Міністерство освіти і науки України

АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ТА СИСТЕМ

Методичні вказівки до лабораторних робіт
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Комп'ютерна інженерія»
галузь знані 12 (F) Інформаційні технології
спеціальності 123 (F7) Комп'ютерна інженерія
денної та заочної форм навчання

Луцьк 2025

УДК 004.01(07)
А31

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № ____ від «____ « _____ 20 25 року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № _____ від « ____ « _____ 20 25 року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

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

Рецензент: _____ Олександр РЕШЕТИЛО, кандидат технічних наук, доцент кафедри автоматизації та комп'ютерно-інтегрованих технологій ЛНТУ

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

А31 Адміністрування комп'ютерних мереж та систем: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 (F) Інформаційні технології спеціальності 123 (F7) Комп'ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, О. Л. Кайдик, К. Я. Бортник. Луцьк: ЛНТУ, 2025. 144 с.

Методичне видання до лабораторних робіт з дисципліни «Адміністрування комп'ютерних мереж та систем» складено відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 123 Комп'ютерна інженерія освітньої програми «Комп'ютерна інженерія».

ЗМІСТ

ВСТУП

Розвиток інформаційних технологій характеризується швидким зростанням потреби у висококваліфікованих фахівцях, здатних забезпечувати ефективне функціонування комп'ютерних мереж та систем. Розвиток цифрової економіки, зростання обсягів даних та ускладнення інфраструктури призводять до підвищення вимог до адміністрування інформаційних ресурсів. У цих умовах особливої актуальності набуває підготовка майбутніх інженерів, які володіють практичними навичками налаштування, підтримки та захисту мережевих технологій.

Метою виконання лабораторних робіт є закріплення теоретичних знань та набуття практичних навичок з адміністрування комп'ютерних мереж і систем, а також застосування їх для розв'язання прикладних завдань, пов'язаних із проєктуванням, налаштуванням і захистом мережевої інфраструктури. У процесі роботи здобувачі вищої освіти повинні опановувати сучасні інструменти та технології, працювати з інструктивними матеріалами, офіційною документацією та спеціалізованим програмним забезпеченням, знаходити алгоритми виконання технічних завдань і застосовувати їх на практиці.

Для виконання лабораторних робіт використовується віртуальне середовище, інтерфейс командного рядка, мережеві сервіси Windows Server і Linux, а також утиліти для аналізу та діагностики трафіку. Виконання робіт спрямоване на всебічне формування прикладних компетентностей у сфері комп'ютерної інженерії, які є необхідною складовою підготовки майбутніх фахівців.

Виконуючи лабораторні роботи, студенти отримують практичний досвід роботи з IPv4- та IPv6-адресацією, освоять принципи побудови та сегментації мереж, вивчають основи функціонування мережевих протоколів і служб, засвоюють методи адміністрування серверних ролей, налаштування групових політик, організації віддаленого доступу, створення та підтримки веб- і FTP-серверів. Особлива увага приділяється питанням інформаційної безпеки, включаючи використання засобів моніторингу, аудитів та протидії загрозам.

Виконання лабораторних робіт сприяє розвитку навичок аналізу мережевих подій, пошуку та усунення несправностей, правильного документування результатів налаштувань і прийняття обґрунтованих інженерних рішень. Крім того, студенти формують уміння працювати з технічною документацією, застосовувати стандарти й протоколи у практичних умовах, оцінювати ефективність та безпеку мережевих рішень.

Всі студенти обов'язково авторизуються на платформі https://www.netacad.com та реєструються на курси CCNA. Курс «Вступ до мереж» на платформі https://www.netacad.com.

Таким чином, методичні вказівки забезпечують практичну складову підготовки здобувачів вищої освіти за спеціальністю «Комп'ютерна інженерія» та створюють основу для формування професійних компетентностей, необхідних у сфері адміністрування комп'ютерних мереж та систем.

Лабораторна робота №1
Обчислення підмереж IPv4

Мета роботи: закріплення знань щодо визначення IP-адреси мережі на основі заданої IP-адреси та маски підмережі.

Хід роботи

Заповніть наведені нижче таблиці відповідями про задану IPv4-адресу вузла, вихідну та нову маски підмережі [1-7].

Завдання 1.

Дано:	
IP-адреса вузла:	192.168.21.156
Вихідна маска підмережі:	255.255.255.0
Нова маска підмережі:	255.255.255.224
Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 2.

Дано:	
IP-адреса вузла:	10.11.82.147
Вихідна маска підмережі:	255.0.0.0
Нова маска підмережі:	255.255.128.0
Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 3.

Дано:	
IP-адреса вузла:	172.22.67.24
Вихідна маска підмережі:	255.255.0.0
Нова маска підмережі:	255.255.224.0
Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 4.

Дано:	
IP-адреса вузла:	192.168.7.38
Вихідна маска підмережі:	255.255.255.0
Нова маска підмережі:	255.255.255.252
Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 5.

Дано:	
IP-адреса вузла:	132.125.9.75
Вихідна маска підмережі:	255.255.0.0
Нова маска підмережі:	255.255.255.0

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 6.

Дано:	
IP-адреса вузла:	192.144.123.137
Вихідна маска підмережі:	255.255.255.0
Нова маска підмережі:	255.255.255.248
Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Дайте відповідь на запитання. Дайте характеристику маски підмережі. Чому маска підмережі так важлива при аналізі IPv4-адреси? [1-3, 5-7].

Лабораторна робота №2
Використання Wireshark для перегляду мережного трафіку

Мета роботи: навчитися аналізувати трафік, використовуючи програмний аналізатор протоколів (або програма «пакетний сніфер») Wireshark.

Теоретичні відомості

В даному завданні потрібнопПерехопити та проаналізувати локальні та віддалені ICMP-дані за допомогою Wireshark (рис. 2.1) [1].

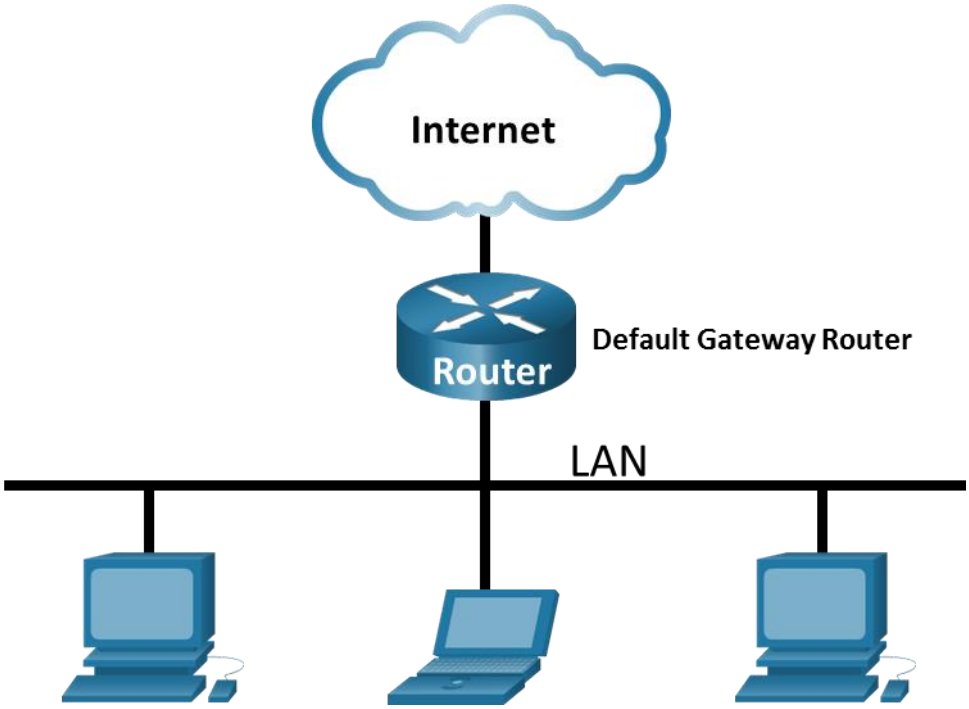

Рисунок 2.1 – Топологія мережі

Wireshark − це програмний аналізатор протоколів або програма «пакетний сніфер», яка використовується для пошуку та усунення несправностей мережі, аналізу повідомлень, розробки програм та протоколів, а також для навчання. Під час передачі даних через мережу, сніфер «захоплює» кожен протокольний блок даних (PDU) і може декодувати та аналізувати його вміст згідно з відповідними RFC або іншими специфікаціями. Wireshark є корисним інструментом для всіх, хто працює з мережами. У цій лабораторній роботі Ви будете використовувати Wireshark для перехоплення IP-адрес з ICMP-повідомлення та MAC-адрес з Ethernet-кадра.

Необхідні ресурси: 1 ПК з ОС Windows та доступом до мережі Інтернет. Додаткові ПК в локальній мережі будуть використовуватись для відповідей на ping-запити.

Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark. У даній лабораторній роботі потрібно перевірити зв’язок з іншим ПК в локальній мережі за допомогою команди ping та перехопити згенеровані ICMP-запити та ICMP-відповіді, використовуючи Wireshark. Також розглянути вміст перехоплених кадрів для отримання певної інформації. Цей аналіз має

допомогти з’ясувати, як заголовки повідомлень використовуються для транспортування даних до місця призначення.

Хід роботи

1. Визначення адрес мережної плати ПК:

– відкрити вікно командного рядка Windows;

– у командному рядку ввести команду ipconfig /all, щоб переглянути IP-адресу, MAC-адресу, опис мережної плати ПК (рис. 2.2).

```
C:\Users\Student> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

Рисунок 2.2 – Перегляд IP-адреси, MAC-адреси та опис мережної плати ПК

Примітка. Запитайте члена або членів команди про IP-адресу їх ПК та надайте їм IP-адресу свого ПК. На цьому етапі не повідомляйте їм свою MAC-адресу.

2. Запуск Wireshark і початок перехоплення даних.

Перейдіть до Wireshark. Двічі натисніть на потрібному інтерфейсі, щоб розпочати перехоплення повідомлень. Переконайтеся, що на потрібний інтерфейс надходить трафік. У верхній частині вікна Wireshark рядки даних почнуть прокручуватися донизу. Рядки даних, залежно від протоколу, матимуть різне забарвлення. Вони можуть прокручуватися дуже швидко. Швидкість залежатиме від інтенсивності спілкування, яке зараз відбувається між Вашим ПК та іншими вузлами локальної мережі. Для полегшення перегляду даних, які перехоплює Wireshark, та подальшого їх опрацювання можна застосувати фільтри.

У цій лабораторній роботі нас цікавить відображення лише повідомлень протоколу ICMP (ping). Наберіть icmp у полі Filter у верхній частині вікна Wireshark і натисніть або Enter, або кнопку Apply (значок стрілочки), щоб переглядати тільки ICMP-повідомлення. Як наслідок застосування цього фільтру всі дані у верхній частині вікна зникнуть, але процес перехоплення

трафіку на мережній платі/інтерфейсі продовжується. Перейдіть до вікна командного рядка та пропінгуйте IP-адресу, надану членом Вашої команди (рис. 2.3).

C:\> ping 192.168.1.114

```
Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 2.3 – Пінг IP-адреси

Зверніть увагу на те, що дані знову з’являються у верхній частині вікна Wireshark (рис. 2.4).

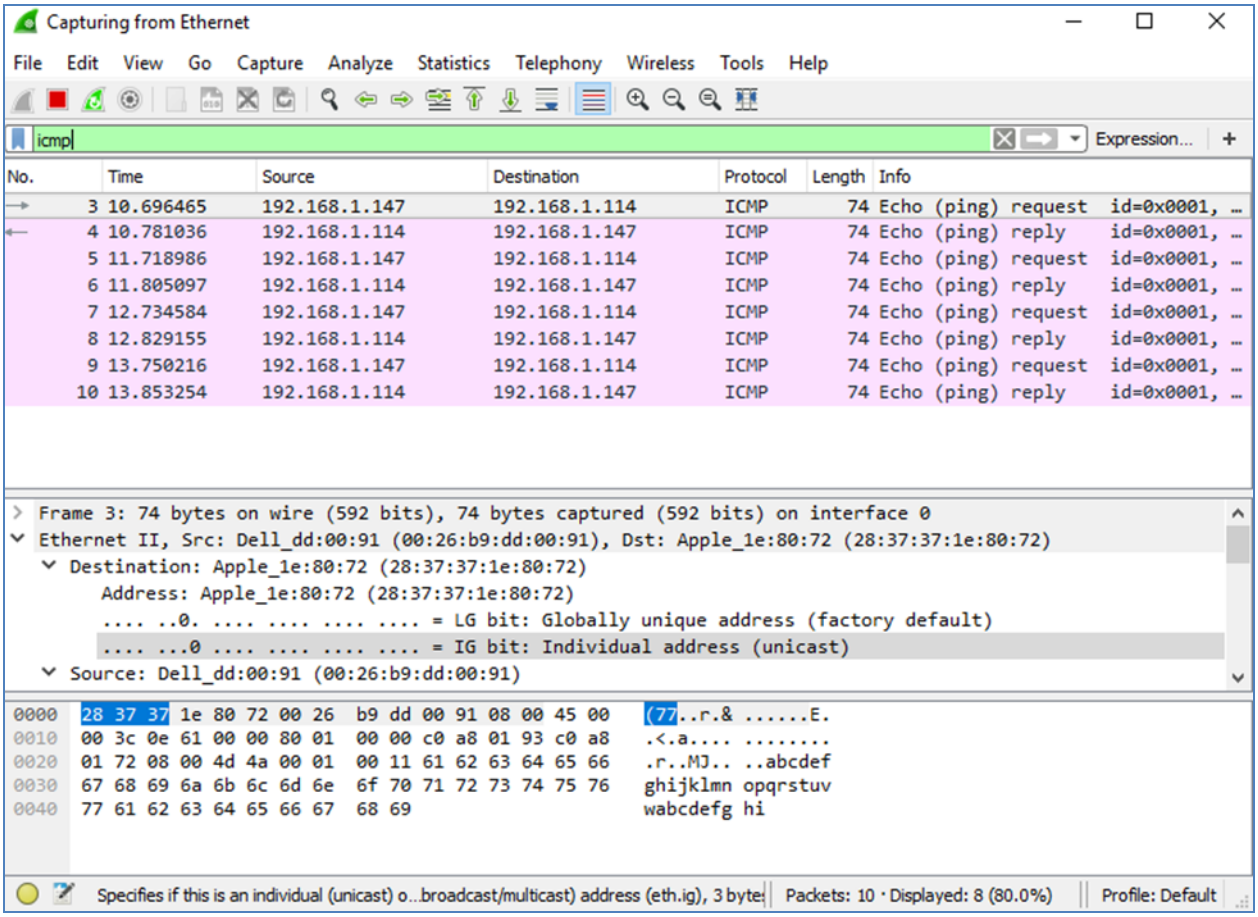

Рисунок 2.4 – Вікно Wireshark з даними

Примітка. Якщо ПК члена Вашої команди не відповідає на Ваші ping-запити, причиною може бути блокування цих запитів його міжмережним екраном (Додаток А

Дозвіл передачі ICMP-трафіку через міжмережний екран ОС Windows знайдіть і перегляньте інформацію про те, як дозволити передачу ICMP-трафіку через міжмережний екран в ОС Windows.

3. Зупиніть перехоплення даних, натиснувши значок Stop Capture.

4. Дослідження перехоплених даних.

Виконати перегляд даних, які були згенеровані ping-запитами ПК члена Вашої команди. Дані Wireshark відображаються у трьох секціях: 1) у верхній секції відображається перелік перехоплених кадрів з узагальненням даних IP-пакета; 2) у середній секції відображаються дані кадру, вибраного у верхній частині екрана і перехоплений кадр розділяється на підсекції відповідно до протокольних рівнів; 3) нижня секція відображає необроблені дані кожного рівня. Необроблені дані відображаються як у шістнадцятковій, так і у десятковій формах.

У верхній частині вікна Wireshark натисніть на кадр, що містить перший ICMP-запит. Зауважте, що стовпчик Source містить IP-адресу Вашого ПК, а стовпчик Destination містить IP-адресу ПК Вашого колеги по команді (саме того ПК, який Ви пінгували).

Якщо цей кадр все ще вибраний, перейдіть до середньої частини. Натисніть на значок стрілки ліворуч від рядка Ethernet II, щоб переглянути MAC-адреси отримувача та відправника кадру.

Дайте відповідь на питання. Чи співпадає MAC-адреса відправника з MAC-адресою мережної плати/інтерфейсу Вашого ПК? Чи відповідає у Wireshark MAC-адреса отримувача MAC-адресі ПК Вашого колеги по команді? Як Ваш ПК отримав MAC-адресу пропінгованого ПК?

Напишіть тут свою відповідь та відобразіть у звіті скріни виконання команди.

Примітка. У попередньому прикладі із перехоплення ICMP-запиту, дані протоколу ICMP інкапсулюються в IPv4-пакет (додається заголовок IPv4), який потім інкапсулюється у кадр Ethernet II (додаються заголовок та трейлер − контрольна сума Ethernet II) для передачі через локальну мережу.

5. Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark.

За допомогою команди ping потрібно перевірите зв’язок з віддаленими вузлами (вузлами, які не належать до Вашої локальної мережі) та дослідити отримані дані. Визначити чим відрізняються ці дані від даних, які досліджувалися у роботі вище:

– початок перехоплення даних на мережній платі/інтерфейсі: розпочніть перехоплення даних знову. Wireshark запропонує Вам зберегти раніше перехоплені дані перед початком іншого перехоплення. Зберігати ці дані не обов’язково. Натисніть Continue without Saving. Після активізації перехоплення у командному рядку Windows виконайте команду ping для таких URL-адрес веб-сайтів: відкрийте вікно командного рядка Windows

www.cisco.com

www.google.com

Примітка. Коли Ви пінгуєте перелічені URL-адреси, зауважте, що DNS-сервер транслює ці URL в IP-адреси. Зверніть увагу на IP-адреси,

отримані для кожної URL-адреси. Ви можете зупинити перехоплення даних, натиснувши Stop Capture.

– дослідіть та проаналізуйте дані з віддалених вузлів: перегляньте перехоплені дані в Wireshark та дослідіть IP-адреси та MAC-адреси веб-сайтів, з якими Ви перевіряли зв'язок. Запишіть IP-адреси та MAC-адреси отримувачів для веб-сайтів, з якими Ви перевіряли зв'язок.

IP-адреса для www.cisco.com:
Напишіть тут свою відповідь.
MAC-адреса для www.cisco.com:
Напишіть тут свою відповідь.
IP-адреса для www.google.com:
Напишіть тут свою відповідь.
MAC-адреса для www.google.com:
Напишіть тут свою відповідь.

Додайте ще один веб-сайт на Ваш вибір, та виконайте аналогічні кроки.

Дайте відповідь на запитання. Що важливе в цій інформації? Чим ця інформація відрізняється від інформації, яку Ви отримали в роботі вище? Напишіть тут свою відповідь.

Питання для самоперевірки

Чому Wireshark показує реальні MAC-адреси вузлів локальної мережі, але не показує реальні MAC-адреси вузлів віддалених мереж? Напишіть тут свою відповідь.

Додаток А

Дозвіл передачі ICMP-трафіку через міжмережний екран ОС Windows

Якщо члени Вашої команди не можуть виконати ping-запити до Вашого ПК, ймовірно саме міжмережний екран блокує ці запити. У цьому додатку наведено опис створення правила на міжмережному екрані, яке дозволяє виконання ping-запитів. Також наведено опис відключення створеного ICMP-правила після завершення виконання лабораторної роботи.

Створення нового вхідного правила, яке дозволить ICMP-трафіку пройти через міжмережний екран:

– перейдіть до Control Panel і натисніть опцію System and Security в Category view;

– у вікні System and Security, натисніть Windows Defender Firewall або Windows Firewall;

– на лівій панелі Windows Defender Firewall або вікна Windows Firewall натисніть Advanced settings;

– у вікні Advanced Security на лівій бічній панелі виберіть опцію Inbound Rules і потім натисніть New Rule… на правій бічній панелі;

– запустіть New Inbound Rule Wizard. У вікні Rule Type спочатку натисніть кнопку Custom, а потім – кнопку Next;

– на лівій панелі вікна виберіть параметр Protocol and Ports і, використовуючи спадне меню Protocol Type, виберіть ICMPv4, а потім натисніть Next;

– переконайтесь, що як для локальних так і для віддалених адрес вибрано Any IP address. Натисніть Next, щоб продовжити;

– виберіть Allow the connection. Натисніть Next, щоб продовжити;

– за замовчуванням це правило застосовується для всіх профілів ОС. Натисніть Next, щоб продовжити;
– задайте назву правила Allow ICMP Requests. Натисніть Finish щоб завершити. Це нове правило дозволить членам Вашої команди отримувати від Вашого ПК відповіді на їх ping-запити.

Вимкнення або видалення ICMP-правила.

Після завершення лабораторної роботи можна вимкнути або навіть видалити створене правило. Для вимкнення правила використовуйте параметр Disable Rule, це дозволить пізніше увімкнути правило знову. Видалення правила повністю видаляє його зі списку вхідних правил.

У вікні Advanced Security натисніть Inbound Rules на лівій бічній панелі та знайдіть правило, створене Вами раніше.

Правою кнопкою миші виберіть ICMP-правило і виберіть Disable Rule, якщо Ви вирішили його відключити. Ви також можете вибрати Delete, якщо Ви вирішили видалити правило назавжди. Якщо Ви вибрали цей варіант, то потім доведеться знову створювати правило, якщо буде потрібно дозволити надсилати ICMP-відповіді.

Лабораторна робота №3
Налаштування Windows Server 2025 у віртуальному середовищі

Мета роботи: ознайомитися з процесом розгортання операційної системи Windows Server 2025 у віртуальному середовищі, навчитися виконувати базові налаштування сервера, зокрема мережевих параметрів, системного часу, віддаленого доступу, ролей та компонентів, а також опанувати механізми резервного копіювання та аналізу системних журналів для забезпечення стабільної та безпечної роботи серверної інфраструктури [7-14].

Хід роботи

Завдання1. Розгортання Windows Server 2025 у віртуальній машині

Для розгортання Windows Server 2025 заходимо в середовище Hyper-V, оскільки воно найкраще підходить для встановлення даної ОС на віртуальну машину (рис. 3.1).

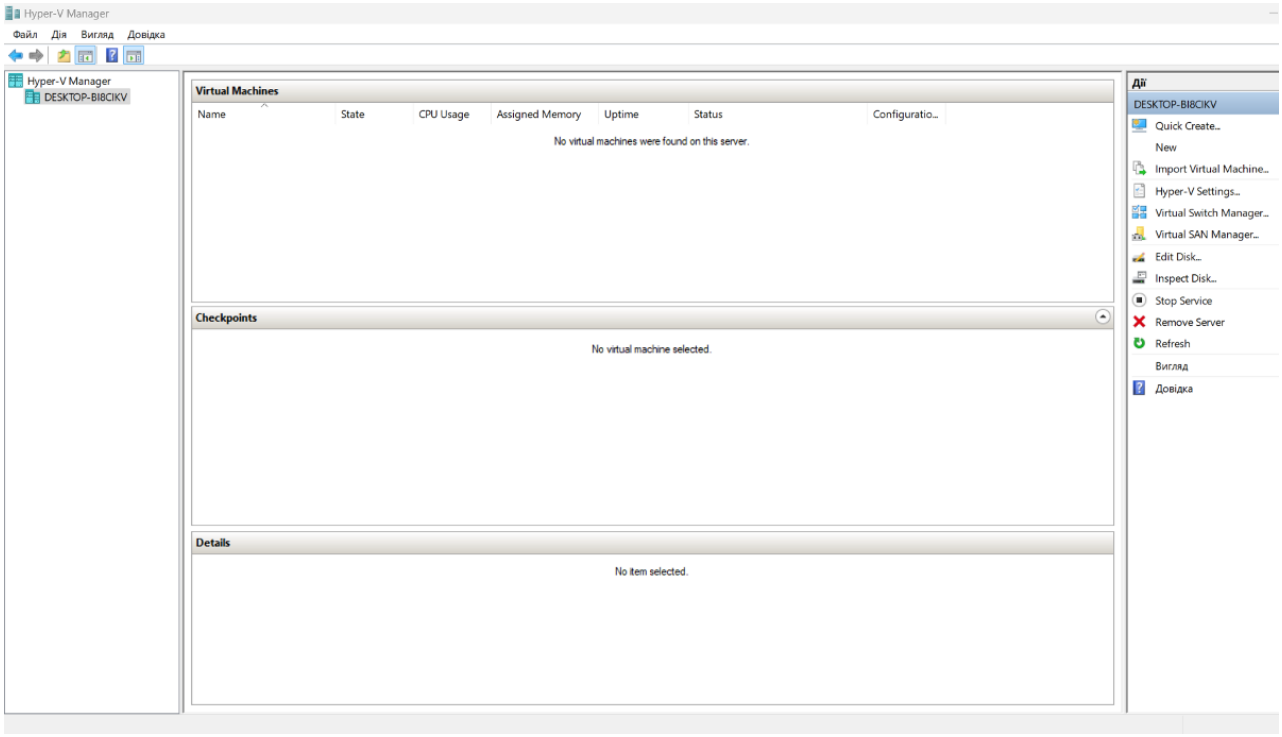

Рисунок 3.1 – Вікно Hyper-V

Після цього натиснути на назву комп’ютера – «New» – «Virtual Machine» (рис. 3.2).

