів системи та їх розгортання на різних пристроях.
- Windows Assessment and Deployment Kit (ADK) - містить інструменти для налаштування та автоматизації розгортання Windows. Включає засоби для створення інсталяційних образів, відлагодження та тестування операційних систем.
- Windows PE add-on for ADK - це додатковий компонент, який дозволяє використовувати Windows Preinstallation Environment (Windows PE) для розгортання та відновлення операційних систем Windows. Windows PE є легковаговим середовищем.





Налаштування WDS та MDT

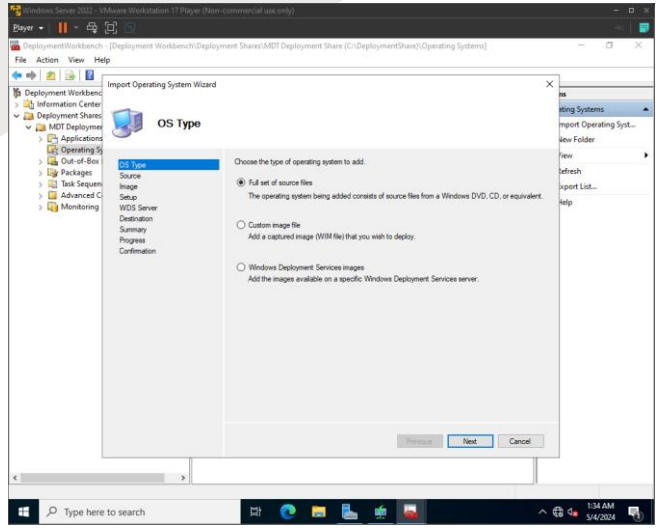
Було сконфігуровано сервер у Windows Deployment Services (WDS), який у майбутньому буде використано для імпорту образу операційної системи. Сервер WDS налаштований таким чином, щоб забезпечити ефективне розгортання операційних систем через мережу, використовуючи технологію PXE (Preboot Execution Environment). Цей сервер стане центральним елементом для розповсюдження завантажувальних образів на клієнтські машини.

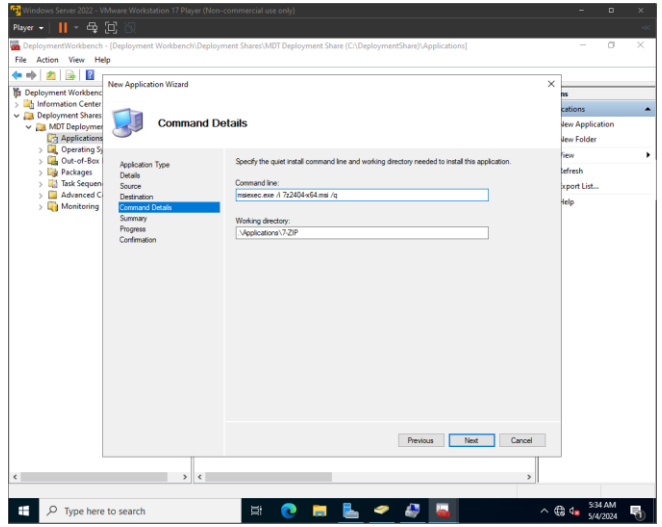
У Microsoft Deployment Toolkit (MDT) було створено новий Deployment Share, який зберігає всі необхідні файли та налаштування для розгортання операційних систем. Deployment Share має мережеве розташування \DEPLOYSERVER\DeploymentShare$, що дозволяє адміністраторам зручно керувати та доступатися до ресурсів для розгортання з будь-якої точки мережі. Це мережеве розташування забезпечує централізоване зберігання всіх компонентів розгортання, включаючи образи операційних систем, драйвери, скрипти, а також конфігураційні файли.

Імпортування ОС та ПЗ

Було змонтовано та імпортовано образ операційної системи Windows 11 Enterprise. Цей образ операційної системи був доданий у MDT, щоб забезпечити можливість розгортання Windows 11 Enterprise на клієнтських комп’ютерах у мережі. Процес імпорту образу включав перевірку сумісності та вказання шляху до змонтованого образу.