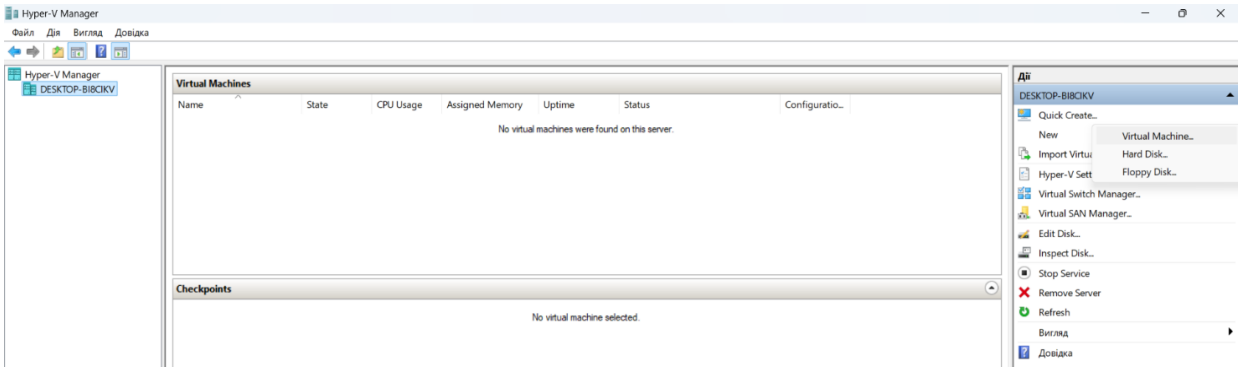

Рисунок 3.2 – Створення нової віртуальної машини для ВС25

Внаслідок цих дій відкривається майстер створення нової віртуальної машини. В першій вкладці (вступній) натискаємо «Next» (рис. 3.3).

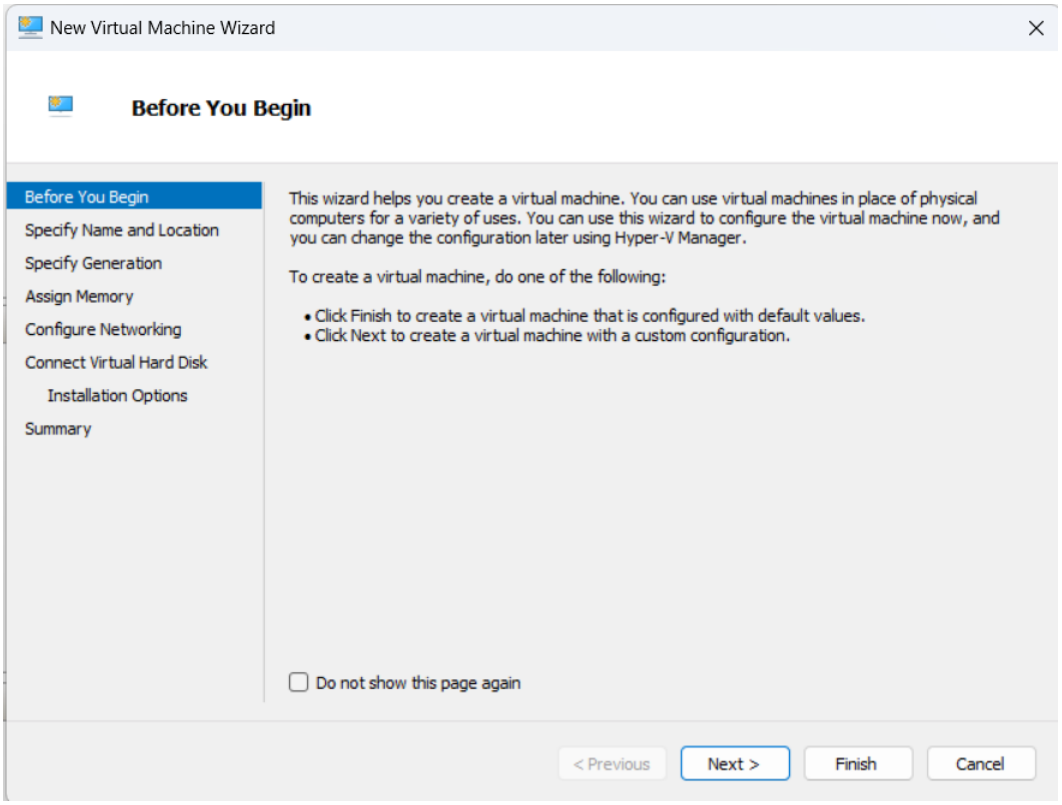

Рисунок 3.3 – Вітальне вікно майстра створення нової віртуальної машини

В наступній вкладці надати ім’я новій віртуальній машині та обирати місце зберігання для її файлів (рис. 3.4).

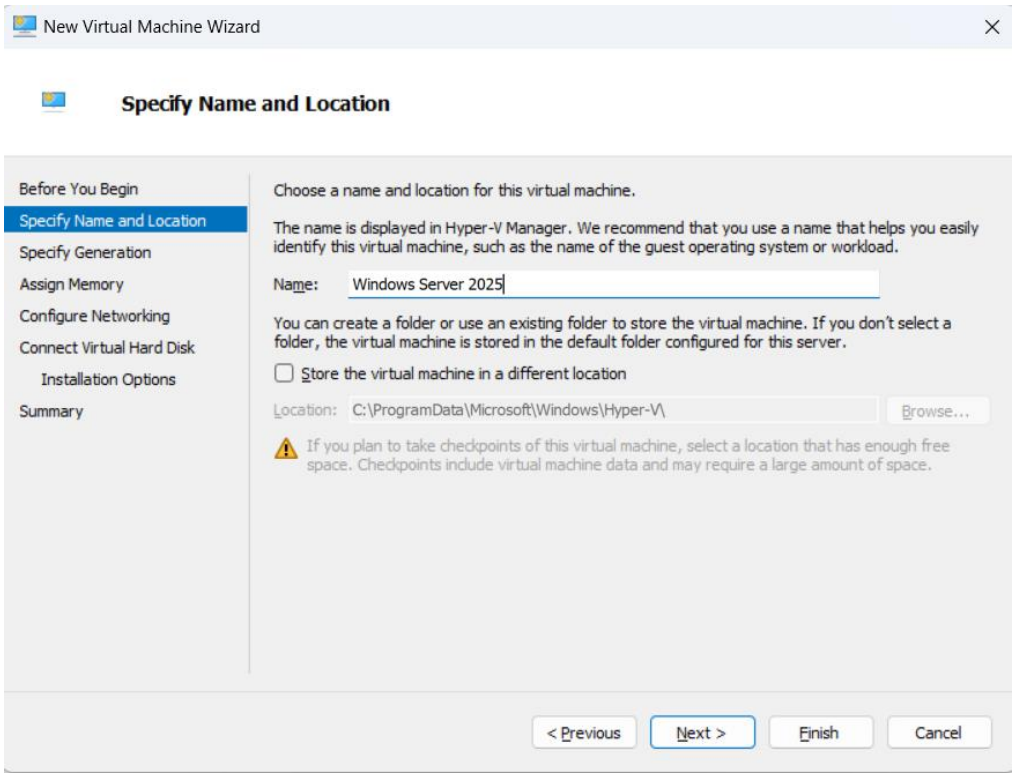

Рисунок 3.4 – Надання імені новій ВМ та вибір місця для зберігання її файлів

Далі обирається специфікація покоління ВМ – «Generation 2» і знову тиснути «Next» (рис. 3.5).

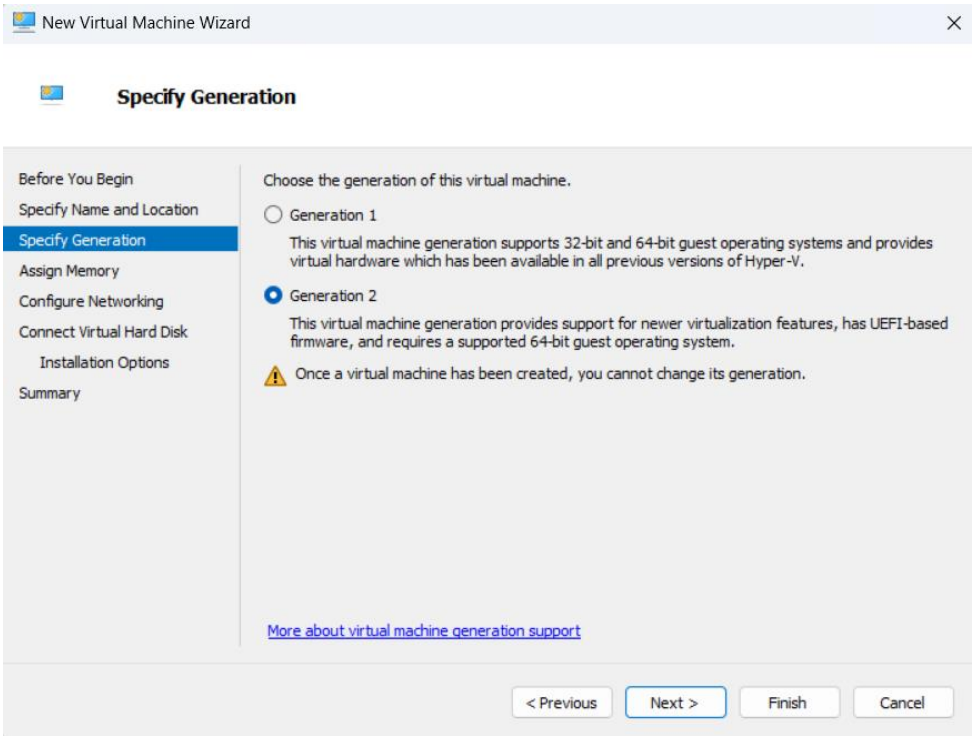

Рисунок 3.5 – Вибір «покоління» для ВМ, що створюється

Після цього вказати розмір оперативної пам’яті, що виділяється для нової ВМ та тиснути «Next». Мінімальний обсяг – 2048 МБ, інакше можлива некоректна робота ОС (рис. 3.6).

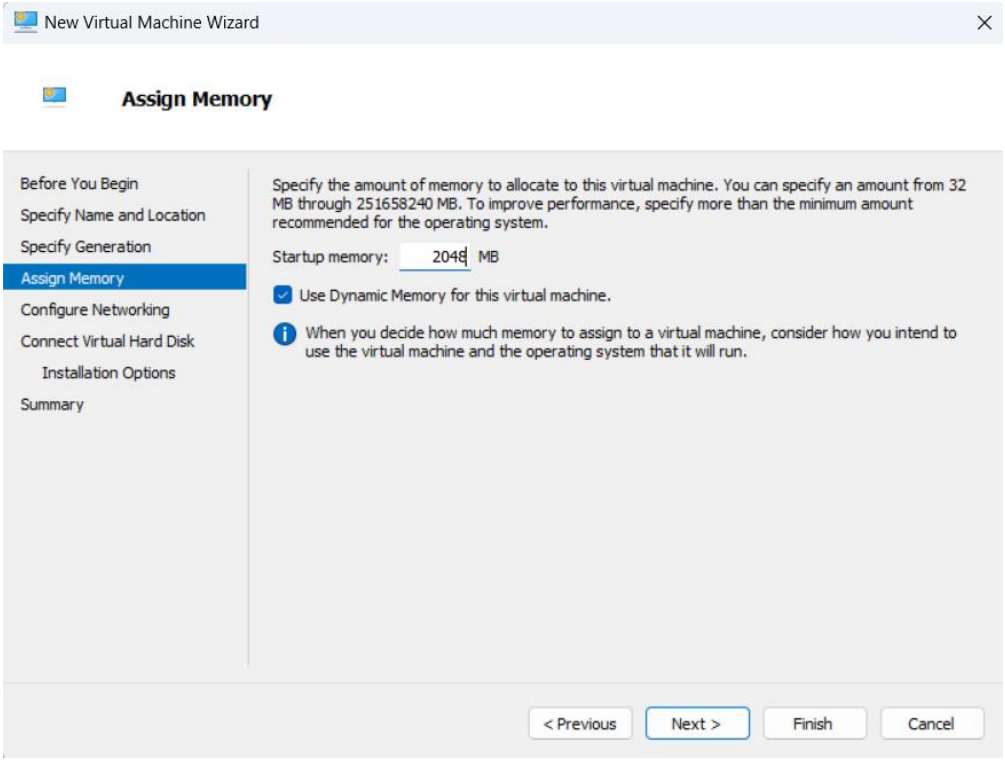

Рисунок 3.6 – Вибір розміру оперативної пам’яті для нової ВМ (вказано мінімальний потрібний об’єм)

Потім провести мережеві налаштування та в полі «Connection» обирати «Default Switch» і знову натиснути «Next» (рис. 3.7).

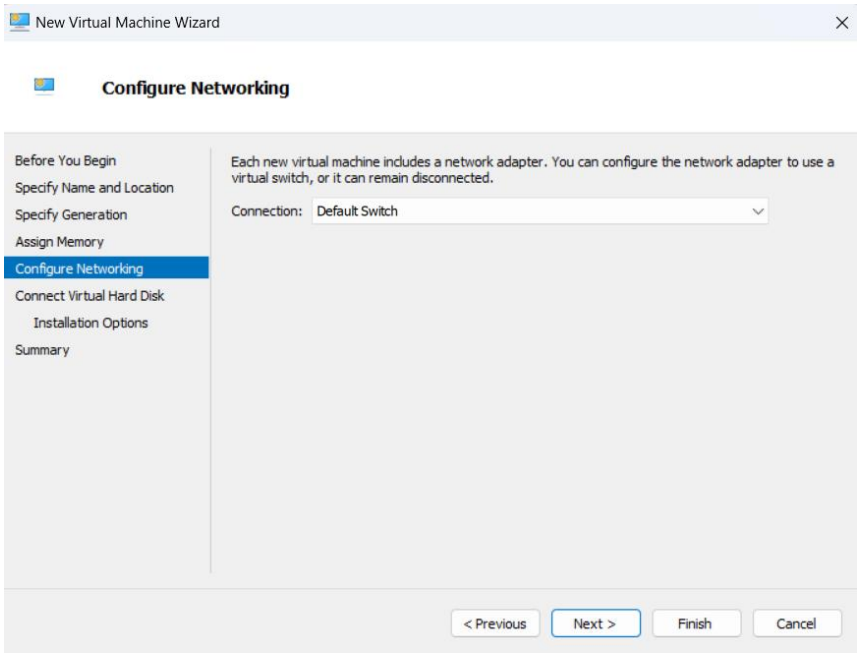

Рисунок 3.7 – Мережеві налаштування

Далі створити віртуальний жорсткий диск та вказати місце його зберігання і обсяг та натиснути «Next». Мінімальний обсяг – 30 ГБ (рис. 3.8).

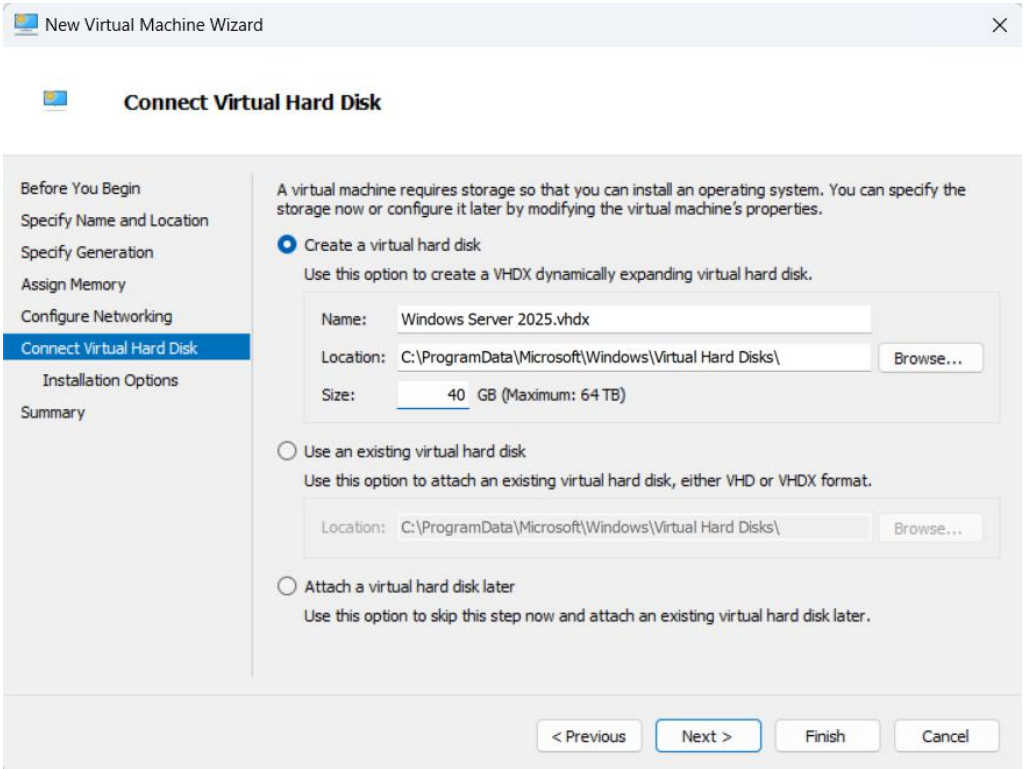

Рисунок 3.8 – Створення віртуального жорсткого диска для ВМ та місця його зберігання на фізичному комп’ютері

Згодом обирати джерело встановлення ОС – завантажений попередньо ISO образ Windows Server 2025 та натиснути «Next» (рис. 3.9).

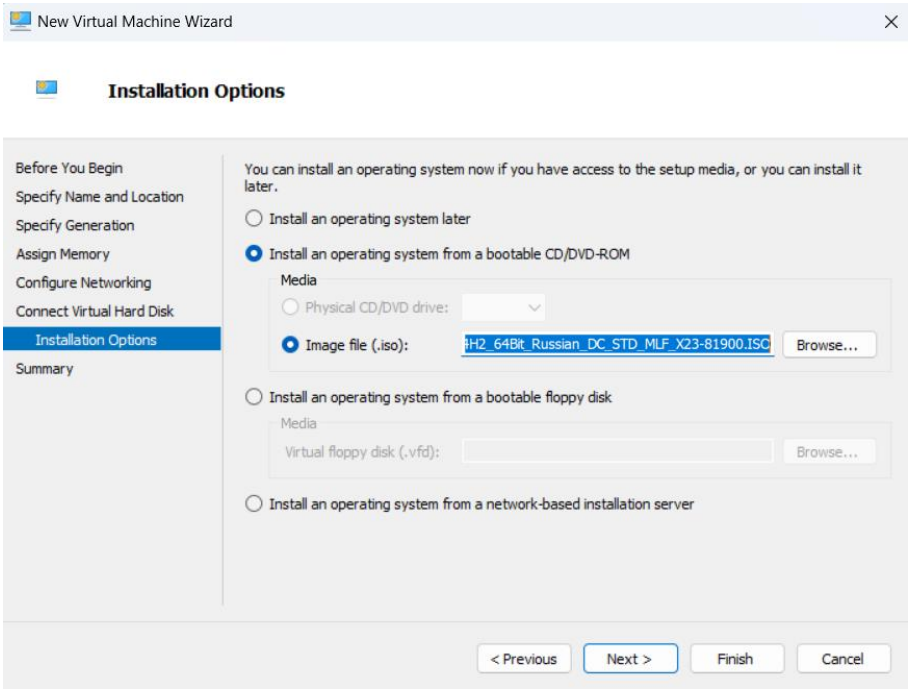

Рисунок 3.9 – Налаштування встановлення ОС – вибір джерела встановлення (ISO образ)

В останній вкладці перевірити проведені налаштування та натиснути «Finish» (рис. 3.10).

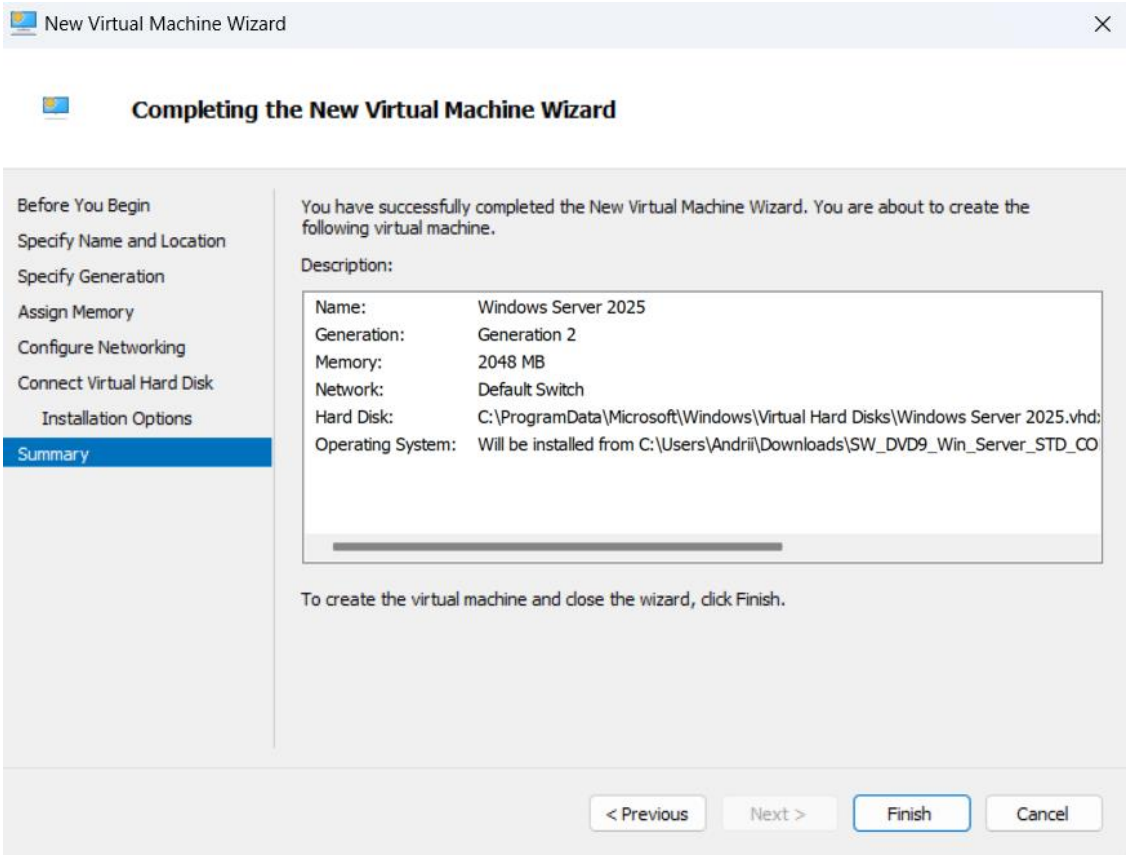

Рисунок 3.10 – Підсумки проведених налаштувань створюваної віртуальної машини

В результаті нова віртуальна машина для розгортання на ній Windows Server 2025 створена та відображається в Hyper-V Manager (рис. 3.11).