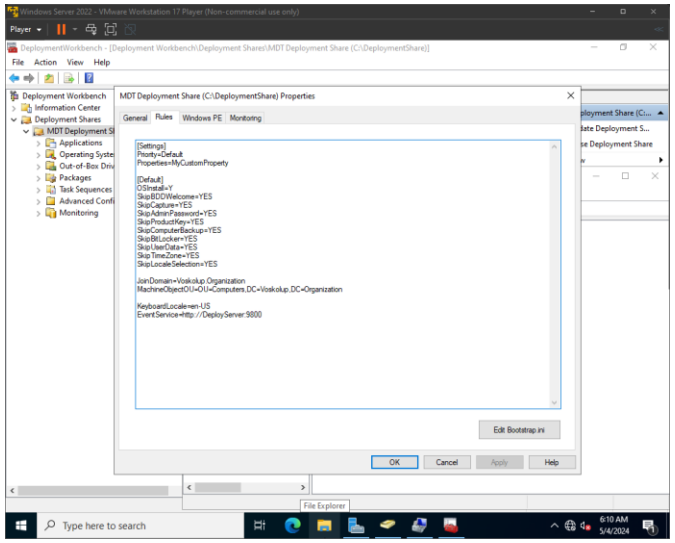
Після імпорту операційної системи було імпортовано додаток 7-zip до MDT Deployment Share. Під час налаштування параметрів для 7-zip, додатково була вказана команда тихого встановлення, яка дозволяє інсталювати програму без взаємодії з користувачем, що значно спрощує автоматизоване розгортання програмного забезпечення.

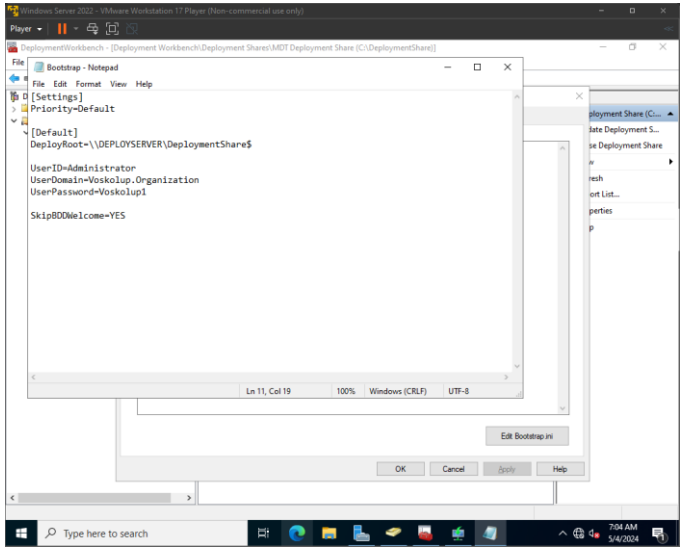


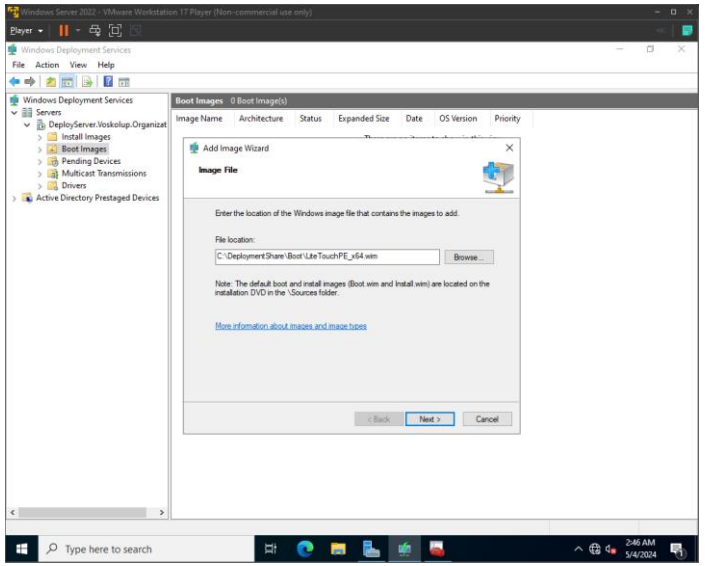


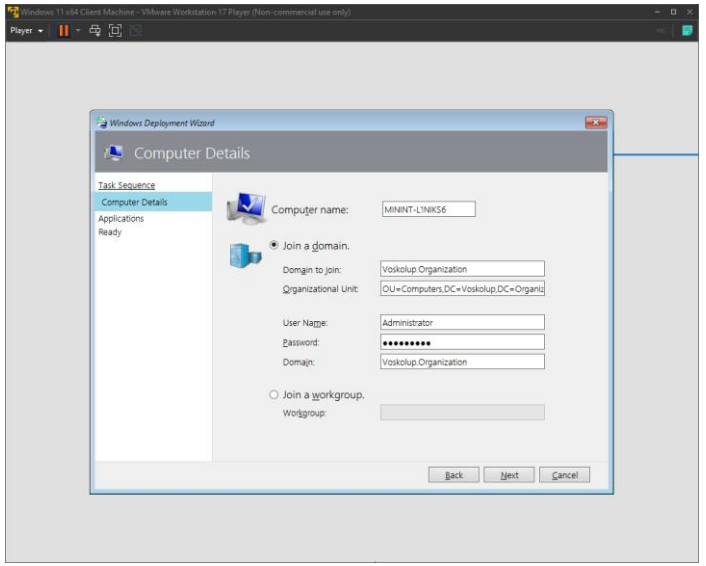
Створення та налаштування сценарію

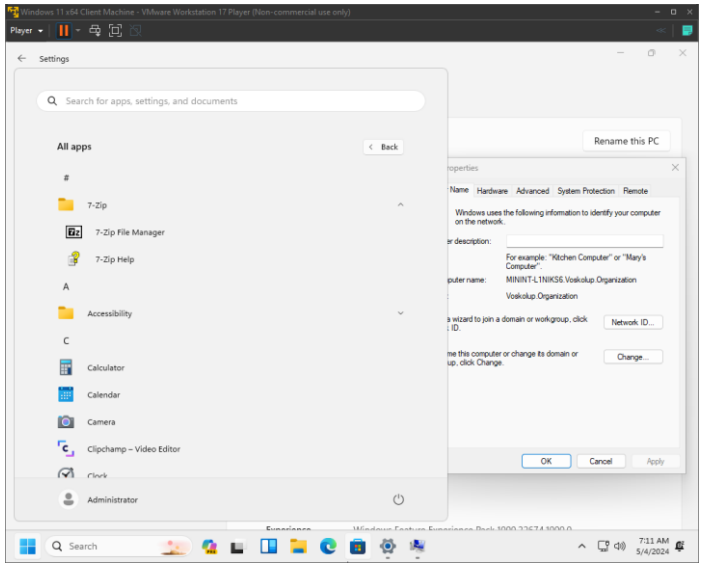
Створено сценарій (task sequence), в якому була вибрана раніше імпортована операційна система Windows 11 Enterprise. У цьому сценарії також було налаштовано профіль користувача та пароль адміністратора. У налаштуваннях MDT Deployment Share було вимкнуто підтримку платформи x86 (32-біта), що забезпечує розгортання лише 64-бітних систем, увімкнено функцію моніторингу та внесено наступні правила для CustomSettings.ini та bootstrap.ini, налаштування яких можна побачити на скріншоті.