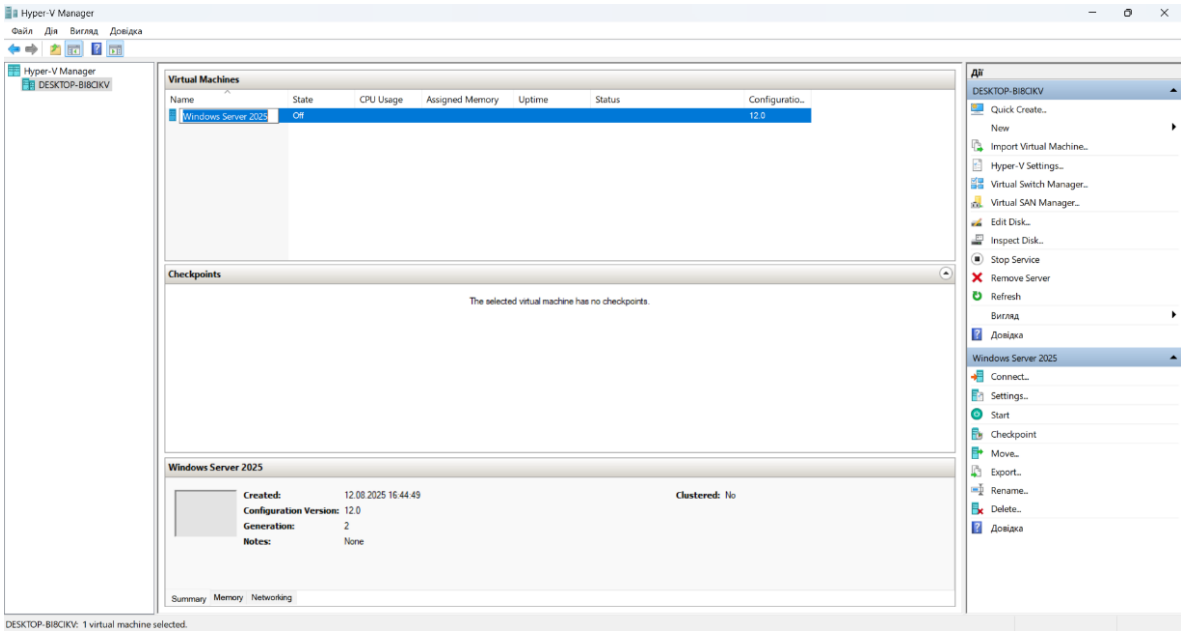

Рисунок 3.11 – Створена віртуальна машина для Windows Server 2025

Щоб її запустити у вікні Hyper-V Manager натиснути на назву цієї ВМ та справа в меню «Дії» перейти «Connect…». Як наслідок, запуститься створена віртуальна машина Windows Server 2025 (рис. 3.12-3.13).

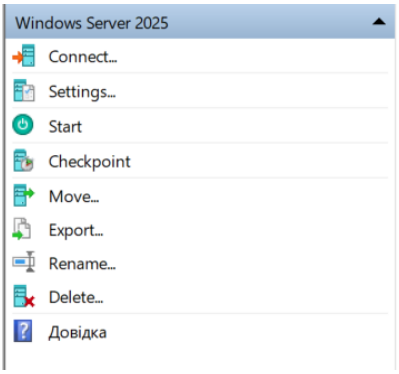

Рисунок 3.12 – Меню роботи зі створеною ВМ у середовищі Hyper-V

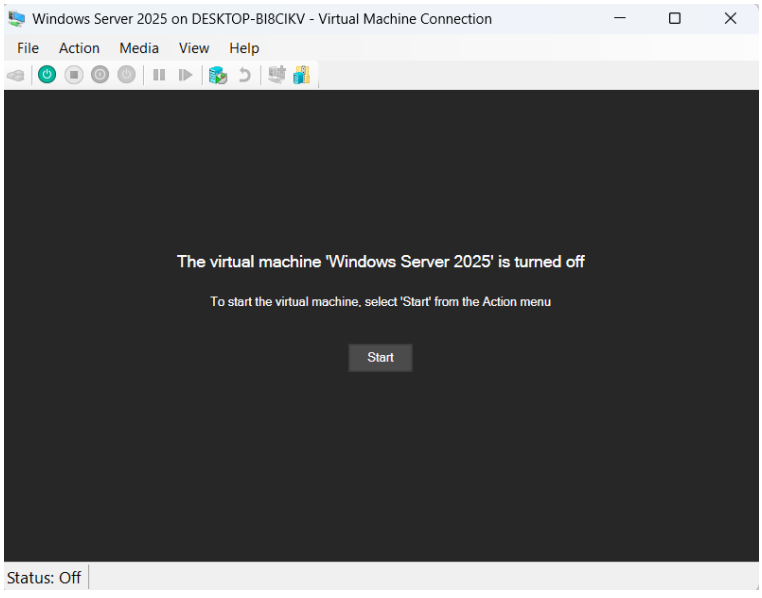

Рисунок 3.13 – Запуск ВМ

Для підтвердження необхідно натиснути будь-яку клавішу, але щоб це стало можливим, слід у верхньому меню вибрати розділ «Action» і у списку, що відкрився вибрати «Ctrl+Alt+Delete». Це потрібно, щоб відбулося «захоплення» клавіатури і миші віртуальною машиною (рис. 3.14).

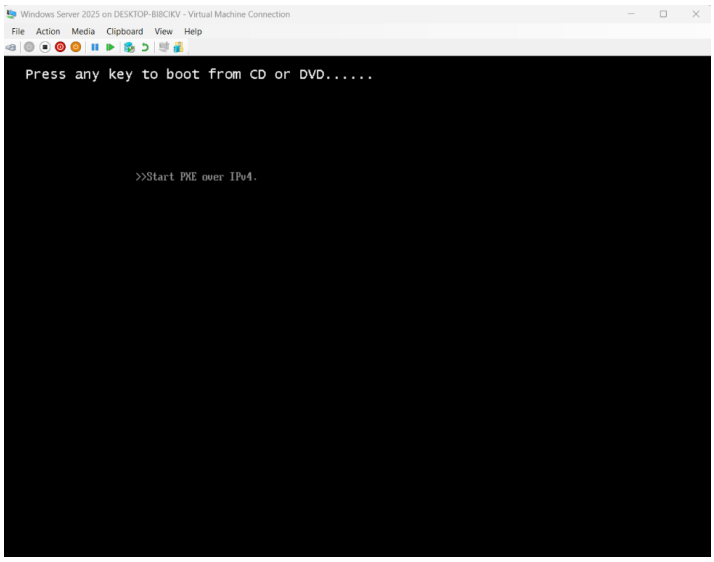

Рисунок 3.14 – Вікно підтвердження вивантаження образу ОС на ВМ

Після цього автоматично починається процес встановлення операційної системи на віртуальний комп’ютер. На першій вкладці налаштування встановлення вибрати мовні параметри та натиснути «Далі» (рис. 3.15).

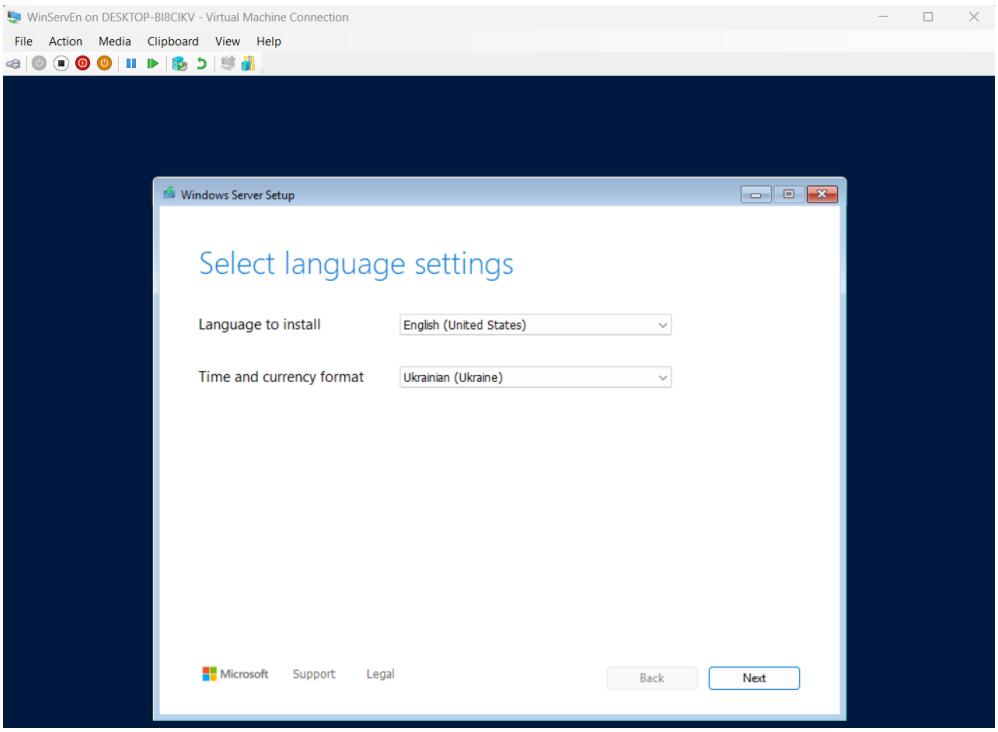

Рисунок 3.15 – Вибір мовних параметрів для встановлюваної ОС

Згодом налаштувати параметри клавіатури, вони автоматично виставляються, відповідно до обраних мовних параметрів, потім натиснути «Далі» (рис. 3.16).

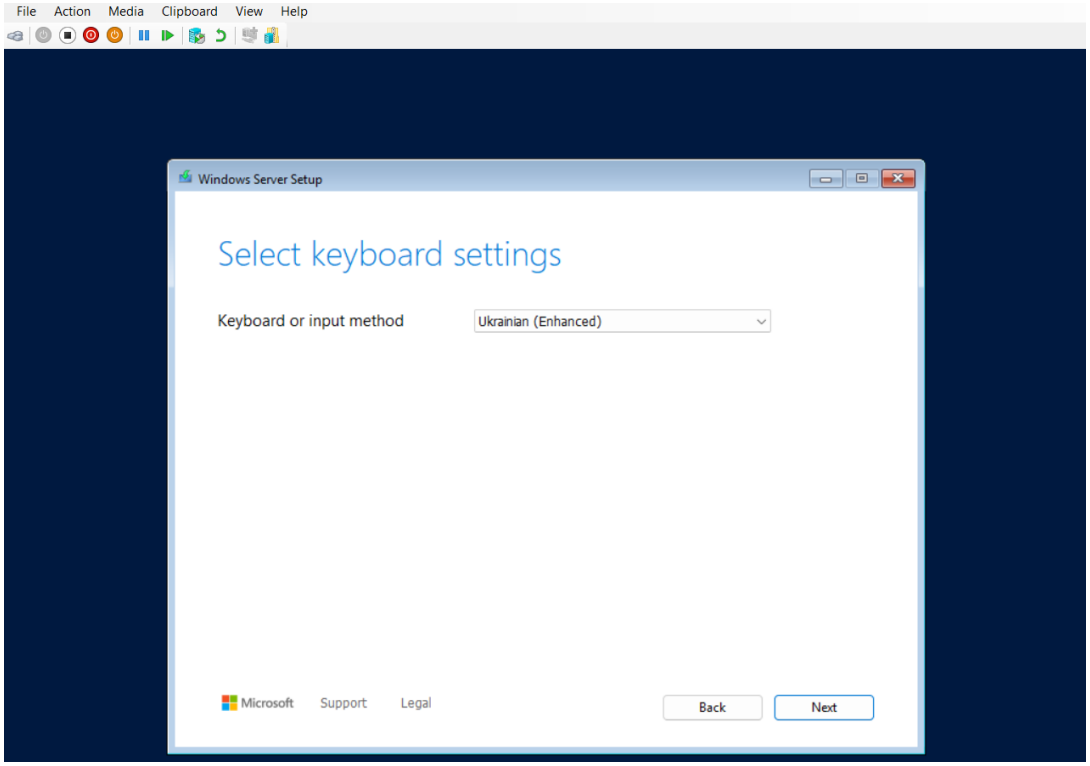

Рисунок 3.16 – Вибір параметрів клавіатури

Далі вибирати варіант встановлення – «Встановити Windows Server 2025», погодитись з тим, що все, що до цього було на комп'ютері буде видалено та натиснути «Далі» (рис. 3.17).

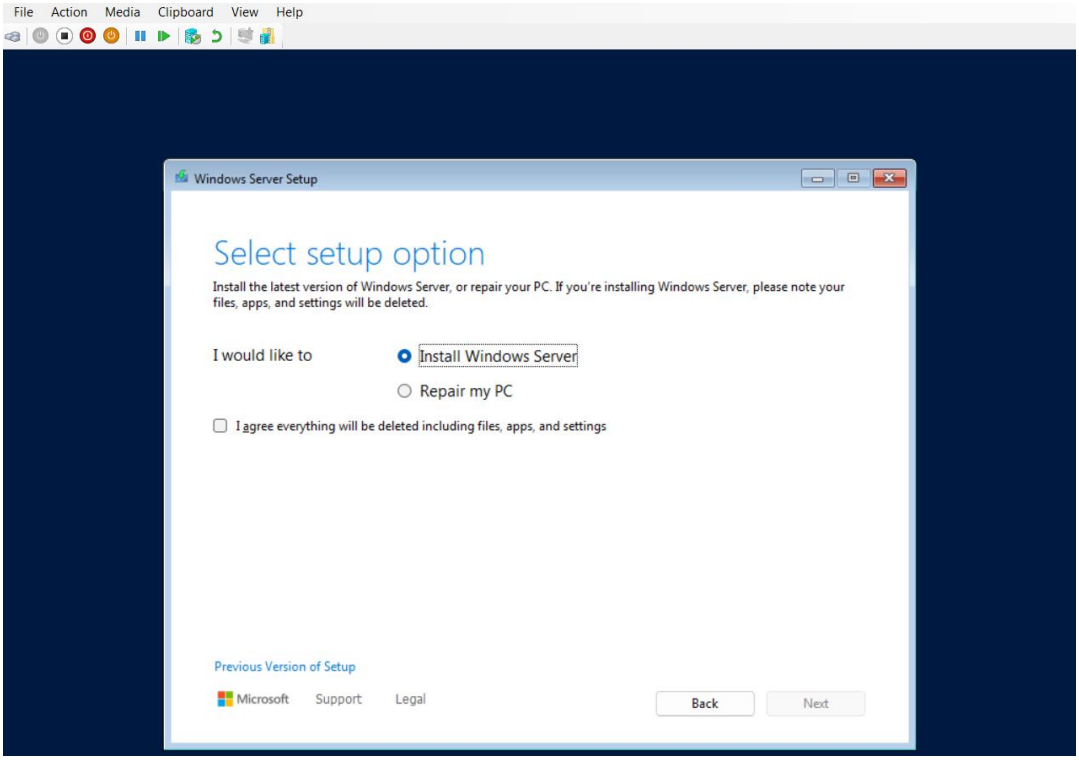

Рисунок 3.17 – Вибір варіанту встановлення Windows Server 2025

Потім вибирати тип операційної системи Windows Server 2025, що буде встановлено. Оскільки нам потрібний Windows Server в графічному варіанті, то

обрати Windows Server 2025 Standard (можливості робочого столу) – «Далі» (рис. 3.18).

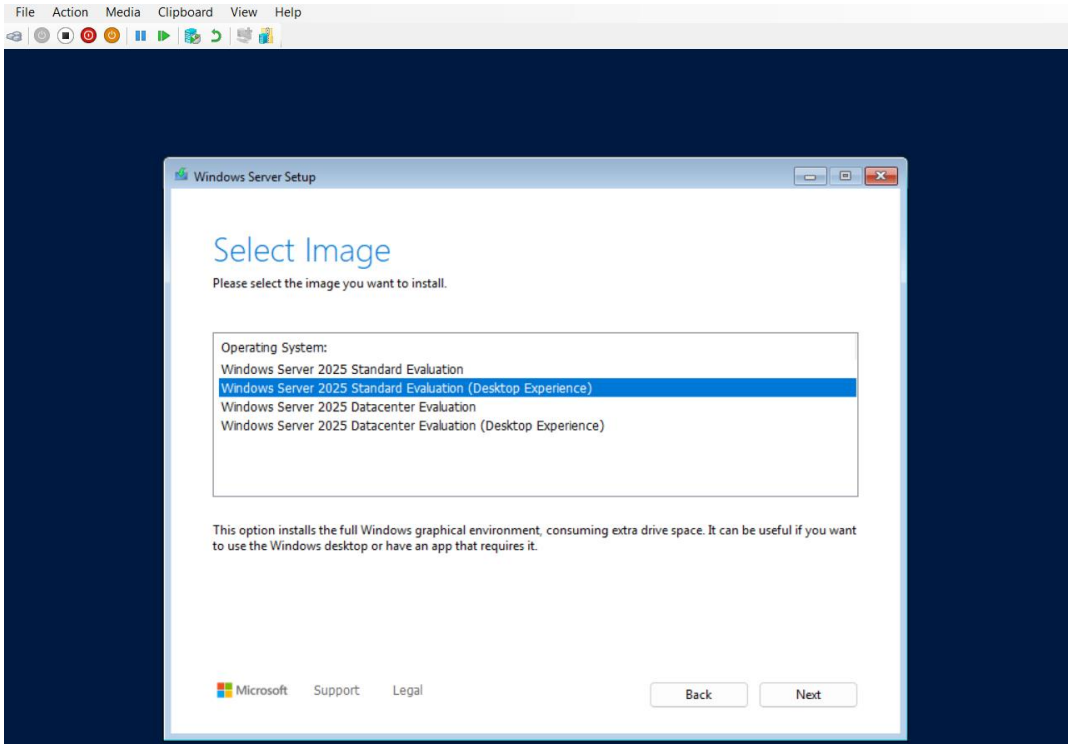

Рисунок 3.18 – Вибір типу ОС Windows Server 2025, який потрібно встановити

Після цього прийняти умови ліцензії та натиснути «Далі» (рис. 3.19).

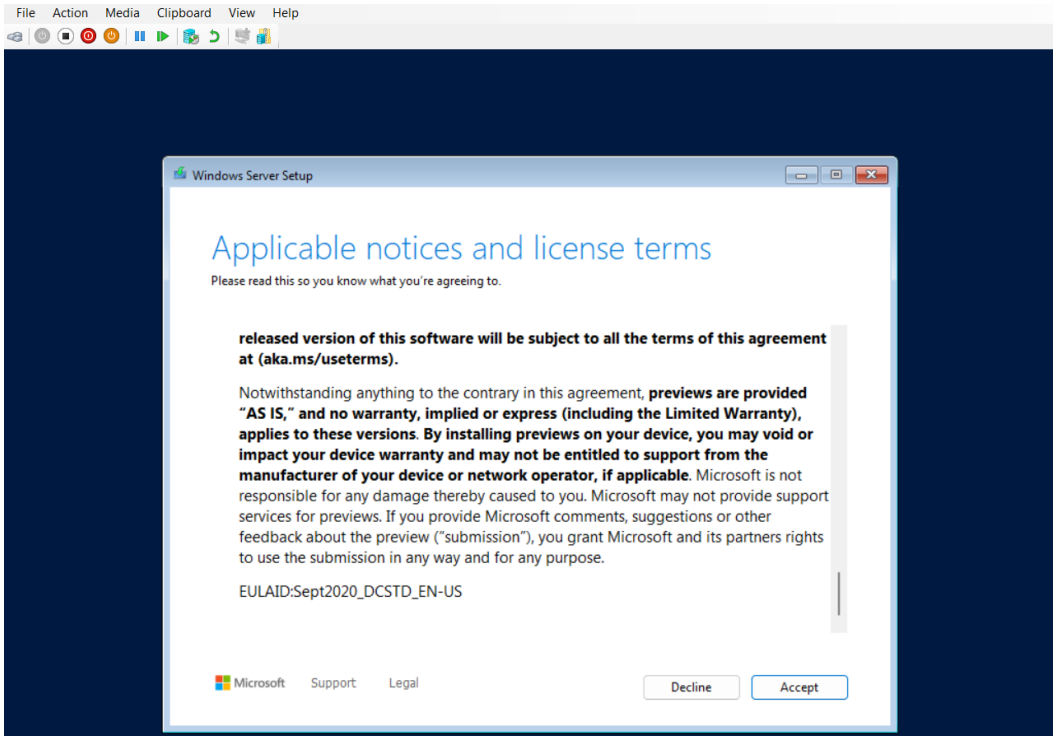

Рисунок 3.19 – Прийняття умов ліцензії

Далі вибрати розташування для встановлення ОС та натиснути «Далі» (рис. 3.20).

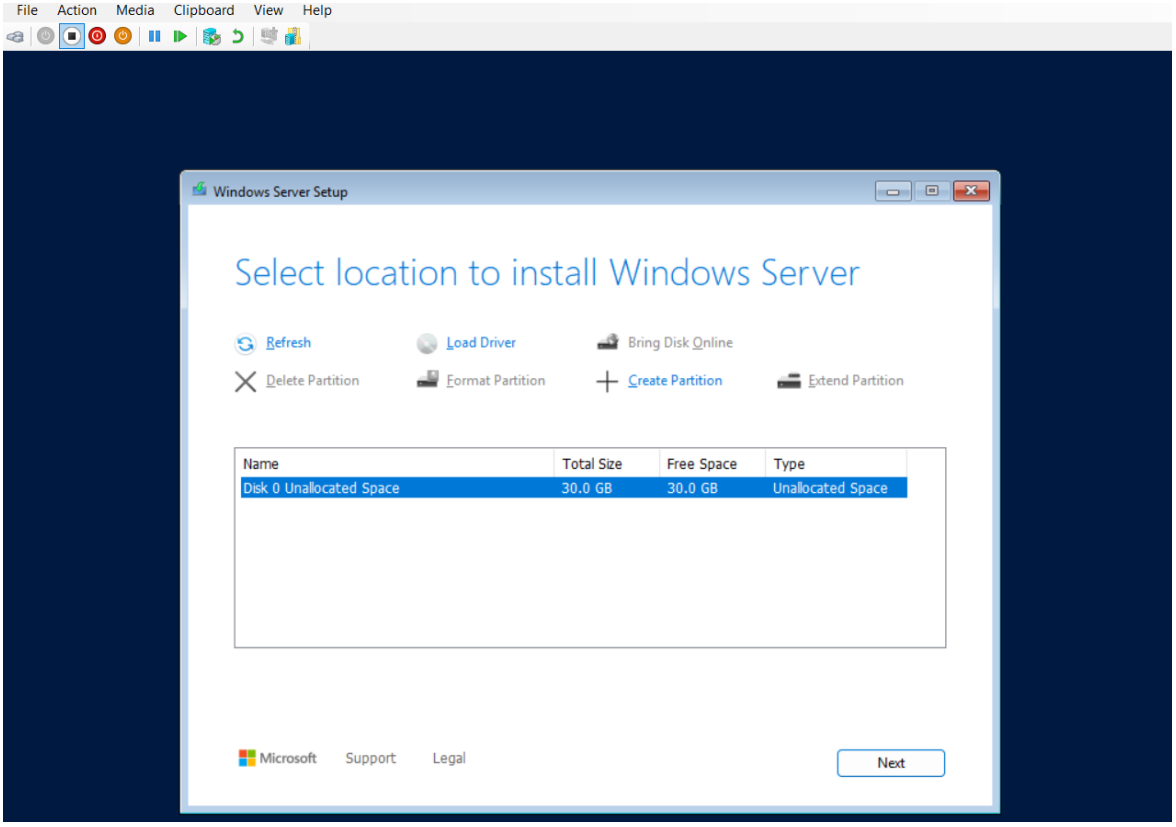

Рисунок 3.20 – Вибір місця (диска) для встановлення ОС

Після цього натиснути «Встановити». Розпочинається процес інсталяції операційної системи на комп’ютер (рис. 3.21-3.22).

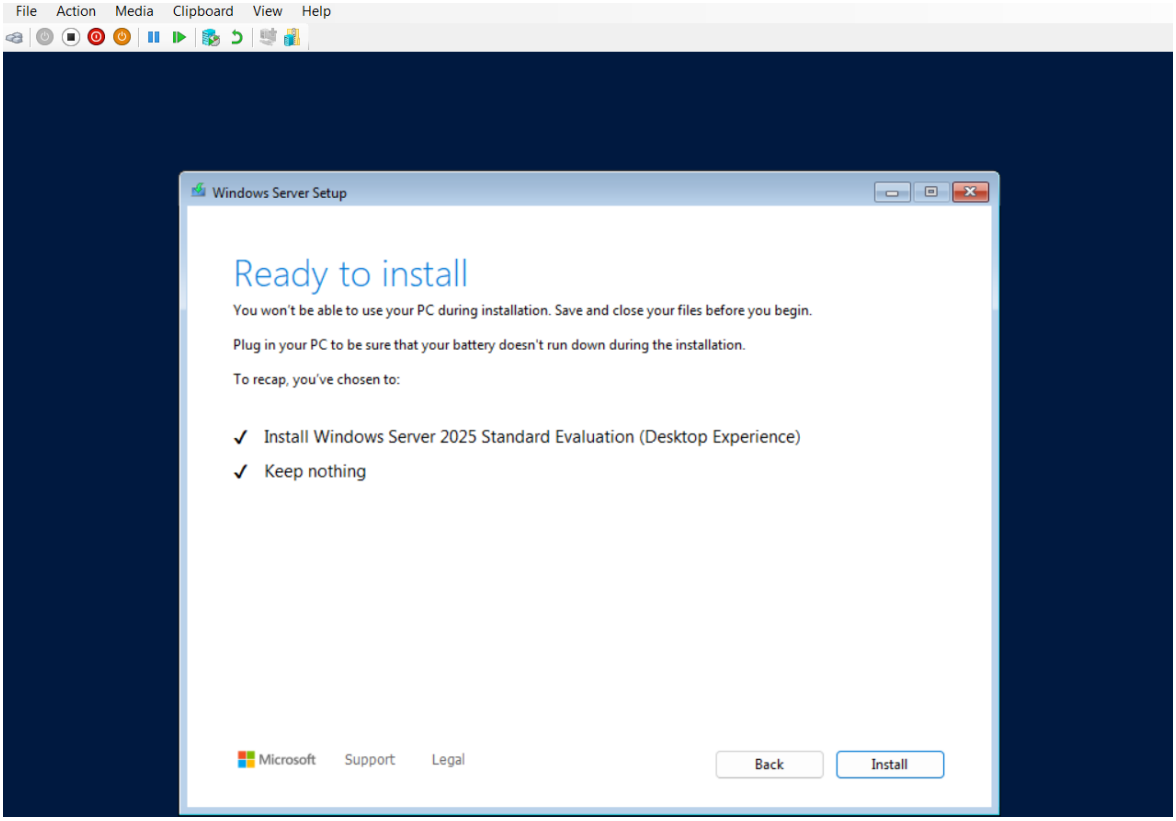

Рисунок 3.21 – Фінальне вікно підтвердження встановлення Windows Server 2025

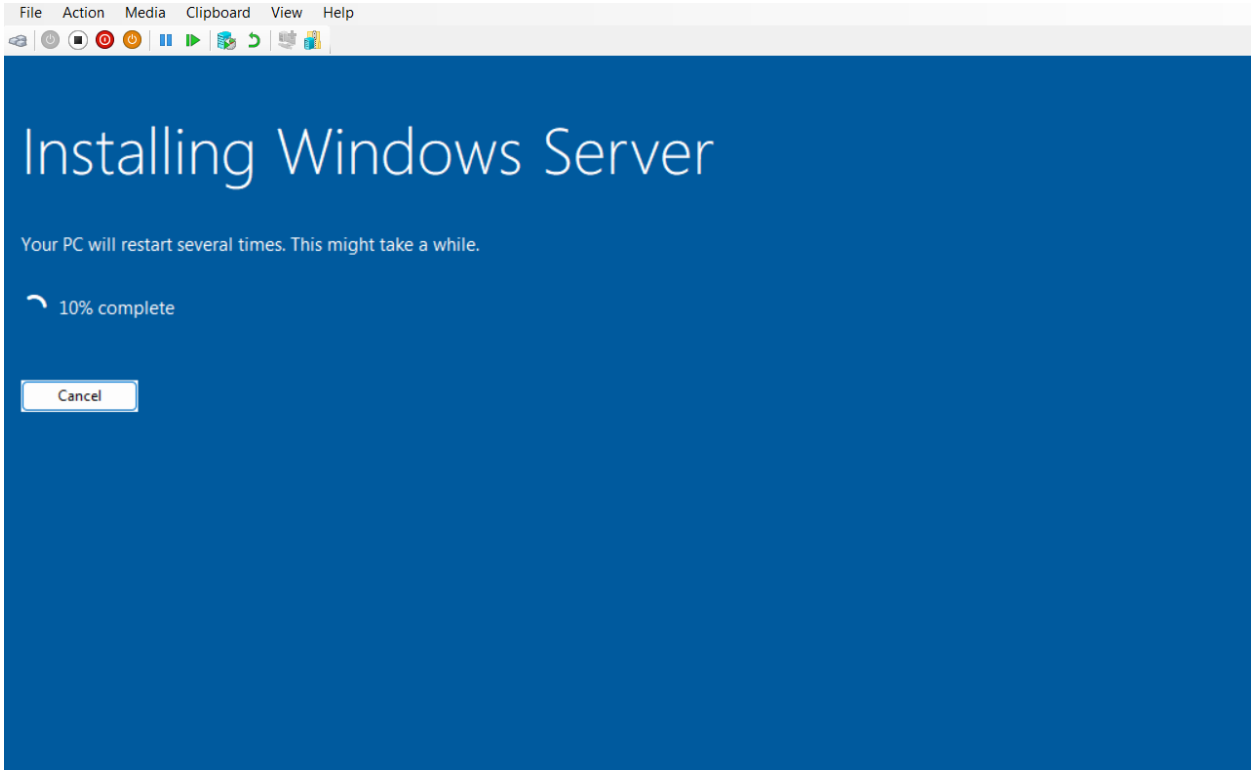

Рисунок 3.22 – Процес встановлення

Коли процес встановлення закінчився, то з’являється сторінка входу в адміністраторський обліковий запис користувача. На даному етапі виконується вхід. Після успішного входу з’являється робочий стіл (рис. 3.23-3.24).

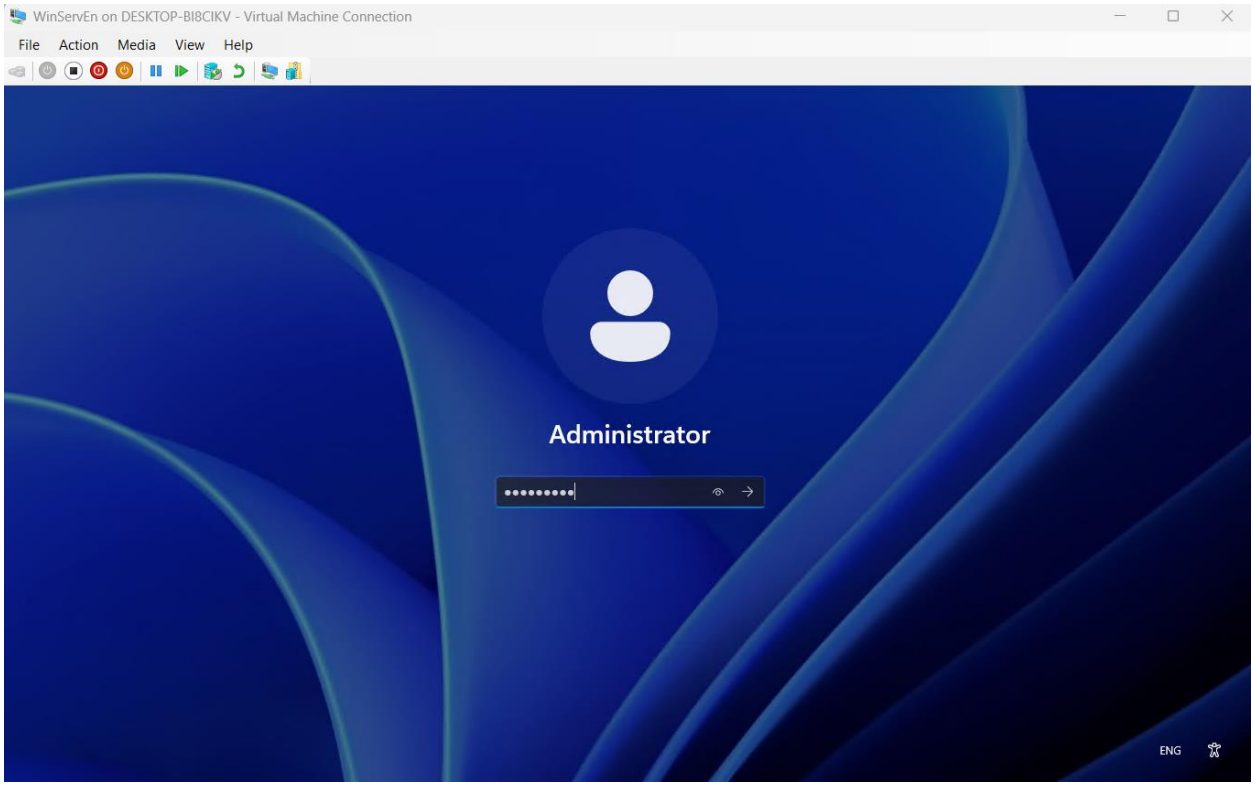

Рисунок 3.23 – Виконання входу в ОС Windows Server 2025

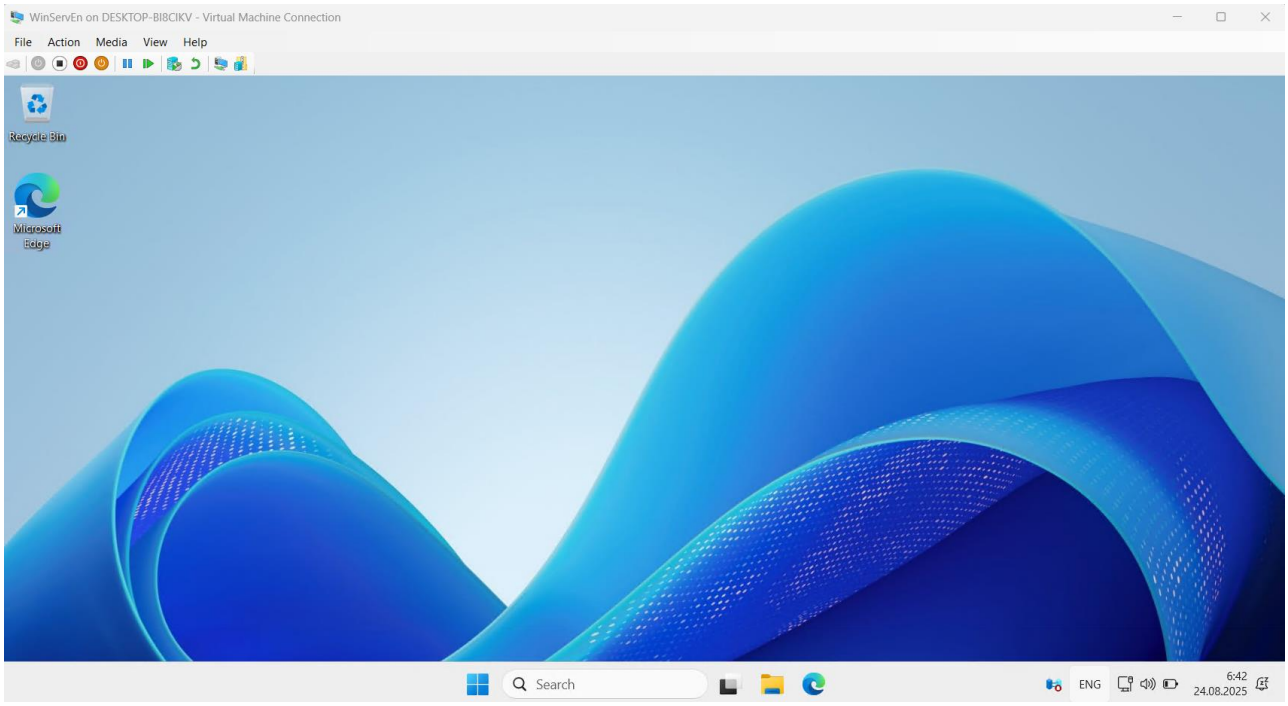

Рисунок 3.24 – Робочий стіл Windows Server 2025 після першого входу в систему

Завдання 2. Налаштування основних параметрів сервера

Перейти до основних налаштувань сервера. Для початку виконати зміну та налаштування IP-адреси сервера. Для цього зайти в «Панель керування», далі «Центр мережних підключень і спільного доступу» – «Зміна параметрів адаптера». Вхід в панель керування здійснюємо, як і в звичайній ОС Windows, через меню «Пуск» (рис. 3.25-3.27).

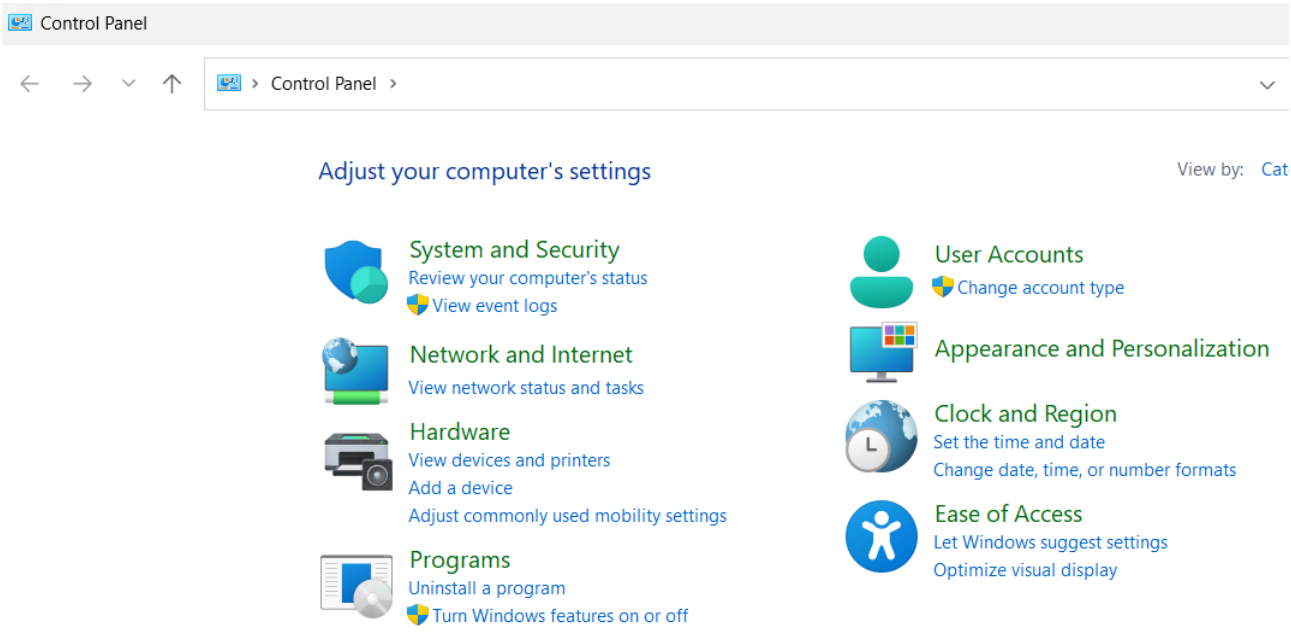

Рисунок 3.25 – Вікно «Панель керування»

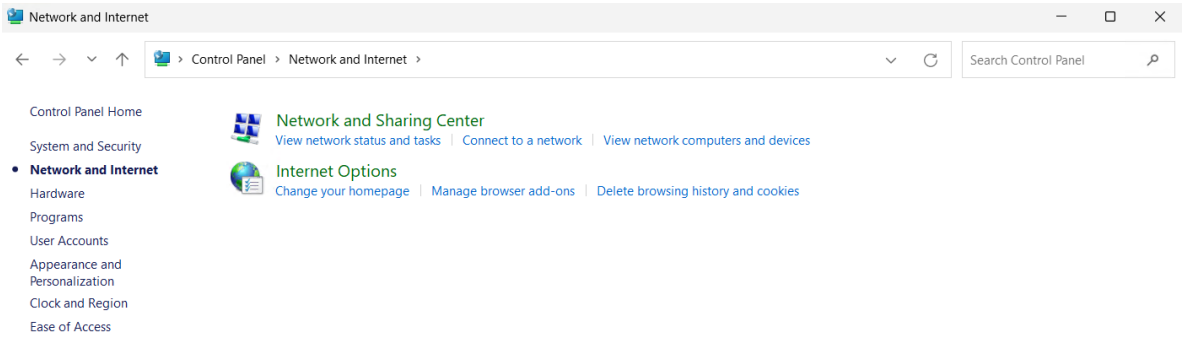

Рисунок 3.26 – Вікно «Мережа та Інтернет»

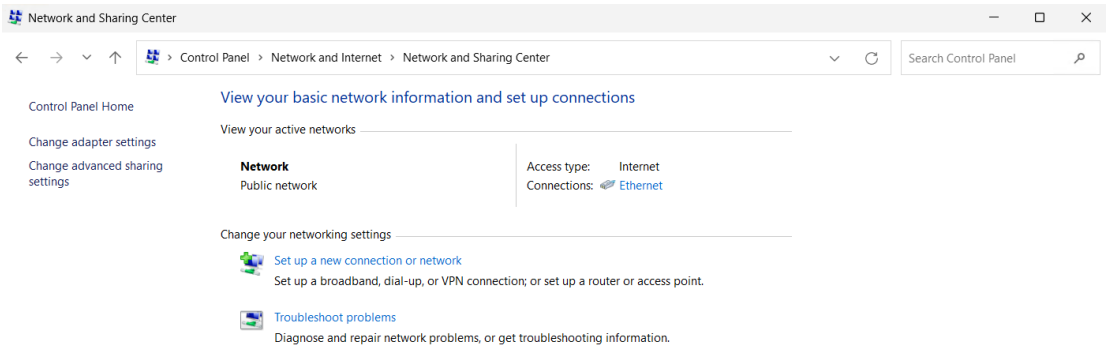

Рисунок 3.27 – Вікно «Центр управління мережами та загальним доступом»

Відкривається вікно «Властивості мережевого адаптера», в цьому вікні перейти до пункту «IP версії 4» та натиснути на нього. В результаті відкривається вікно налаштування IP-параметрів для даного сервера. Ввести IP-адресу, маску мережі, вказати шлюз за замовчуванням та DNS-сервер. Коли налаштування IP завершені, натиснути «ОК» (рис. 3.28-3.29).

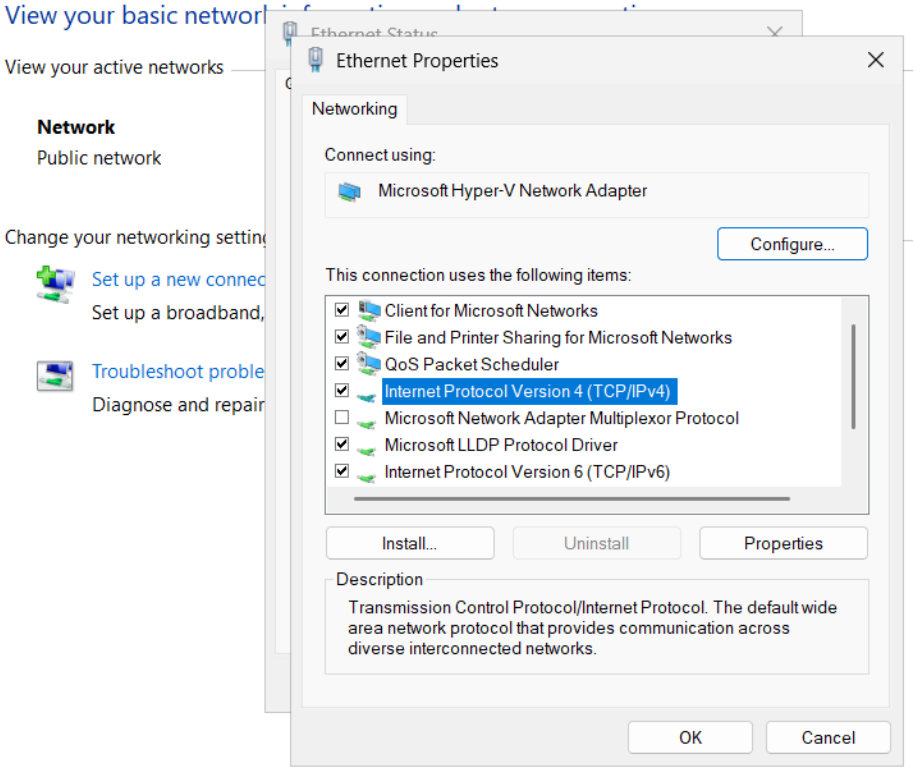

Рисунок 3.28 – Властивості мережевого адаптера

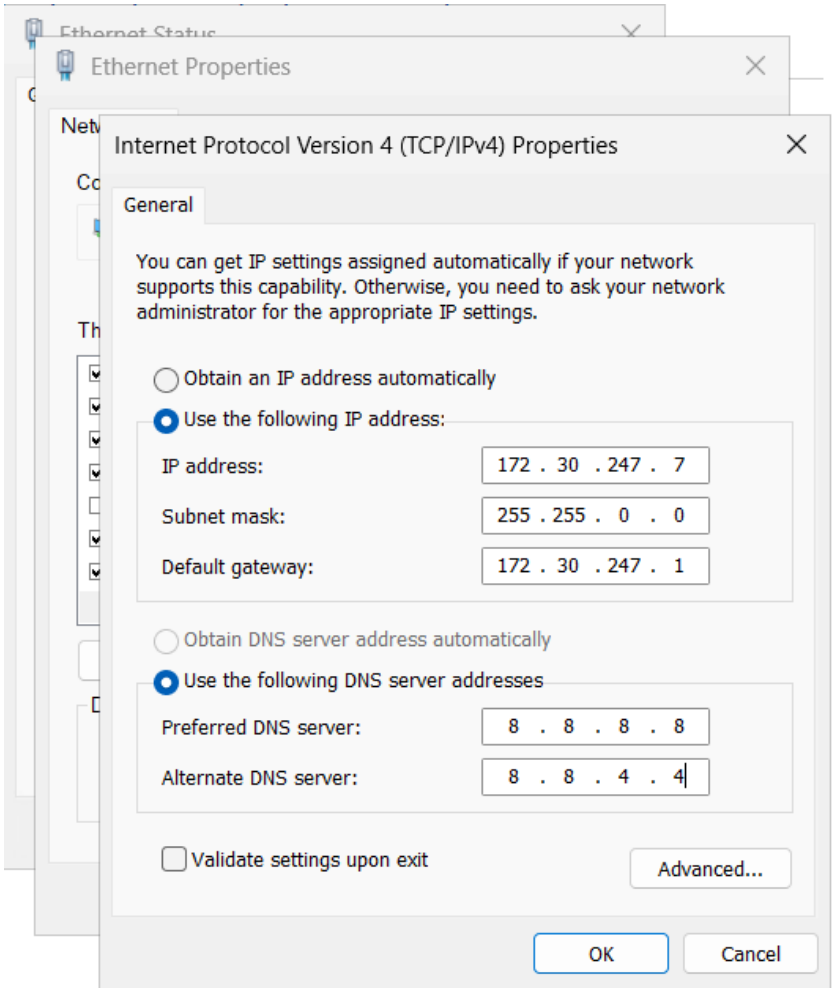

Рисунок 3.29 – Зміна IP-адреси сервера

Після цього виконати перевірку налаштувань IP-параметрів сервера за допомогою команди «ipconfig» в командному рядку (рис. 3.30).