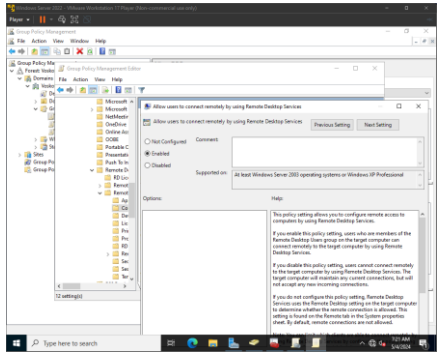


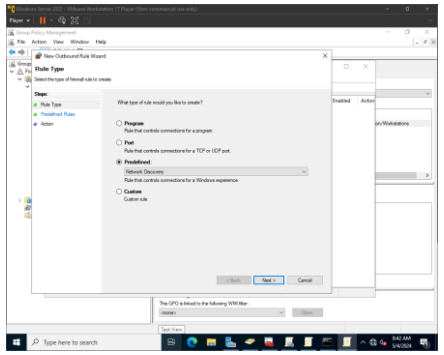


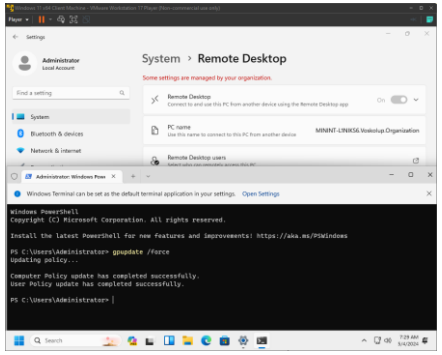
Генерація образу

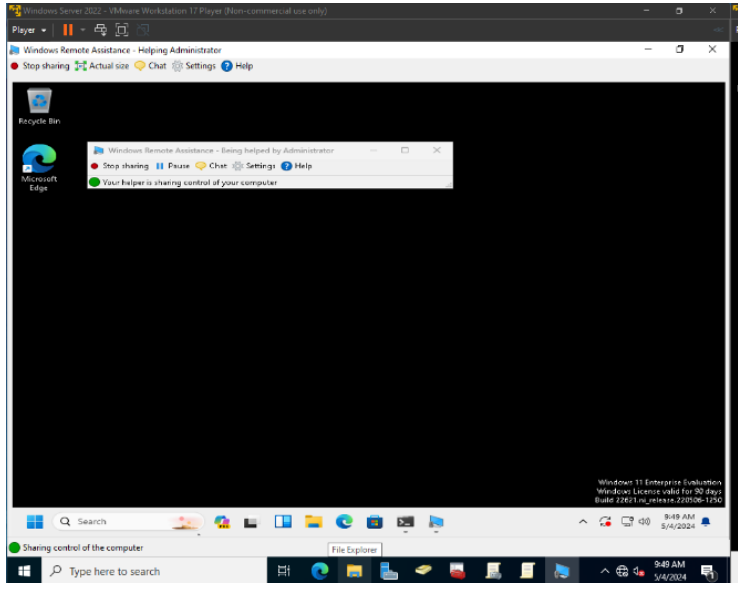
У налаштуваннях MDT Deployment Share було проведено регенерацію образу, після чого створений .wim файл був імпортований у Windows Deployment Services (WDS). Цей процес забезпечує оновлення всіх необхідних компонентів та налаштувань в образі перед його розгортанням на клієнтських машинах.

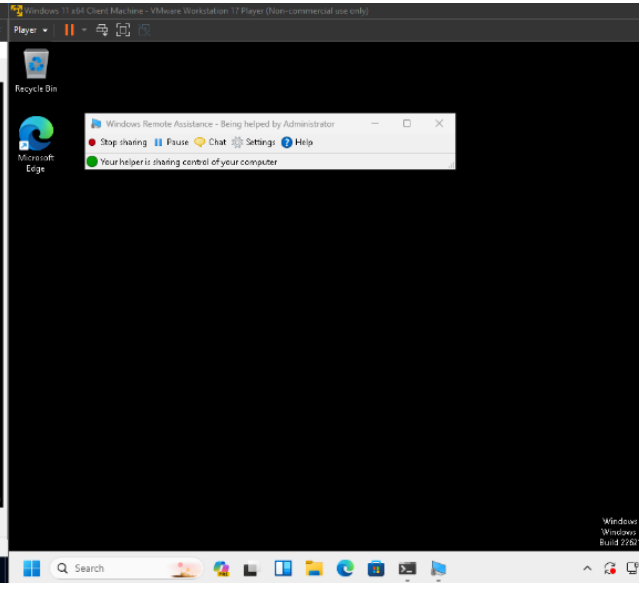
Після цього, на клієнтській машині було здійснено завантаження через мережу, використовуючи сервер WDS. Завантаження з мережі дозволило автоматично застосувати всі налаштування та конфігурації, визначені у сценарії розгортання. В результаті, операційна система Windows 11 Enterprise була встановлена з урахуванням всіх заданих параметрів, включаючи приєднання до домену та встановлення заданого ПЗ.





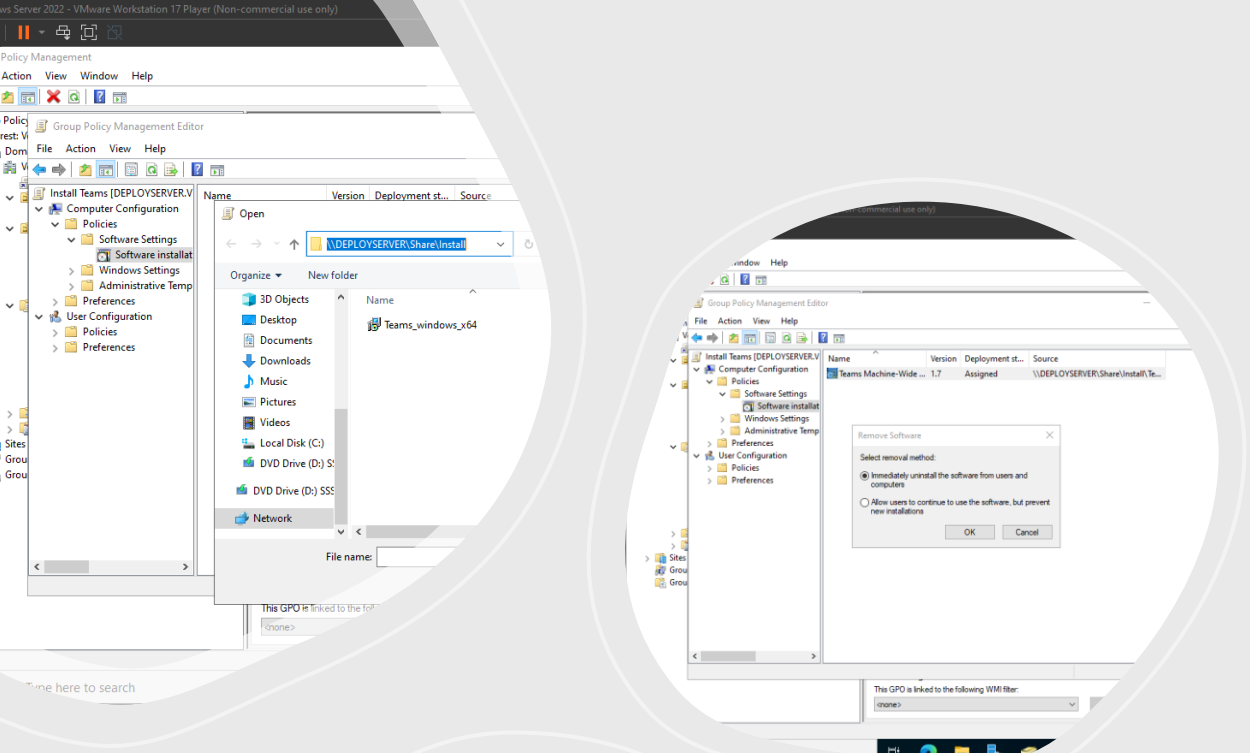


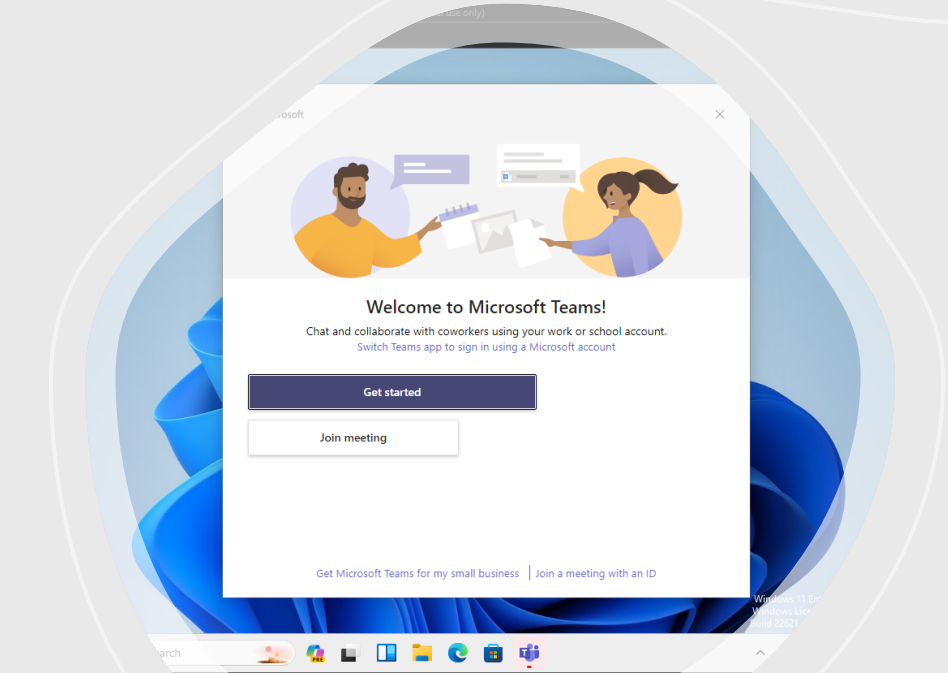




Налаштування віддаленого підключення

Через групові політики було налаштовано дозвіл на підключення до цієї клієнтської машини за допомогою протоколів Remote Desktop Protocol (RDP) та Microsoft Remote Assistance (MSRA). Крім того, було увімкнено можливість мережевого обміну, щоб комп'ютер був доступним для інших пристроїв у мережі.





Встановлення додаткового ПЗ

Через групові політики на клієнтську машину було успішно розгорнуто програмне забезпечення Microsoft Teams. Для цього спочатку була створена мережева папка, в яку був поміщений інсталяційний файл програми. При додаванні програмного забезпечення через групові політики також був вказаний мережевий шлях до цієї папки. На клієнтському ПК після перезавантаження системи програмне забезпечення автоматично встановилося.

При необхідності видалення програмного забезпечення також застосовані групові політики. Після видалення з машини користувача має дві опції: видалити на всіх ПК, де воно було встановлено, або залишити на тих, де воно вже присутнє, і не розгортати на нових. Після підтвердження видалення програмне забезпечення Microsoft Teams було успішно видалено з клієнтського ПК, відповідно до вибраної опції.

Висновки

Було розглянуто процес створення та налаштування інфраструктури віртуалізації та автоматизованого розгортання ОС і ПЗ за допомогою VMware Workstation, WDS, MDT та групових політик Active Directory. Більшість інструментів встановлюються через Server Manager у Windows Server 2022. Після налаштування серверних ролей, таких як Active Directory, DNS та WDS, за допомогою MDT було автоматизовано розгортання ОС і ПЗ на клієнтські машини. Також налаштовано віддалене управління (RDP, msra) та мережевий фаєрвол. Додаткові програми, такі як Microsoft Teams, розгорталися через групові політики, що створило повністю автоматизовану систему управління інфраструктурою у корпоративному середовищі. Система може бути модифікована для розширення можливостей керування клієнтськими системами.