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dd05:79d7:7801:77b7%4
   IPv4 Address. . . . . . . . . . . : 172.30.247.7
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.30.247.1
PS C:\Users\Administrator>
```

Рисунок 3.30 – Перевірка виконаних змін IP-адреси сервера

Далі виконати налаштування дати та часу для сервера. Для цього відкрити «Параметри» в меню «Пуск», далі перейти в пункт меню «Час та мова» – «Дата й час». Змінюємо потрібні параметри, наприклад, часовий пояс вказуємо «UTC +02:00» (рис. 3.31).

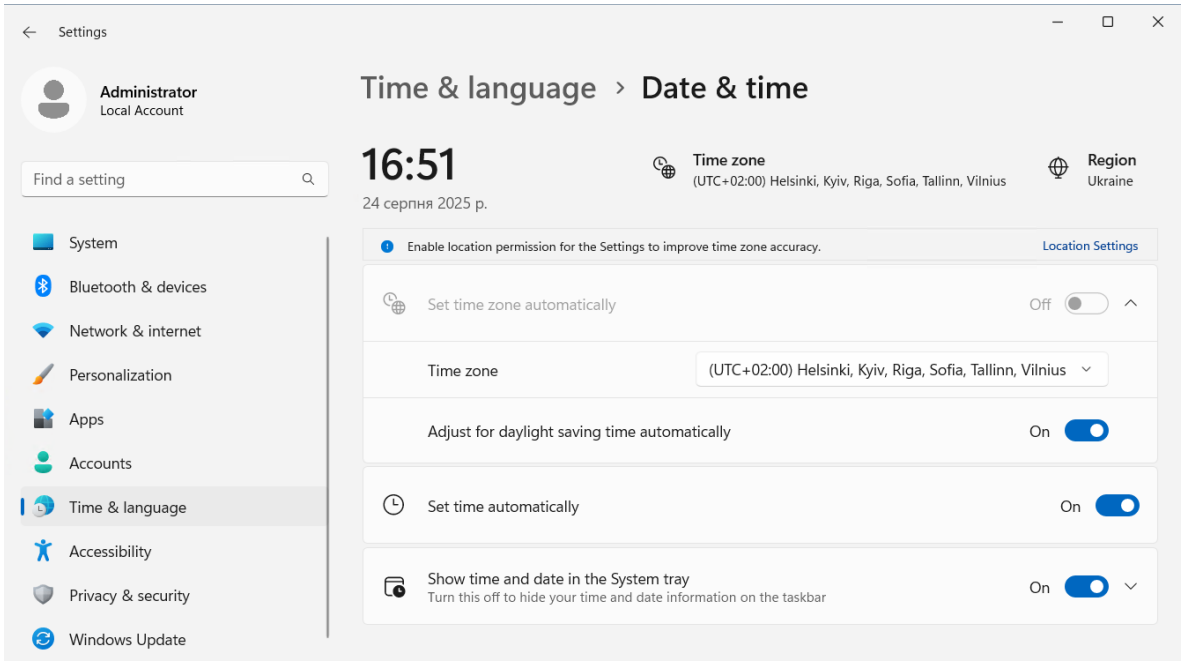

Рисунок 3.31 – Зміна параметрів дати та часу

Згодом провести увімкнення віддаленого робочого столу, що дуже важливо та особливо корисно для віддаленого адміністрування сервера. Для цього відкрити «Диспетчер серверів», далі обирати «Локальний сервер», знайти рядок «Віддалений робочий стіл» і встановити «Увімкнути» (рис. 3.32).

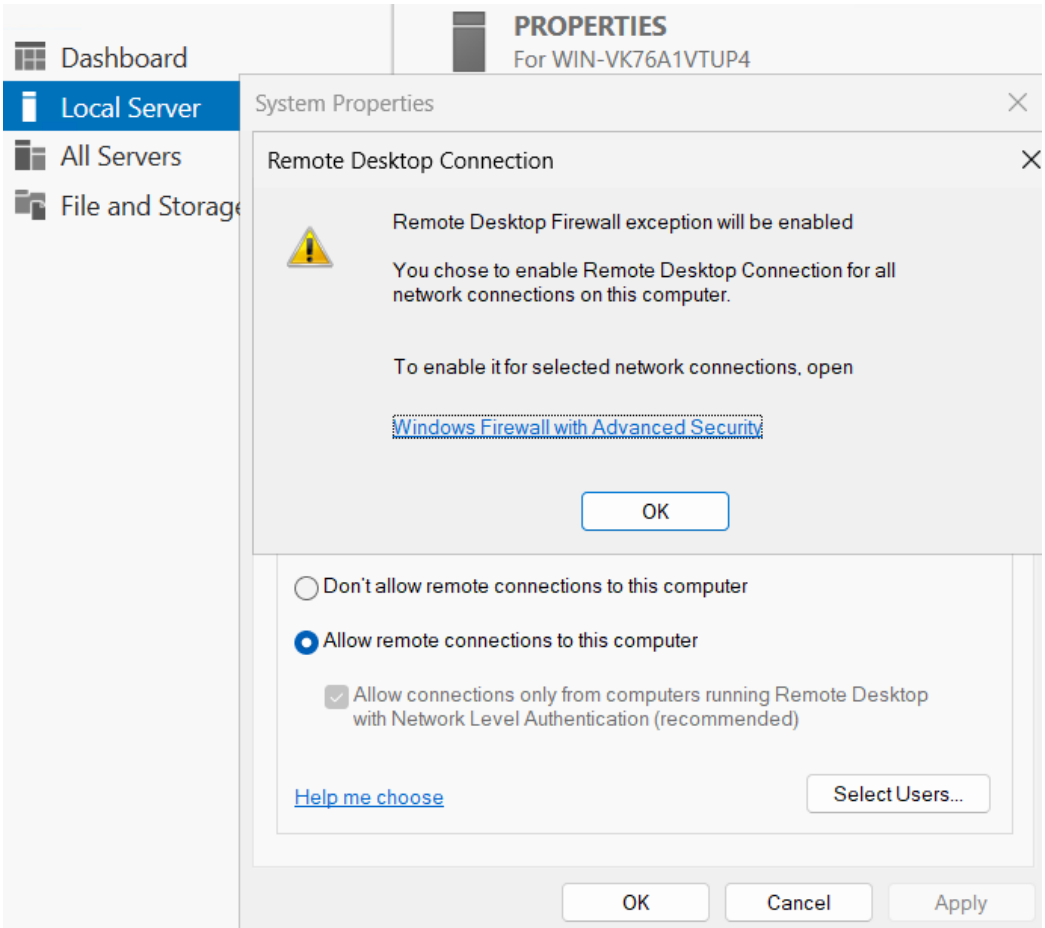

Рисунок 3.32 – Ввімкнення віддаленого доступу до сервера

Наступним етапом налаштування є додавання ролей та компонентів. Це особливо важливо вміти здійснювати, адже від цього залежить, що робитиме та як буде налаштований сервер. Наприклад, якщо встановити роль «DHCP», то даний сервер після налаштування зможе виконувати функції DHCP-сервера. Якщо цю роль не встановити, то він таким видом сервера бути не зможе.

В меню «Диспетчера серверів» – «Налаштувати цей локальний сервер» натиснути «Додати ролі та компоненти». Відкривається «Майстер додавання ролей та компонентів». В першій вкладці даного майстра обирати тип встановлення – «Встановлення ролей та компонентів» (рис. 3.33-3.34).

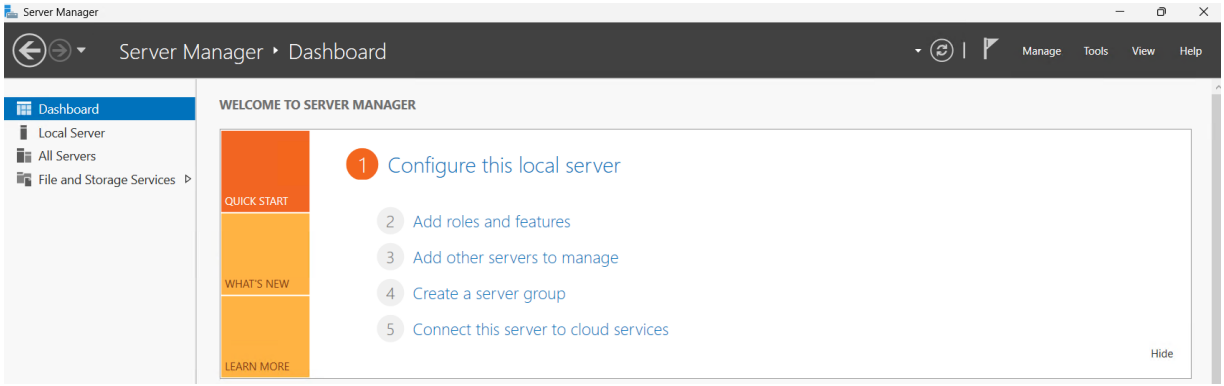

Рисунок 3.33 – Меню налаштування локального сервера

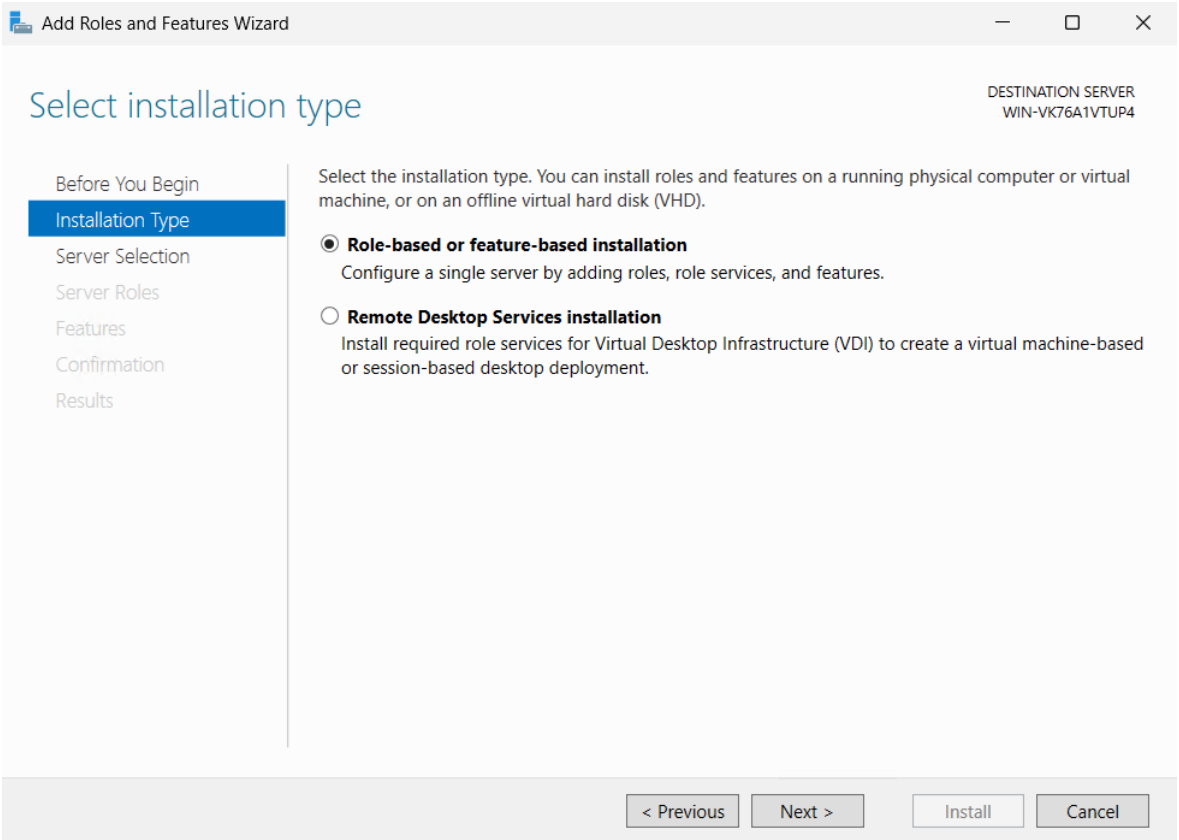

Рисунок 3.34 – Вибір типу встановлення в «Майстрі встановлення ролей та компонентів»

В наступній вкладці майстра вибирати наш сервер, як цільовий для встановлення ролей та компонентів та натиснути «Далі» (рис. 3.35).

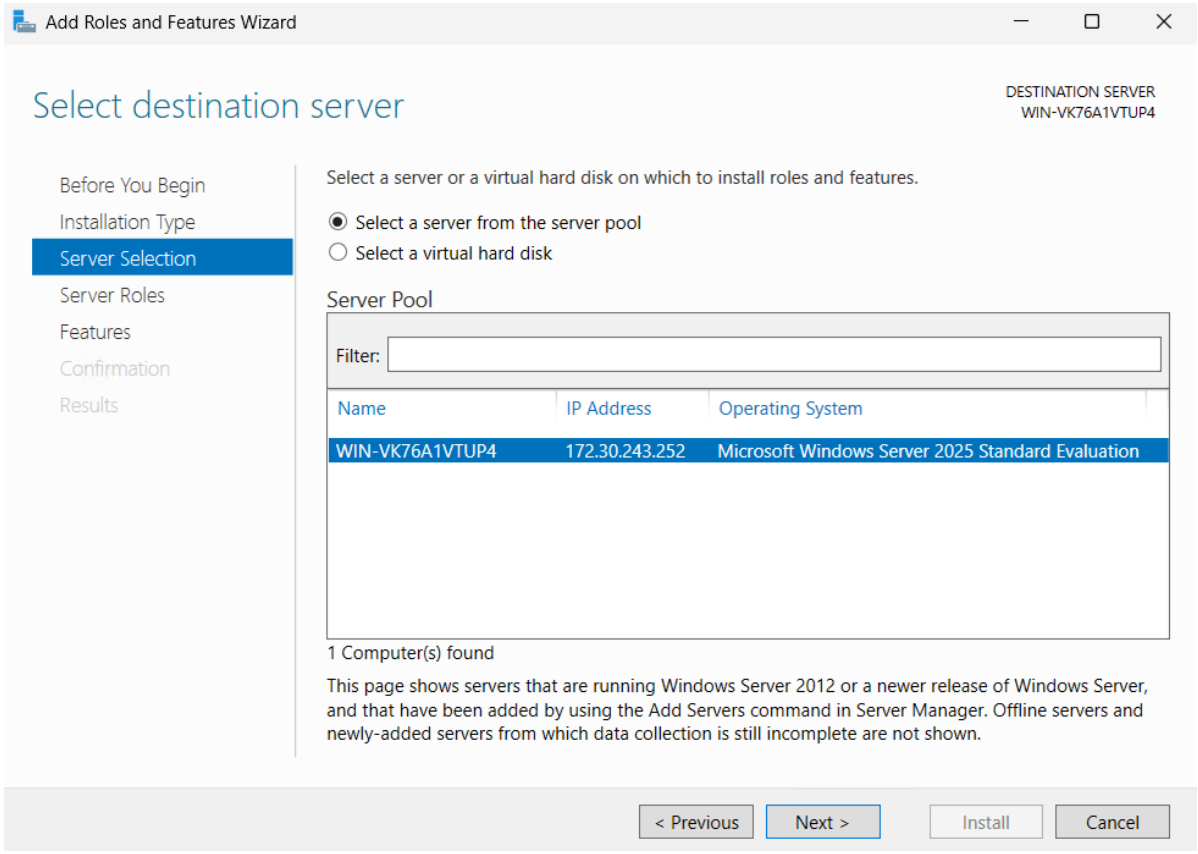

Рисунок 3.35 – Вибір сервера до якого будуть застосовані дії

В наступній вкладці майстра безпосередньо вибирати ролі, які слід додати серверу. Для цього поставити «галочку» навпроти потрібної ролі та у вікні, що відкривається натиснути «Додати компоненти», після цього натиснути «Далі» (рис. 3.36-3.37).

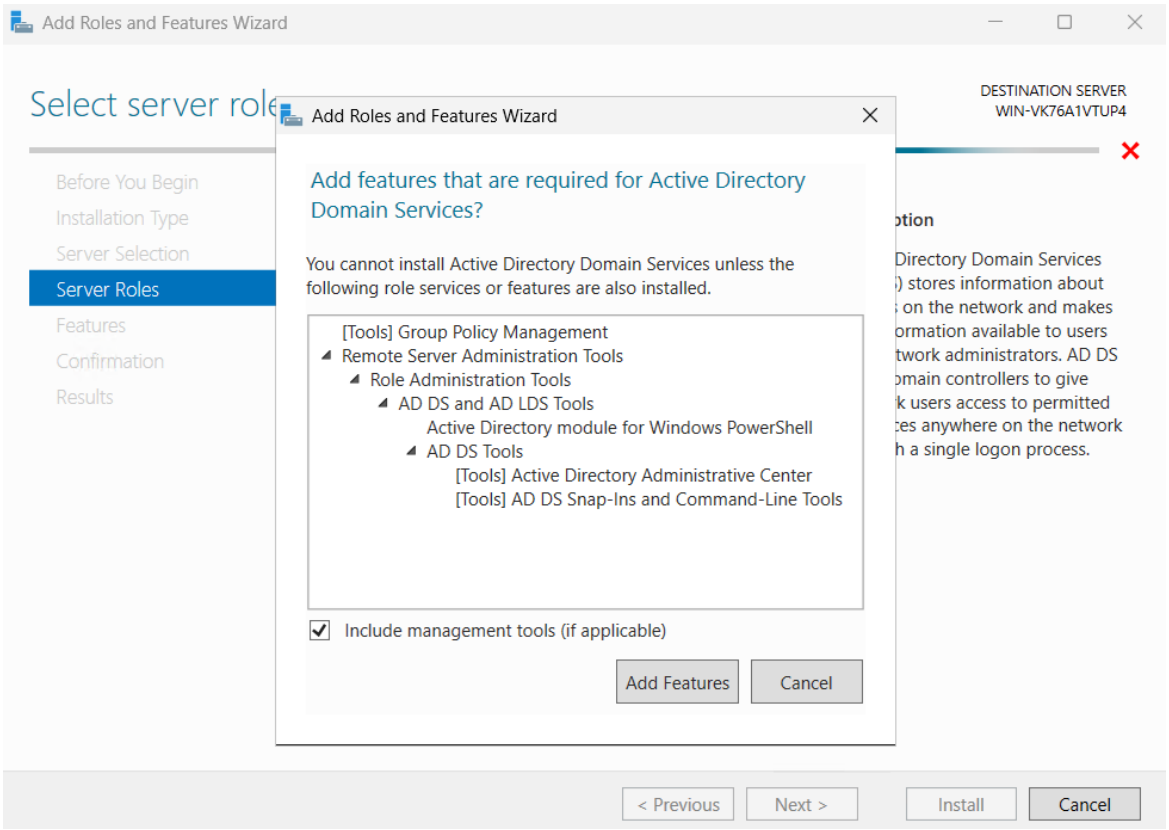

Рисунок 3.36 – Додавання конкретної ролі та її компонентів для сервера

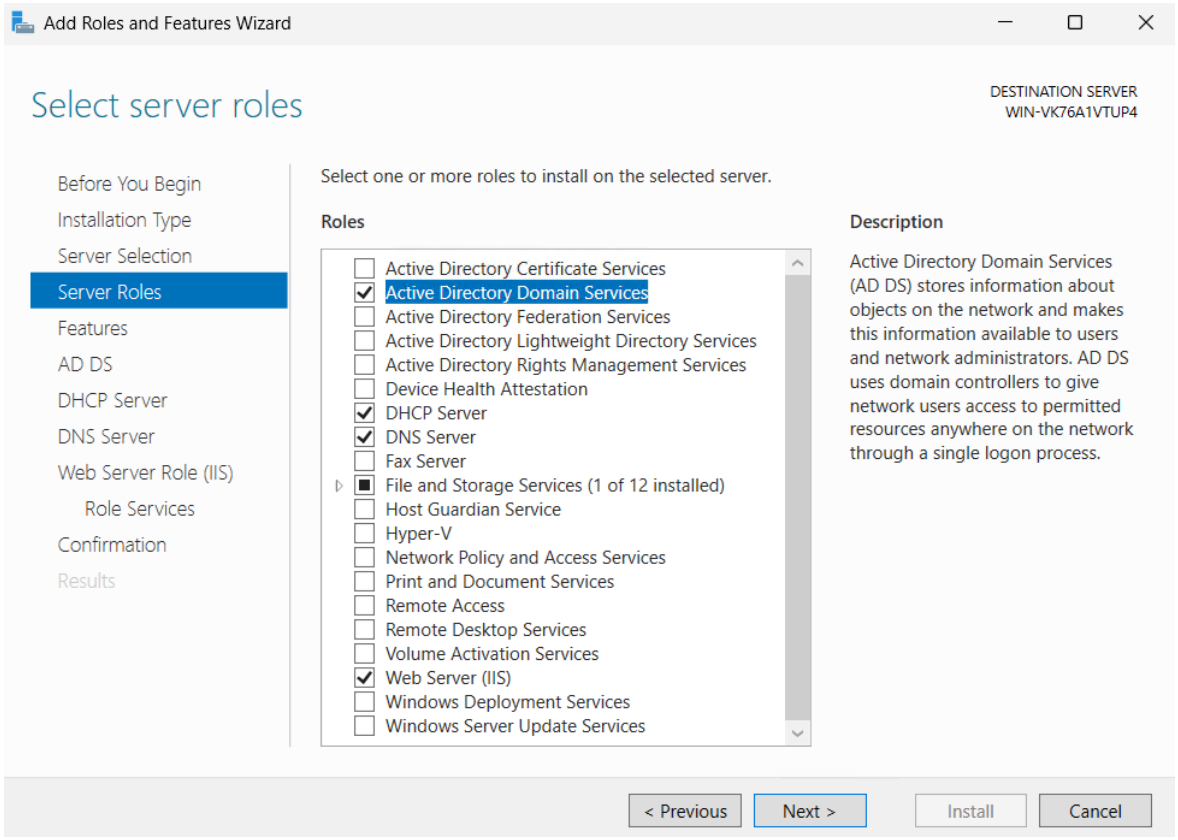

Рисунок 3.37 – Вибір ролей для сервера

В наступній вкладці майстра вибирати компоненти, які слід додати серверу. Для цього ставимо «галочку» навпроти потрібного компонента та після цього натискаємо «Далі» (рис. 3.38).

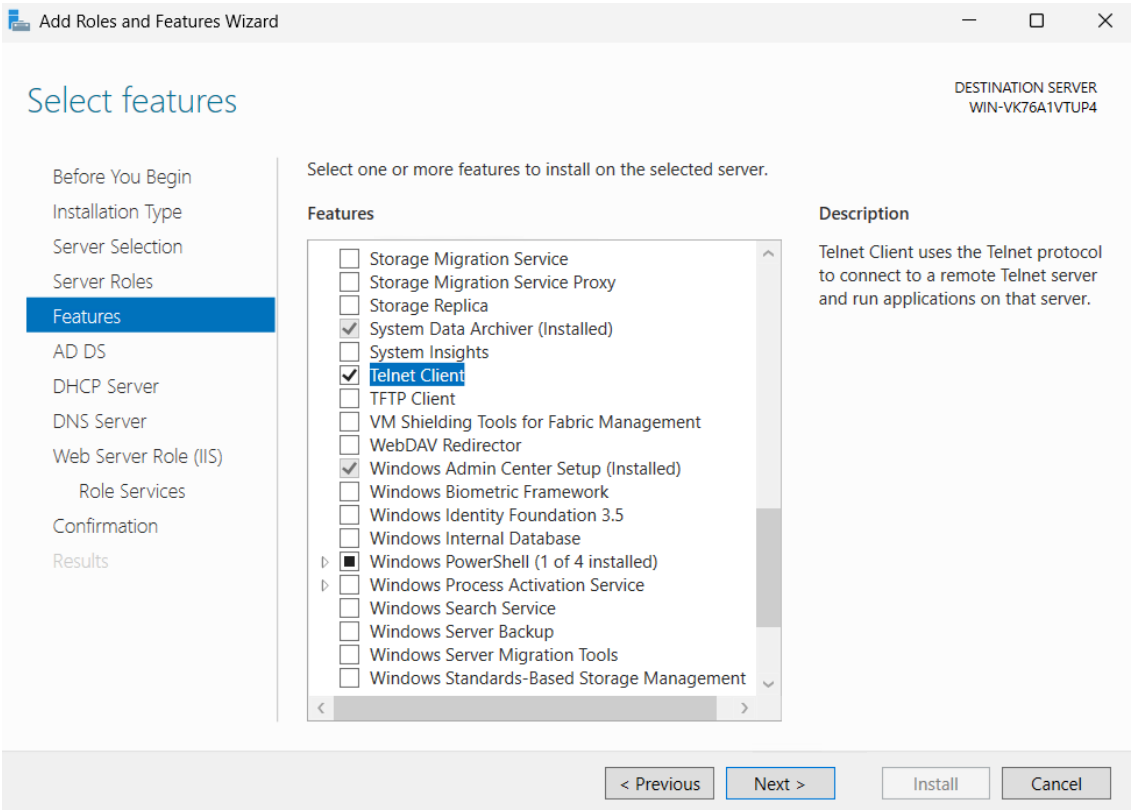

Рисунок 3.38 – Вибір та додавання компонентів

Далі, в наступній вкладці майстра, вибирати служби ролей, які слід додати серверу. Для цього поставити «галочку» навпроти потрібної та після цього натиснути «Далі». Цей вибір є більш вузьким, ніж вибір ролі, адже, щоб його зробити, треба точно знати, що має виконувати сервер (рис. 3.39).

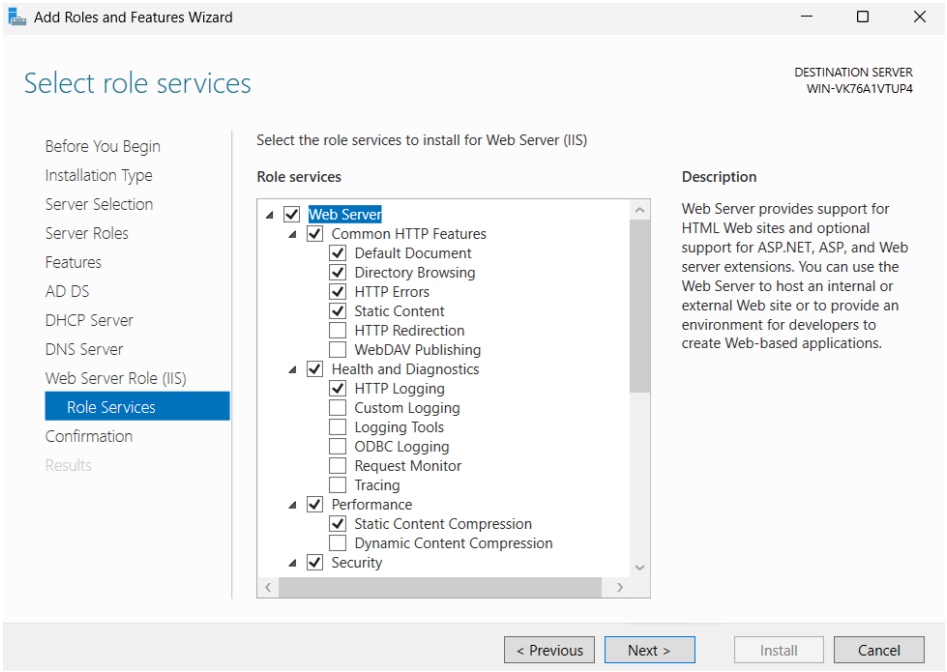

Рисунок 3.39 – Вибір та додавання служб ролей сервера

Далі виконати підтвердження встановлення вибраних ролей та компонентів і натиснути «Встановити». Розпочинається процес встановлення (рис. 3.40-3.41).

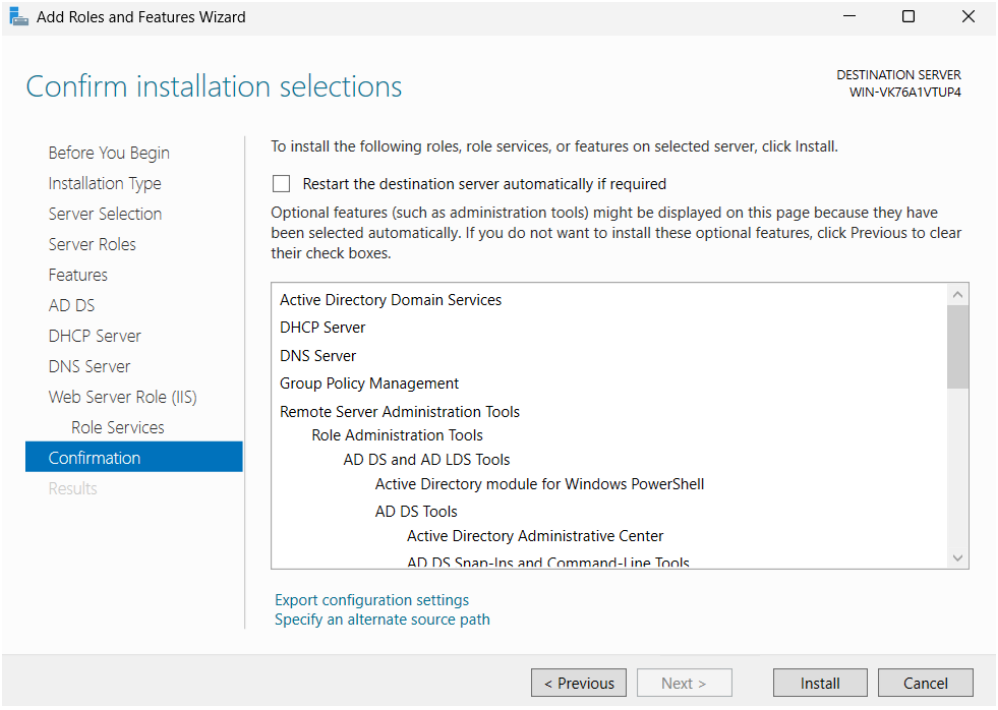

Рисунок 3.40 – Підтвердження встановлення ролей та компонентів для вибраного сервера

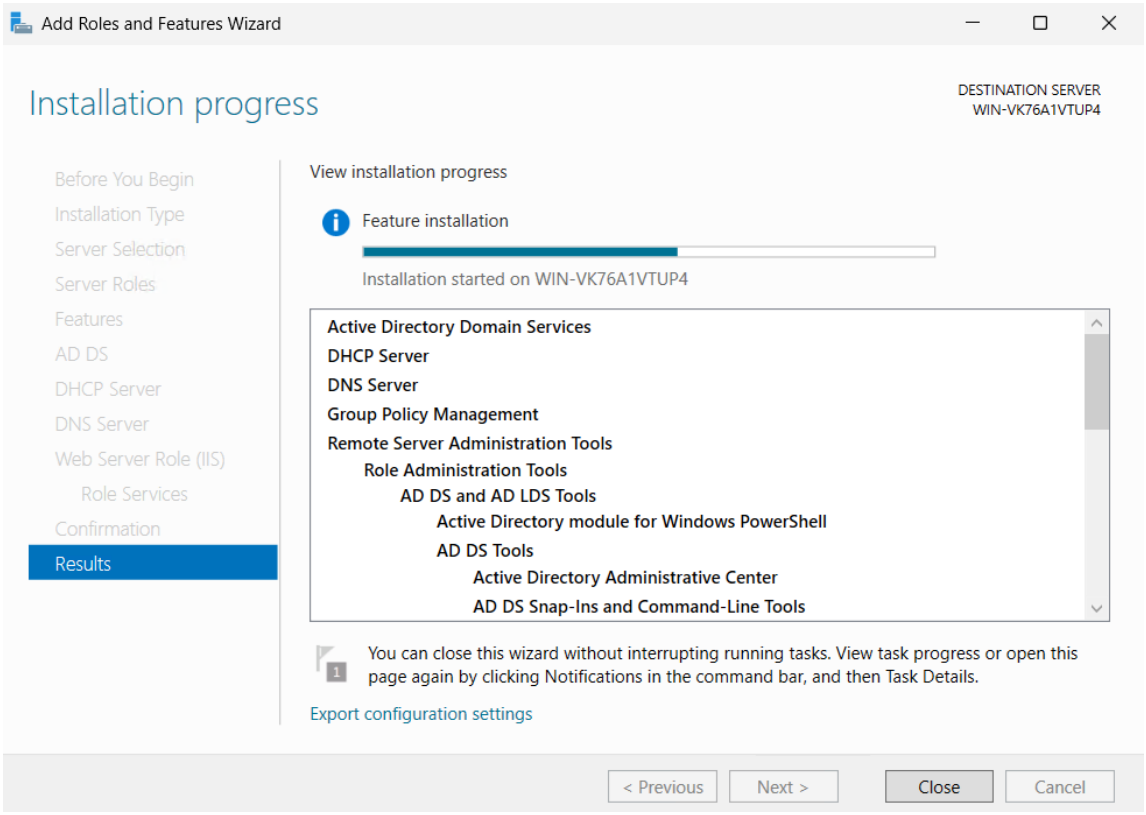

Рисунок 3.41 – Процес встановлення ролей та компонентів після вибору та підтвердження

Після встановлення менеджер відповідної ролі з'явиться у вкладці «Інструменти» в «Диспетчері серверів». Проте інколи виникає необхідність видалити певну роль для сервера. Щоб це виконати в «Диспетчері серверів» натиснути «Управління» – «Видалити ролі та компоненти». В результаті запускається «Майстер видалення ролей та компонентів». Він діє за алгоритмом таким, як і в випадку додавання ролей та компонентів. Звертаємось до вкладки вибору ролей та вибираємо, ту яку необхідно видалити. Підтвердити вибір і запуститься процес видалення обраної ролі та компонента (рис. 3.42-3.44).

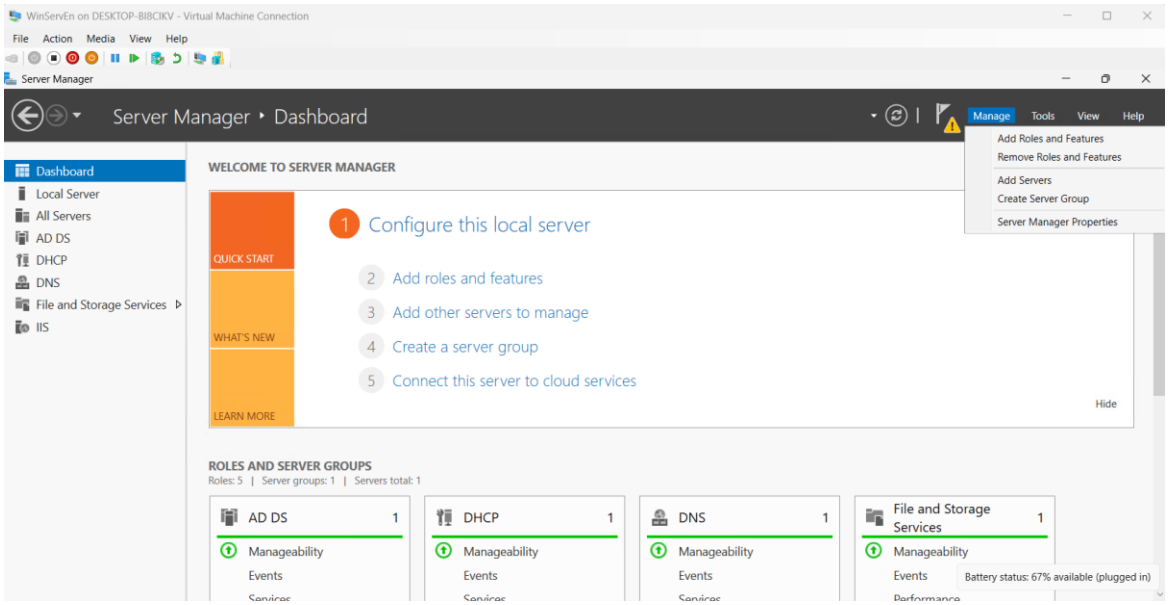

Рисунок 3.42 – Вибір пункту меню «Видалити ролі та компоненти»

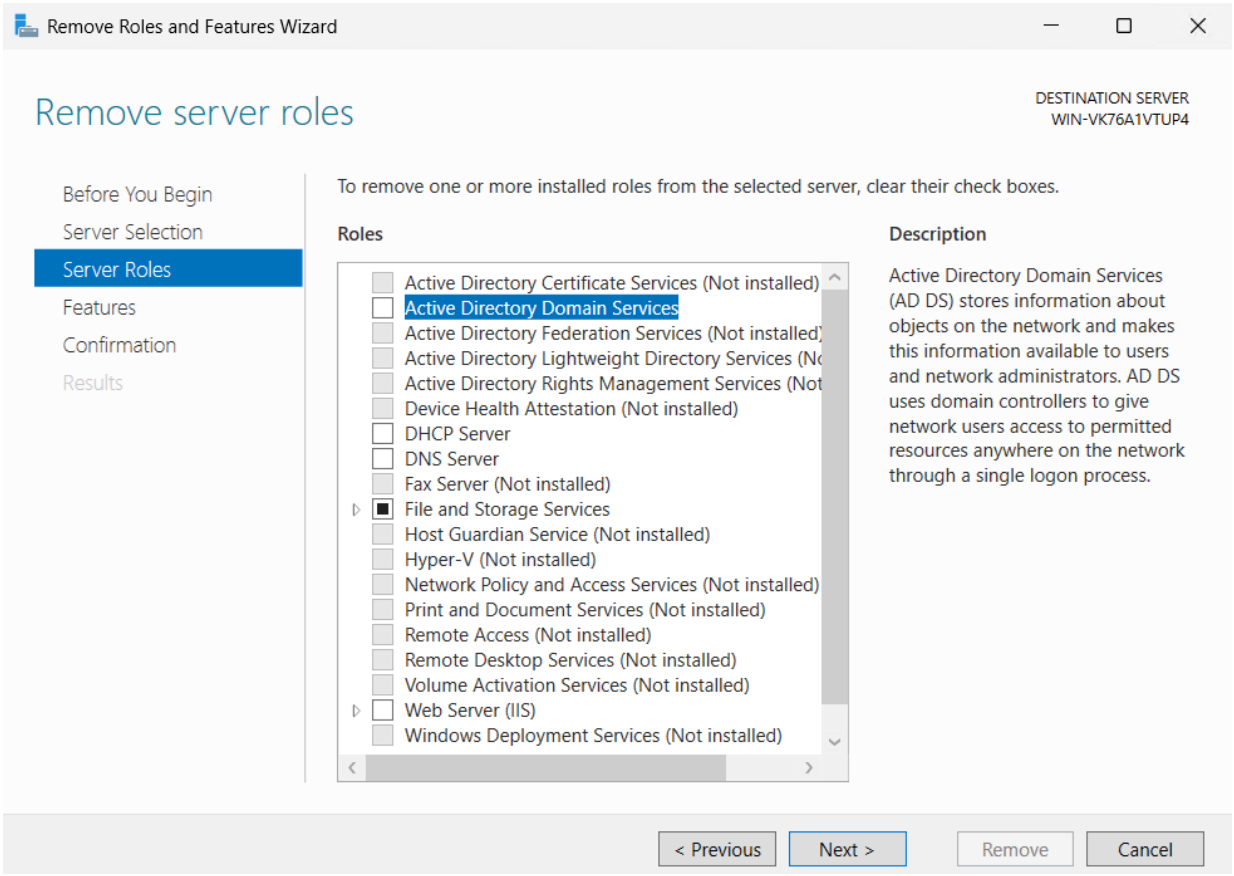

Рисунок 3.43 – Вибір ролі, що буде видалена

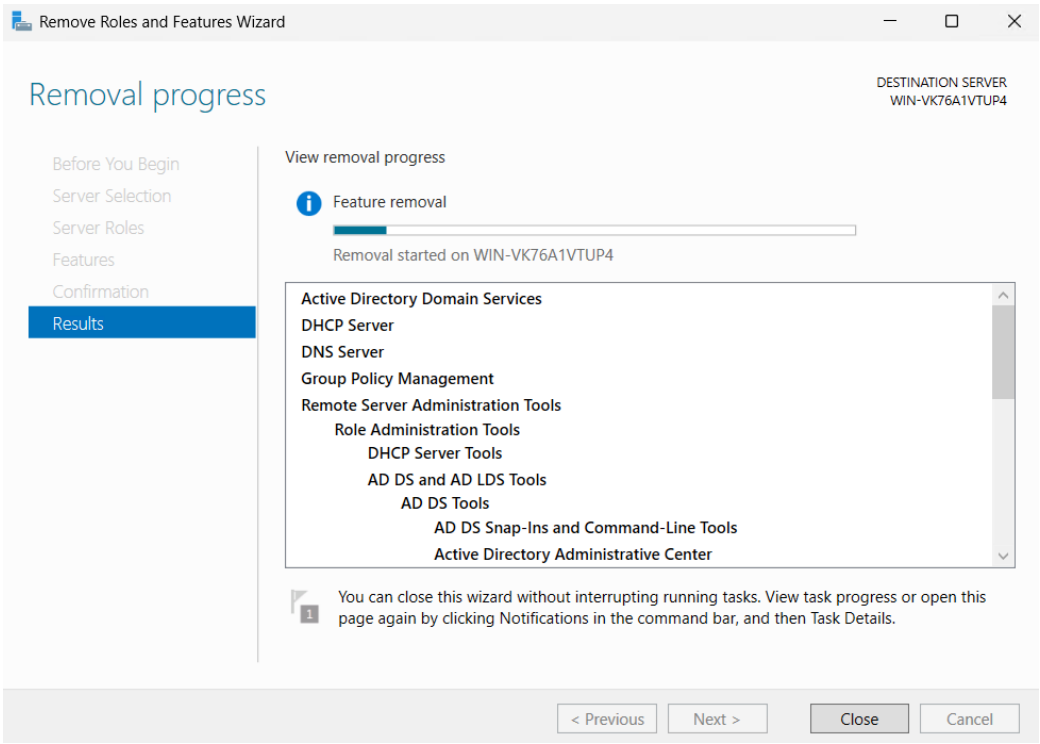

Рисунок 3.44 – Процес видалення вибраних ролей та компонентів

Наступним етапом базового налаштування сервера є налаштування резервного копіювання. Для його здійснення додаємо для сервера компонент «Система архівації даних Windows Server», що відповідає за резервне копіювання. Резервне копіювання у Windows Server можна здійснити вручну або ж іншим словом одноразово або налаштувати автоматичне резервне

копіювання в певний час доби та з певною частотою. Зазвичай, адміністратори використовують саме другий метод резервного копіювання (автоматичне) (рис. 3.45).

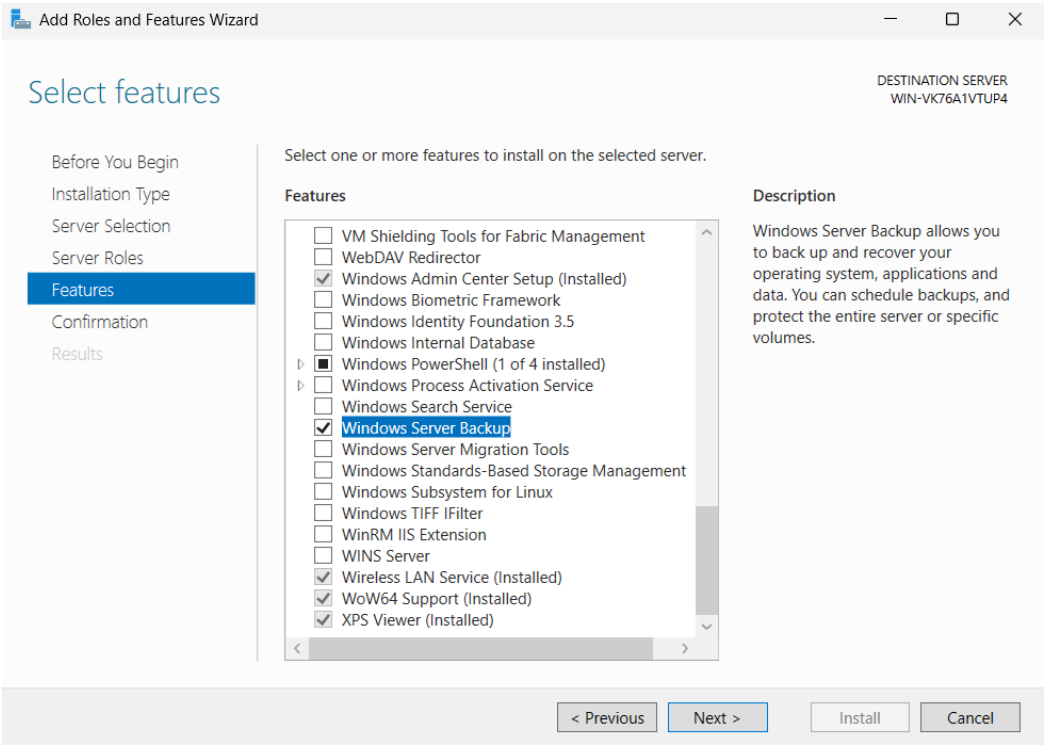

Рисунок 3.45 – Встановлення компонента «Система архівації даних Windows Server»

Відкрити «Систему архівації даних Windows Server» для налаштування резервного копіювання. Натиснути «Інструменти» – «Система архівації даних Windows Server» (рис. 3.46).

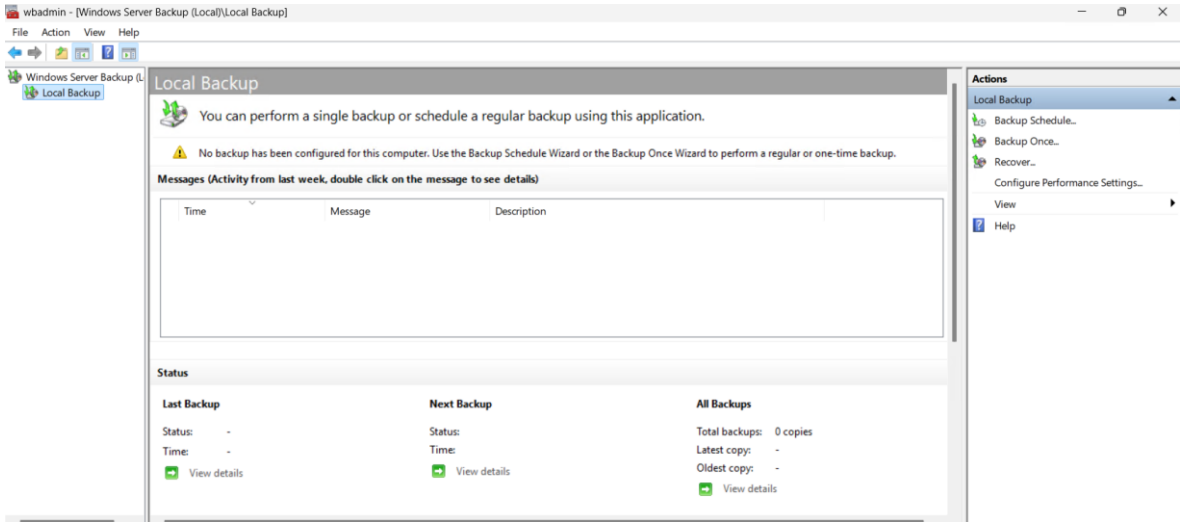

Рисунок 3.46 – Відкрите вікно «Система архівації даних Windows Server»

Налаштуємо автоматичне резервне копіювання, для цього у вікні «Система архівації даних Windows Server» – «Дії» натиснути «Розклад архівації». Відкриється нове вікно «Майстра розкладу архівації», там обирати тип архівації «Весь сервер» і натиснути «Далі». Після цього перейти до

наступної вкладки, де налаштувати час здійснення резервного копіювання та частоту (рис. 3.47-3.48).

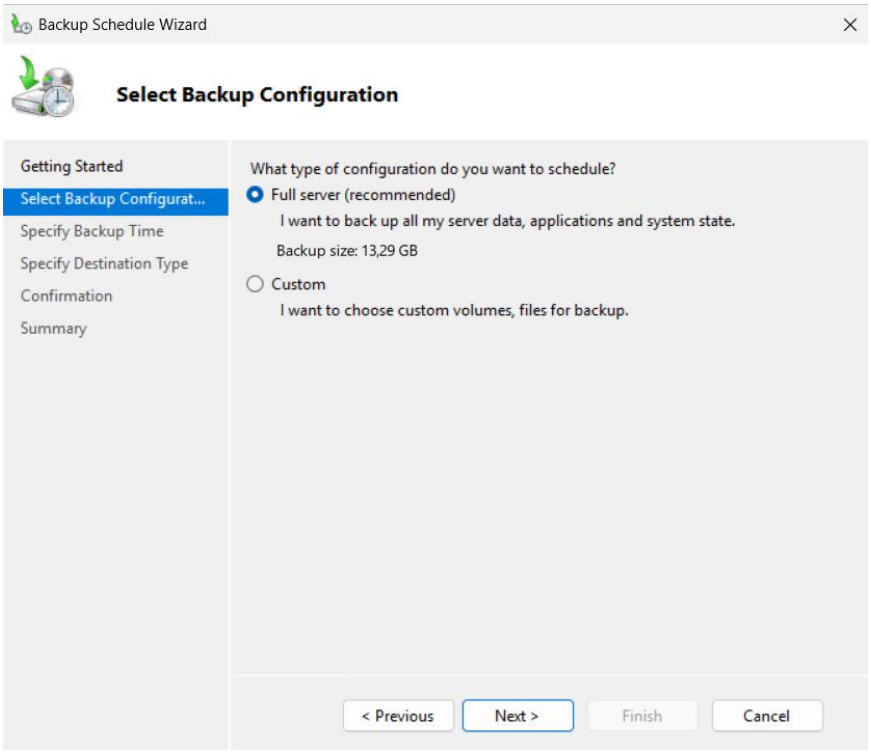

Рисунок 3.47 – Початок налаштування автоматичного резервного копіювання

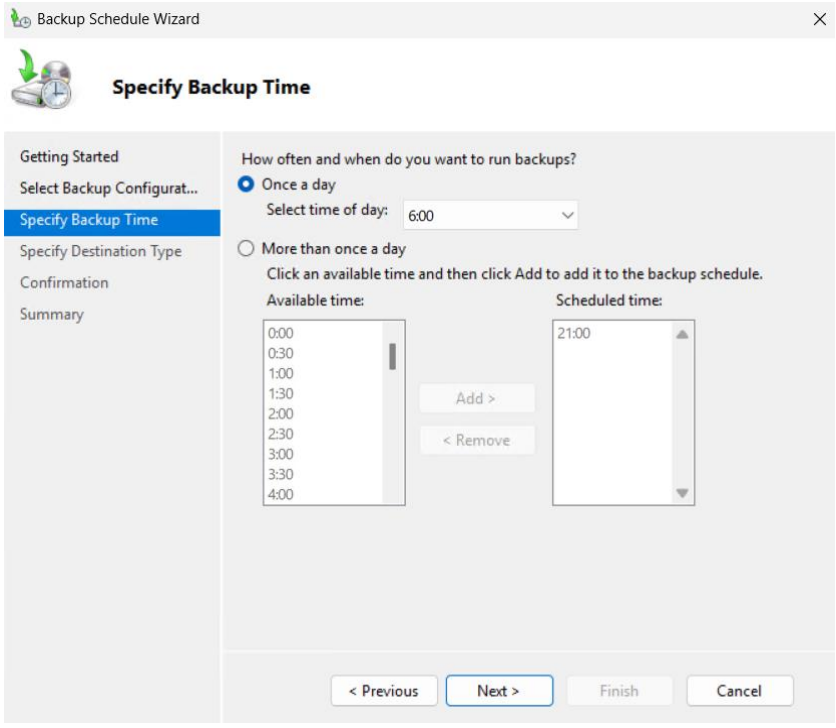

Рисунок 3.48 – Вибір часу та частоти резервного копіювання

Далі вибирати місце зберігання резервних копій, що будуть створюватися. В цьому випадку обирати «Архівація на жорсткий диск для архівів», далі здійснити безпосередню вказівку диска, який саме відповідатиме за збереження резервних копій. Потім підтвердити налаштування та натиснути

«Готово». В результаті цих дій автоматичне резервне копіювання налаштовано (рис. 3.49).

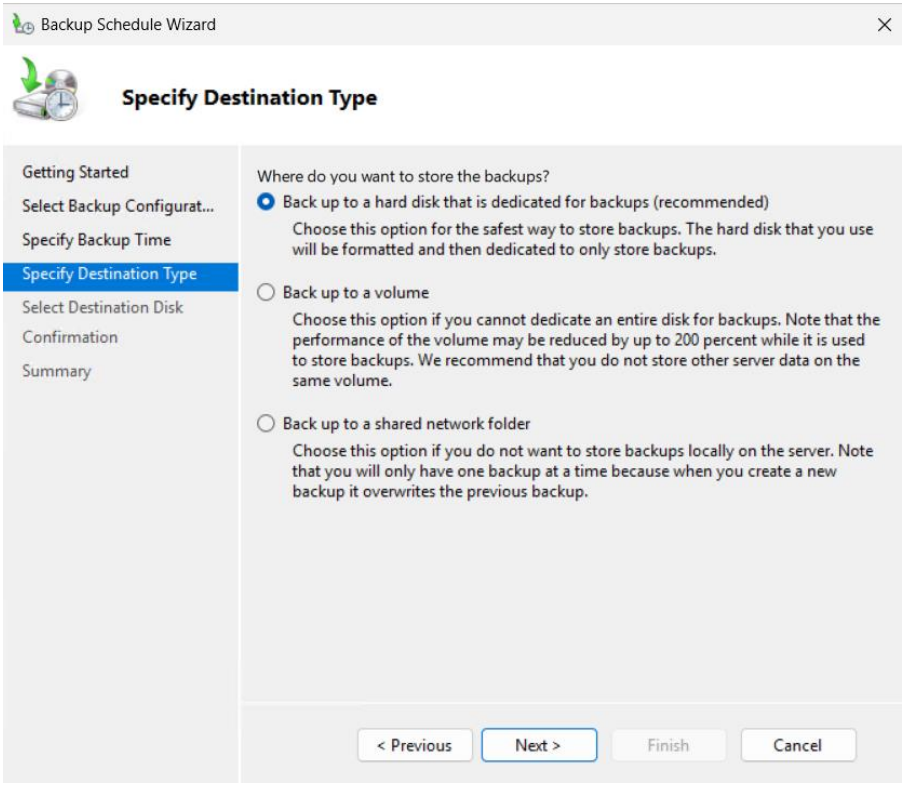

Рисунок 3.49 – Вибір типу місця призначення для автоматичного резервного копіювання сервера

Завдання 3. Аналіз системних журналів Windows Server 2025

Для роботи з системним журналами у Windows Server 2025, як і в інших ОС серії Windows, використовується утиліту «Перегляд подій». На робочому столі натиснути «Пуск». У полі пошуку вводимо «Event Viewer» та відкриваємо знайдену програму. Альтернативний шлях відкриття – це «Win + R» – «eventvwr.msc» – «Enter». Відкривається вікно «Перегляд подій» (рис. 3.50).

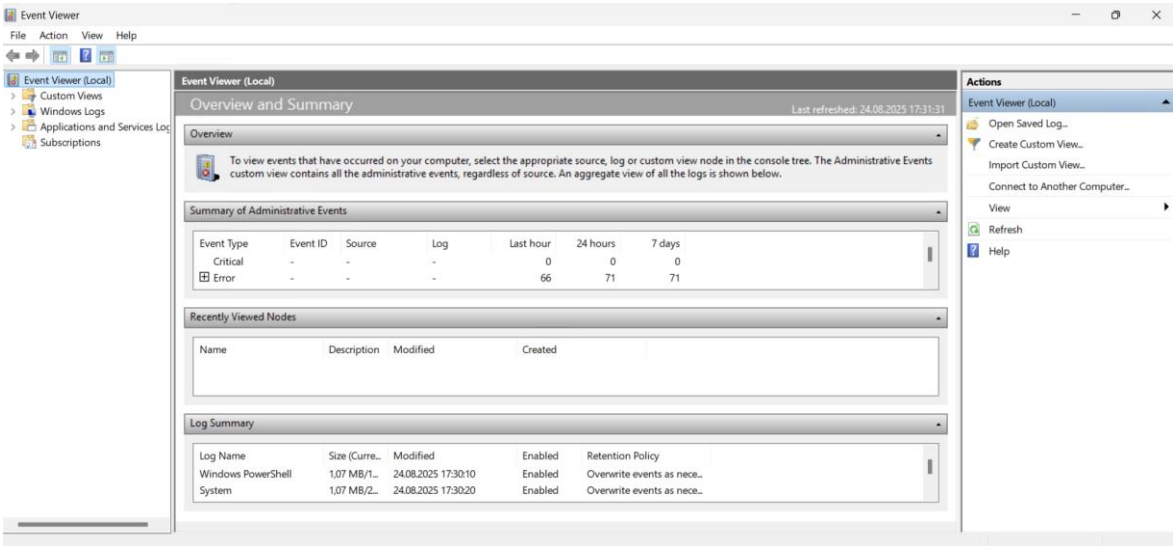

Рисунок 3.50 – Вікно «Перегляд подій»

У лівій панелі є основні розділи за кожним з яких є свій журнал певного виду. Перший з них – це «Застосунки» (Журнал програм). У цьому журналі зберігаються події, пов’язані з роботою програм і застосунків, які встановлені в системі. Тут можна знайти інформацію про помилки, попередження чи інформаційні повідомлення від програмного забезпечення. Наприклад, якщо програма аварійно завершила роботу або не змогла знайти потрібний файл, у журналі буде відповідний запис. Це допомагає адміністраторам і користувачам діагностувати проблеми з конкретними застосунками (рис. 3.51).

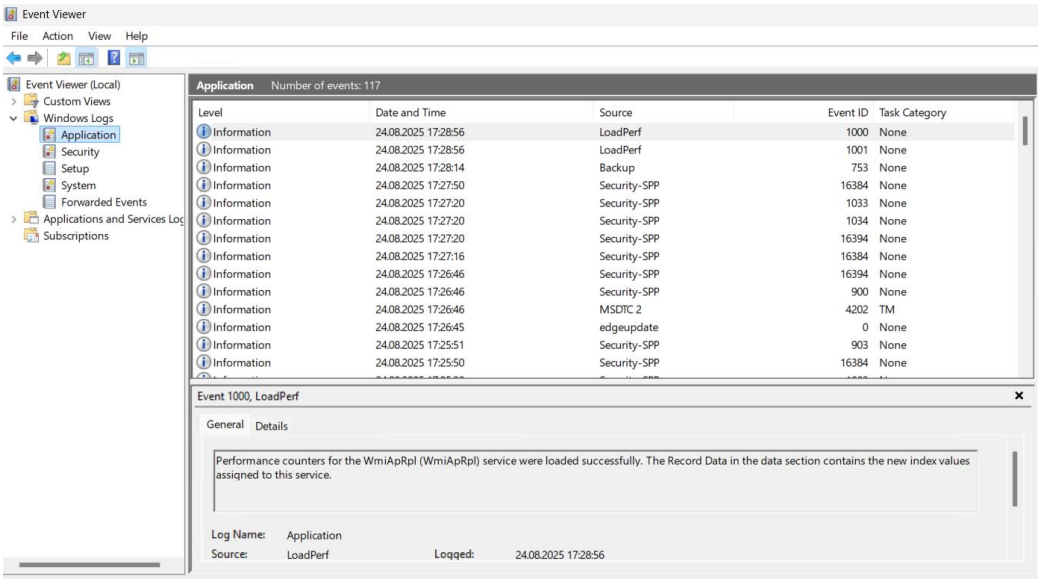

Рисунок 3.51 – Журнал «Застосунки»

Наступний журнал – це журнал «Безпека». Його назва говорить сама за себе і цей журнал використовується для відстеження подій, пов’язаних із безпекою системи. У ньому фіксуються як успішні, так і невдалі спроби входу в систему, зміни прав користувачів, спроби доступу до файлів або ресурсів, а також інші події, що можуть впливати на безпеку. Це головний журнал, який адміністратори перевіряють під час аналізу можливих атак чи порушень політик безпеки (рис. 3.52).

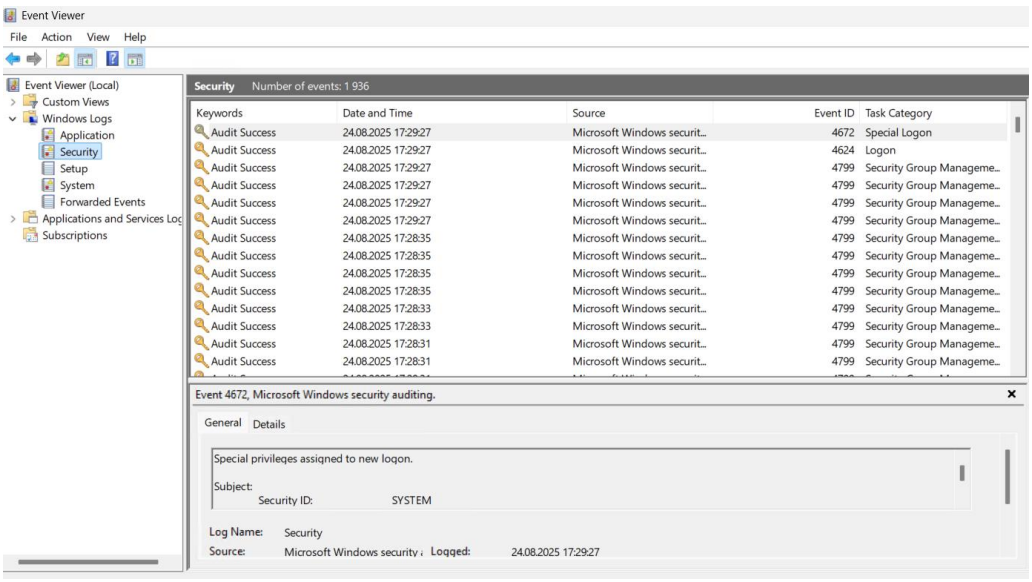

Рисунок 3.52 – Журнал «Безпека»

Третій журнал – це «Встановлення» (Журнал налаштувань). Тут зберігаються записи, пов’язані з інсталяцією та налаштуванням системних компонентів Windows. У цьому журналі можна побачити інформацію про встановлення оновлень, зміни конфігурації системи або додавання ролей і функцій на сервері. Він найчастіше використовується для аналізу процесу інсталяції чи перевірки, чи коректно відбулося встановлення програмного забезпечення (рис. 3.53).

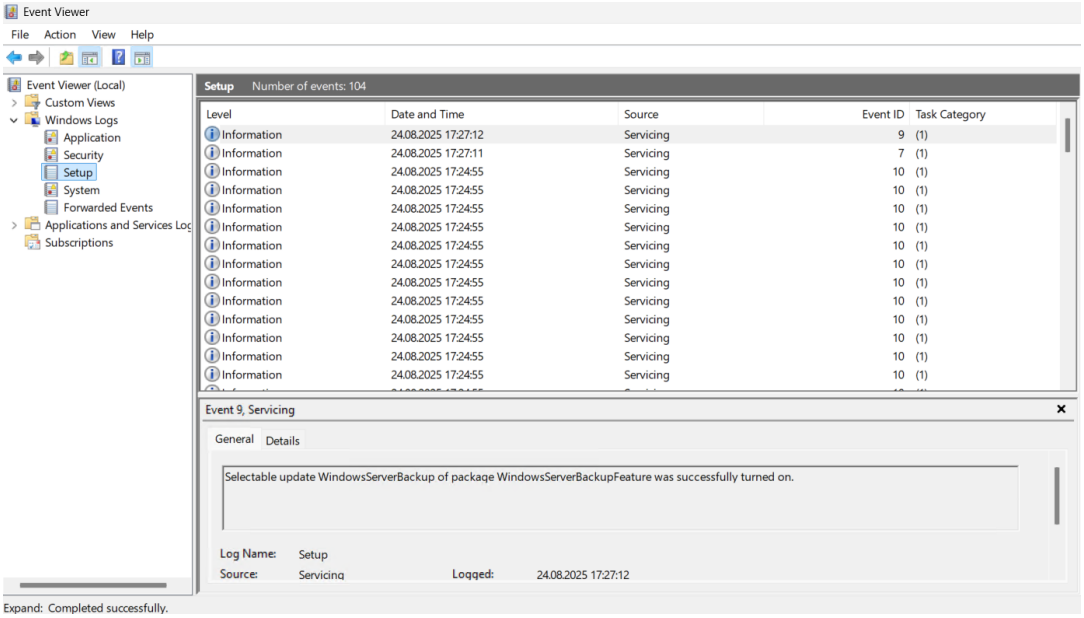

Рисунок 3.53 – Журнал «Встановлення»

Четвертий журнал – «Система» (Системний журнал). У цьому журналі фіксуються події, пов’язані з роботою самої операційної системи. Тут можна знайти повідомлення від драйверів пристроїв, системних служб і модулів Windows. Наприклад, якщо збій спричинив драйвер відеокарти або служба Windows не змогла запуститися, подія буде зафіксована саме в журналі «Система». Це основне джерело інформації для діагностики апаратних і системних проблем (рис. 3.54).

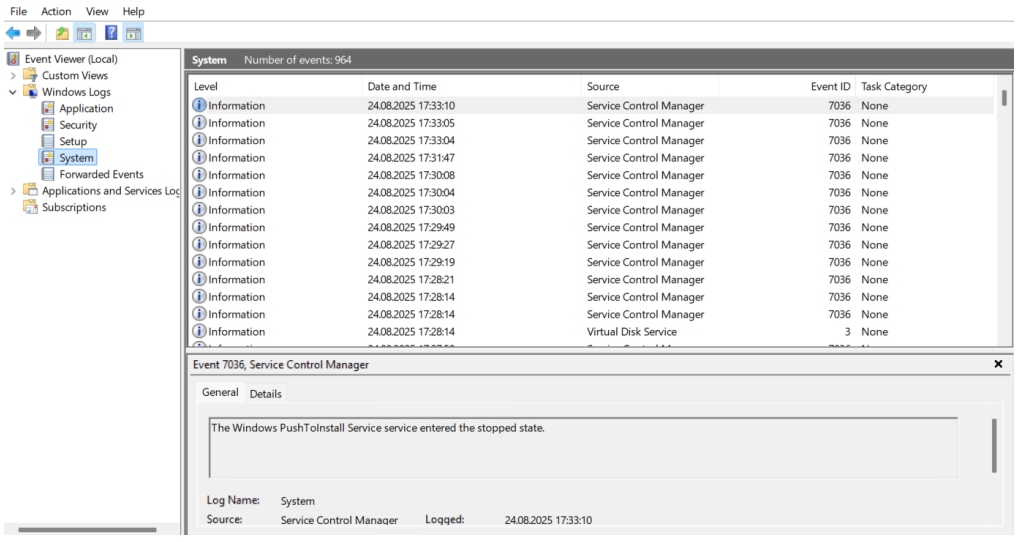

Рисунок 3.54 – Журнал «Система»

Ще один журнал «Переслані події» використовується у випадках, коли налаштований збір подій із кількох комп'ютерів у мережі. Події з віддалених машин пересилаються в центральний комп'ютер і зберігаються саме тут. Це зручно для адміністраторів, які керують великою кількістю серверів або робочих станцій, оскільки дозволяє централізовано відслідковувати всі важливі події.

Існує також такий вид журналів, як журнали програм та служб. Це спеціалізований розділ, де зберігаються події від окремих сервісів або компонентів Windows, а також від деяких сторонніх програм. Наприклад, тут можна знайти журнали служби Active Directory, DNS-сервера чи інших системних ролей. На відміну від загальних журналів, цей розділ дає змогу отримати більш детальну і вузьконаправлену інформацію про роботу конкретних служб.

Кожен журнал містить записи про події, які відносяться до сфери його відповідальності. Для детального аналізу події на неї потрібно натиснути двічі і відкриється вікно «Властивості події», де буде представлена інформація про вибрану подію (рис. 3.55).

Рисунок 3.55 – Властивості події

Для зручності аналізу журналів передбачена можливість фільтрації кожного журналу. Для цього вибравши потрібний журнал, справа в меню обираємо «Фільтрувати поточний журнал». Далі у вікні, що відкрилося встановити параметри фільтрації подій. Наприклад, можна встановити час, за який показувати події та рівень або тип події, можна фільтрувати за кодом події. Виставити потрібні параметри та натиснути «ОК» і у вікні з'являється «відфільтрований» журнал (рис. 3.56-3.57).

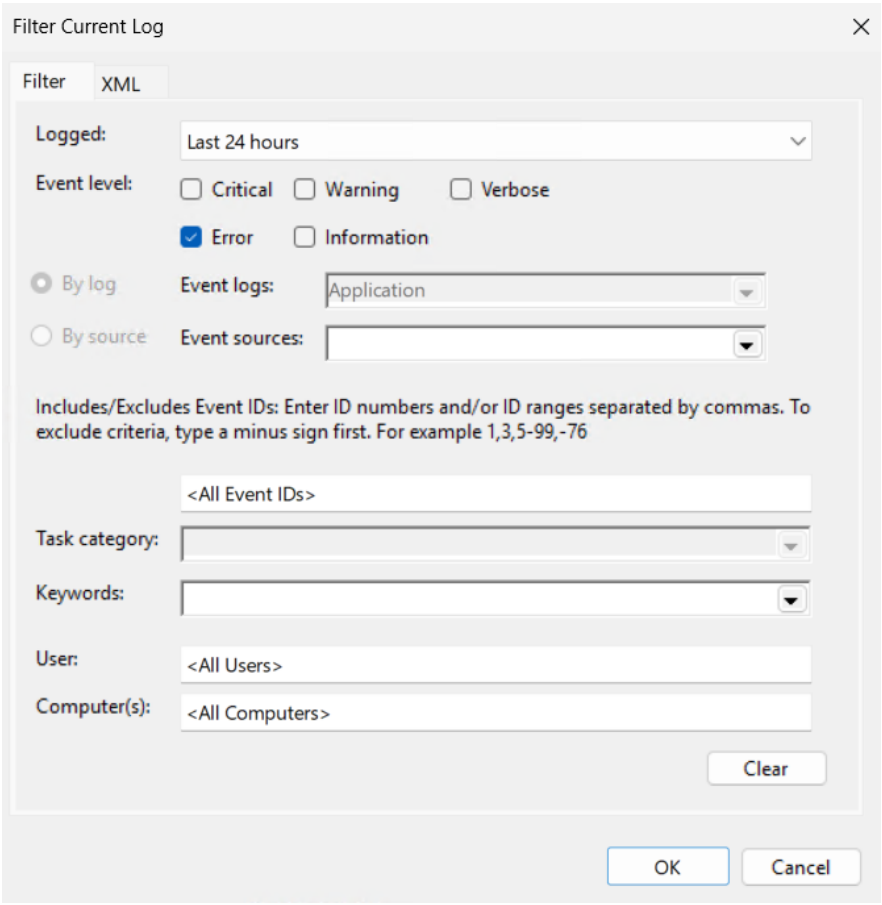

Рисунок 3.56 – Фільтрацію журналу для знаходження помилок за останні 24 години

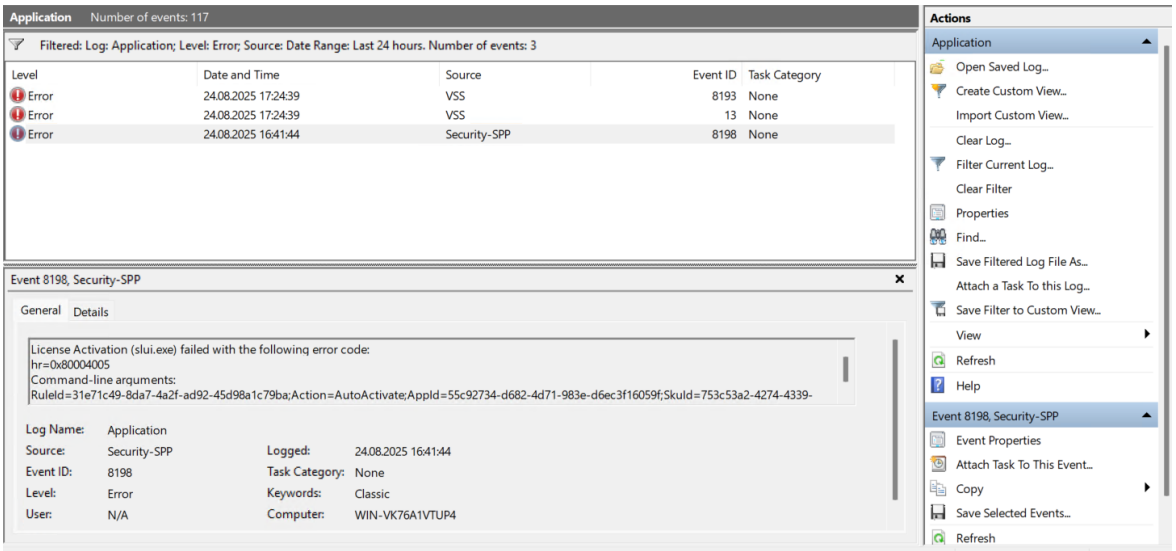

Рисунок 3.57 – Результати фільтрації на знаходження помилок

Для подальшого або пізнішого аналізу журнал можна зберегти, натиснувши в меню «Дії» – «Зберегти всі події як…» та обрати куди зберегти файл та під якою назвою. Можна зберігати, як увесь журнал, так і його частину, отриману шляхом фільтрації подій (рис. 3.58).

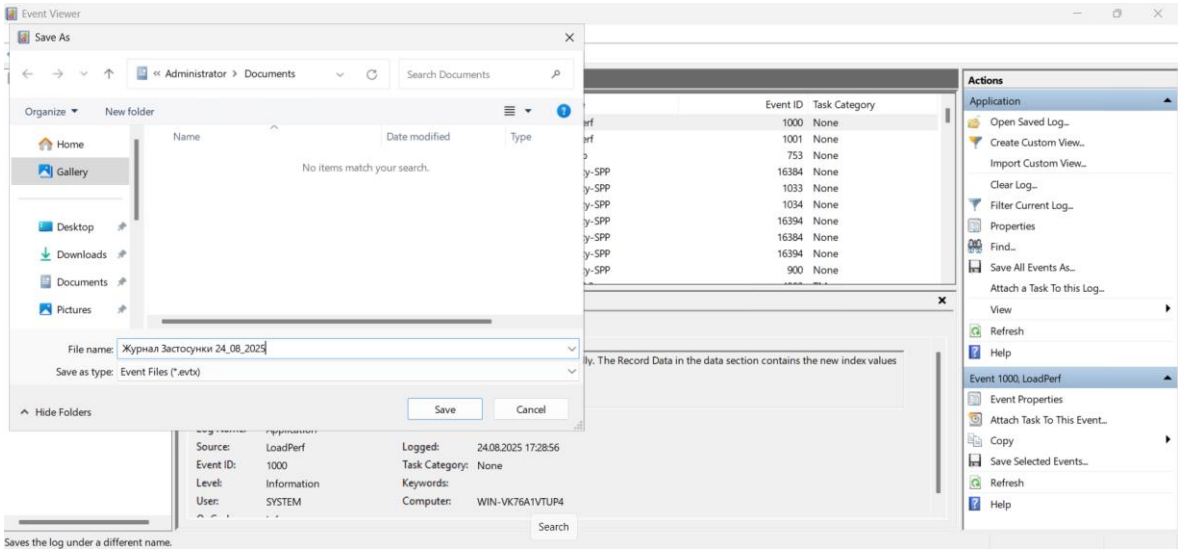

Рисунок 3.58 – Збереження журналу

Для аналізу подій у журналі безпеки особливо корисною буде можливість фільтрації за кодом події. Наприклад, для відстеження подій типу «Спроба входу в систему не вдалася» відриваємо «Фільтрувати поточний журнал» та вказуємо код події «4625», застосовуємо фільтр. В результаті побачимо випадки невдалого входу. Якщо таких подій багато і вони здійснювалися з одного комп'ютера та облікового запису користувача, то може свідчити про зловмисні дії (рис. 3.59-3.60).

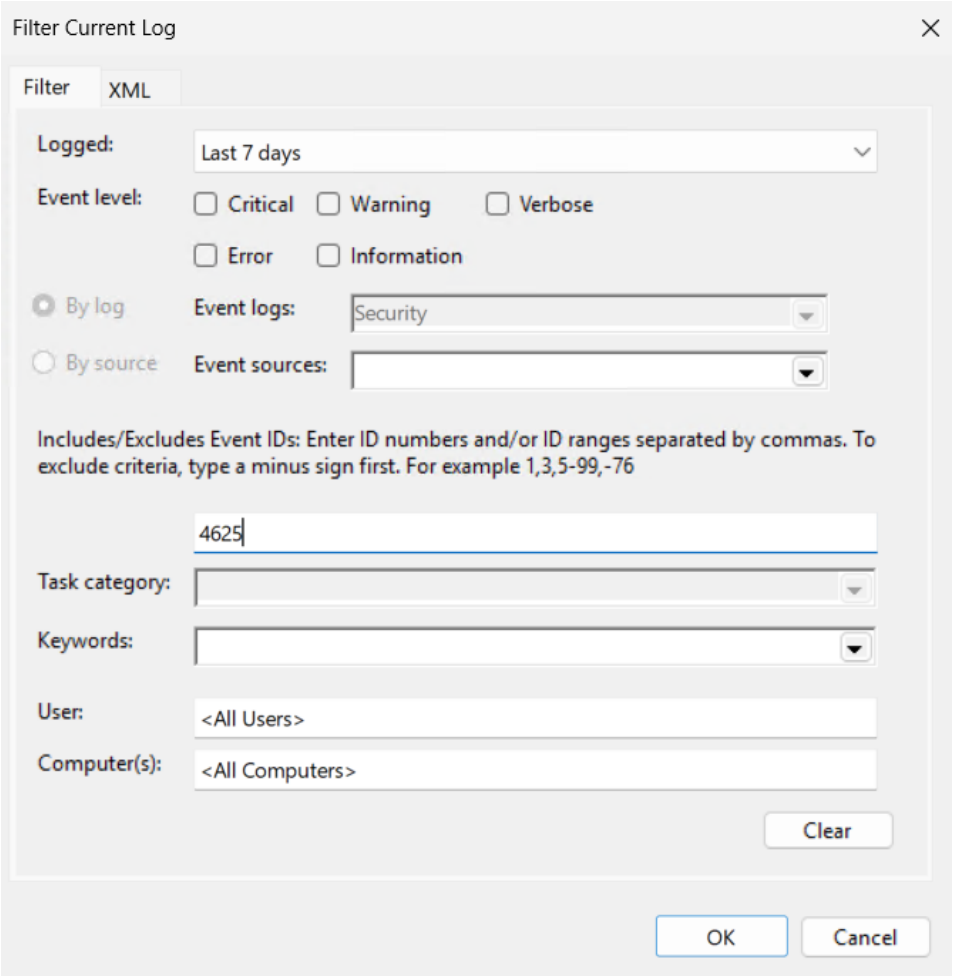

Рисунок 3.59 – Фільтрація журналу за кодом події

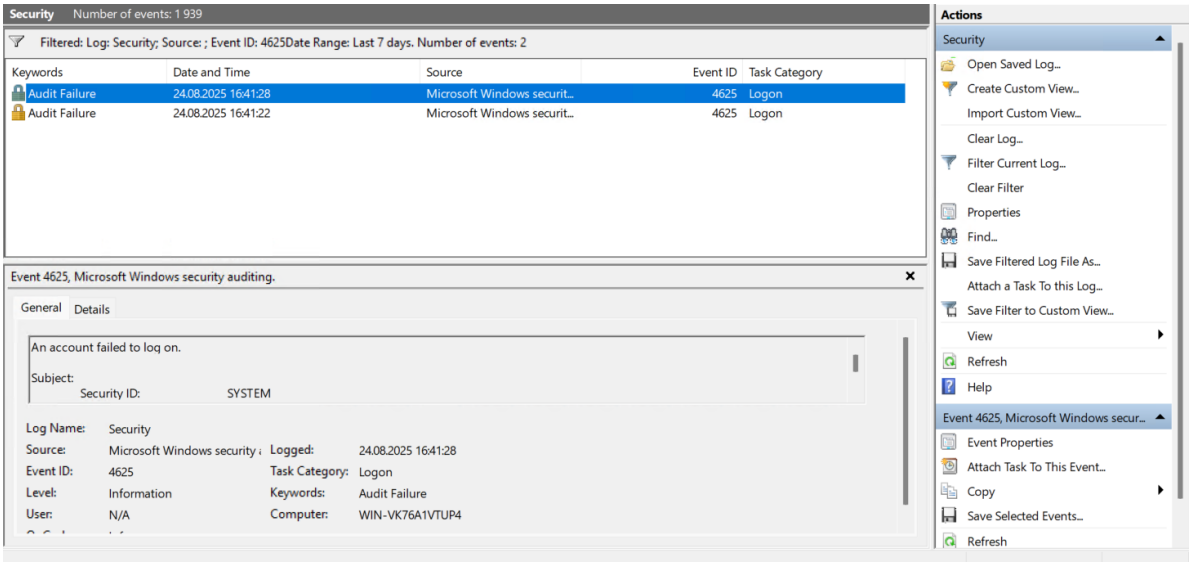

Рисунок 3.60 – Результат фільтрації журналу за кодом події «4625»

Для адміністратора регулярний контроль журналів є основою забезпечення стабільності та захищеності серверної інфраструктури. Систематичний аналіз записів дозволяє не лише виявляти проблеми, а й прогнозувати їх, що підвищує надійність та стійкість роботи корпоративного середовища. Таким чином, журнали подій у Windows виступають невід’ємним інструментом управління інформаційною безпекою та підтримки працездатності серверів.

Лабораторна робота №4
Active Directory у Windows Server 2025

Мета роботи: закріпити практичні навички встановлення та налаштування ролі «Доменні служби Active Directory» у середовищі Windows Server 2025, навчитися створювати та конфігурувати домен, додавати облікові записи користувачів і груп, а також здійснювати аналіз процесів реплікації між контролерами домену для забезпечення надійного функціонування корпоративної мережевої інфраструктури [22-25].

Хід роботи

Завдання 1. Створення та налаштування домену

Перед початком виконання завдань даної практичної роботи запустити розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань попередньої практичної роботи.

Після успішного запуску відкрити «Диспетчер серверів». Для того, щоб створити та налаштувати домен, встановимо нову роль для цього сервера. Тому натискаємо «Управління» – «Додати ролі та компоненти». І за допомогою майстра додавання ролей та компонентів встановлюємо нову роль – «Доменні служби Active Directory». Алгоритм додавання простий та зрозумілий і опрацьований нами детально в попередній практичній роботі (рис. 4.1).

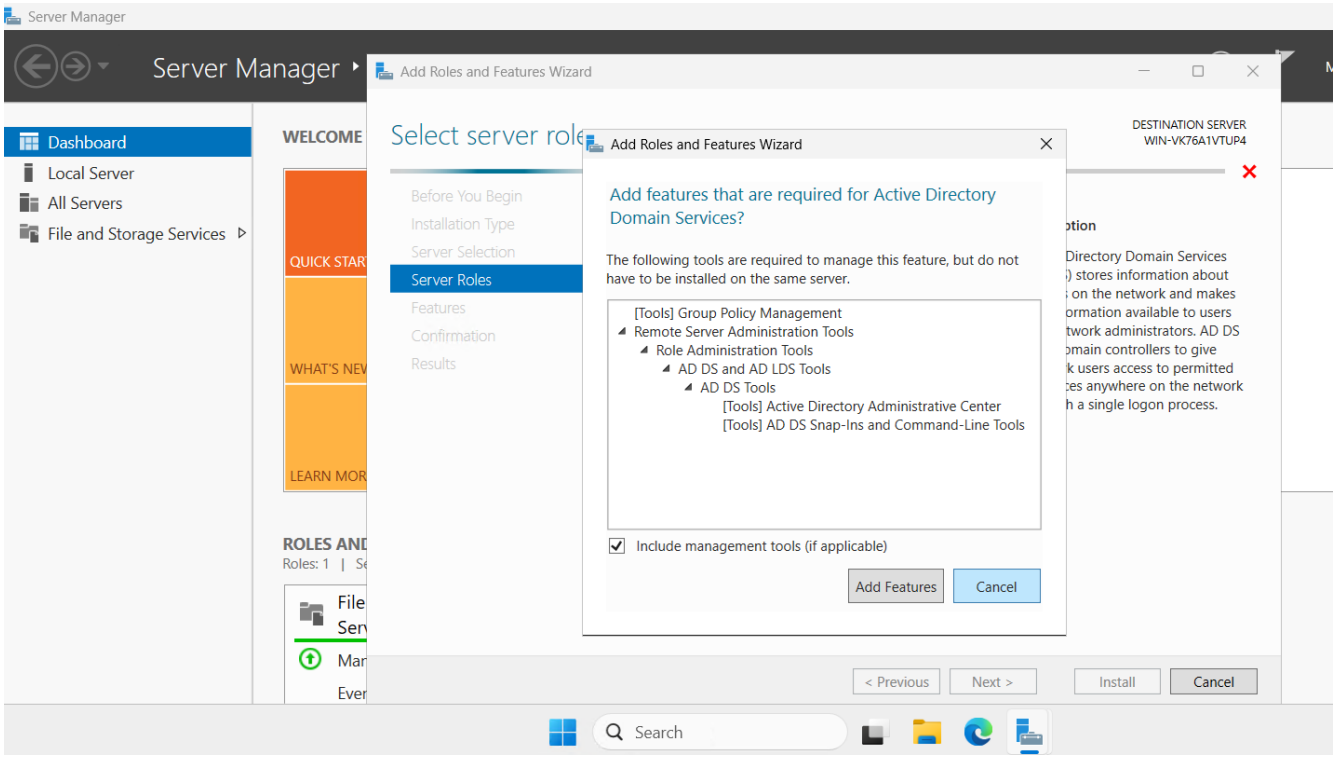

Рисунок 4.1 – Встановлення ролі «Доменні служби Active Directory»

Після вибору потрібної ролі, натискаємо «Далі» і так переключаємося до вікна підтвердження, де підтверджуємо встановлення вибраної ролі та чекаємо завершення цього процесу (рис. 4.2).

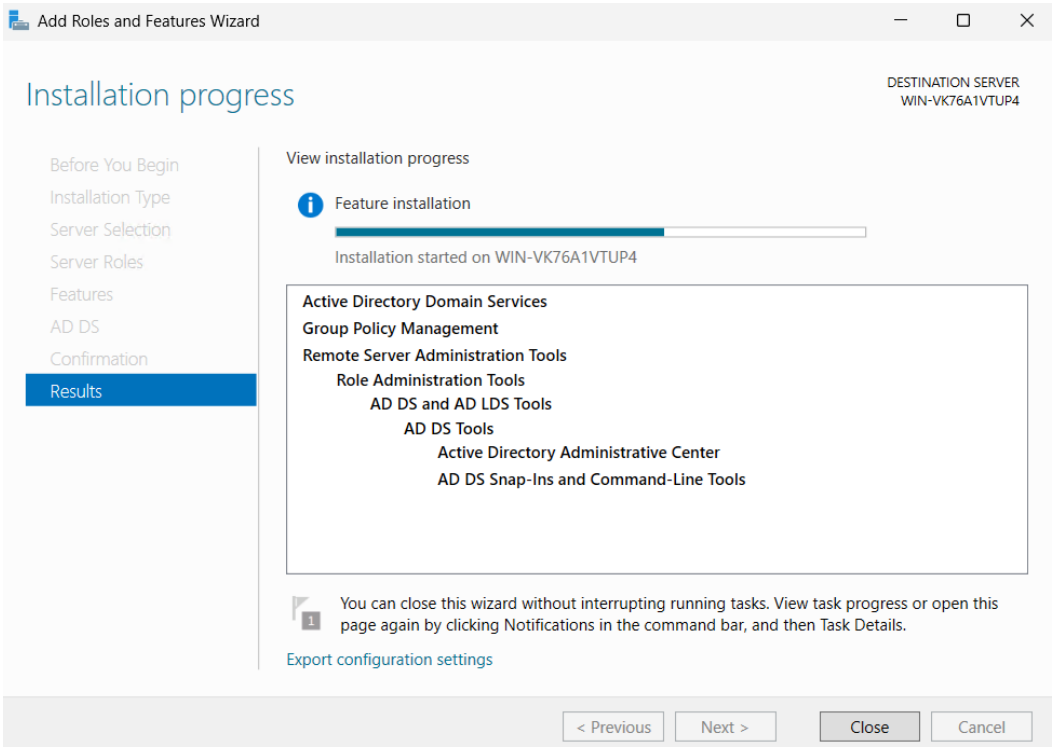

Рисунок 4.2 – Процес встановлення вибраних ролей та компонентів (ролі «Доменні служби Active Directory»)

Коли завершився процес встановлення вибраної ролі та компонентів, то з’явиться повідомлення «Підвищити роль цього сервера до рівня контролера домена» – натискаємо на нього (рис. 4.3).

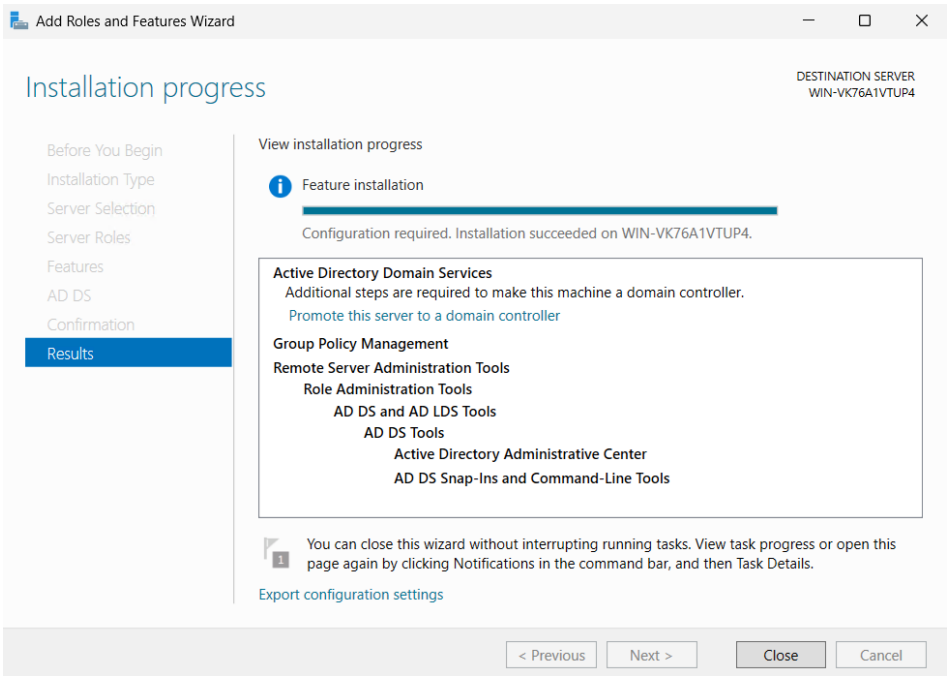

Рисунок 4.3 – Повідомлення «Підвищити роль цього сервера до рівня контролера домена»

Після натиснення відкривається «Майстер налаштування доменних служб Active Directory» (рис. 4.4).

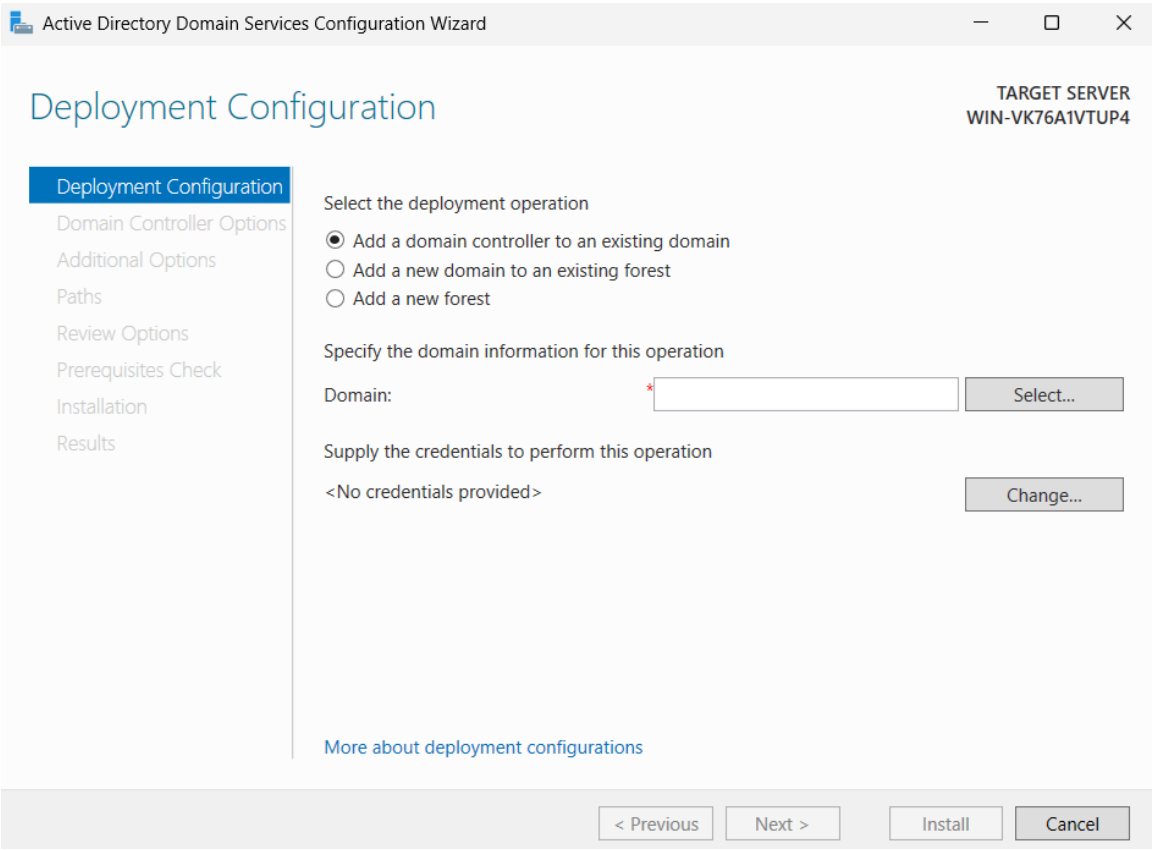

Рисунок 4.4 – «Майстер налаштування доменних служб Active Directory»

В цьому вікні є можливість обрати один з трьох варіантів:

«Додати контролер домена в існуючий домен» – використовується, якщо домен уже існує, і ви хочете додати ще один контролер.

«Додати новий домен в існуючий ліс» – якщо у нас уже є «ліс» (forest), і ми хочемо створити в ньому новий домен.

«Додати новий ліс» – використовується, коли створюється домен уперше, тобто ще немає ні «лісу», ні домену.

Оскільки, ми створюємо домен уперше, то натискаємо «Додати новий ліс» та вводимо назву домену. Потім натискаємо «Далі» (рис. 4.5).

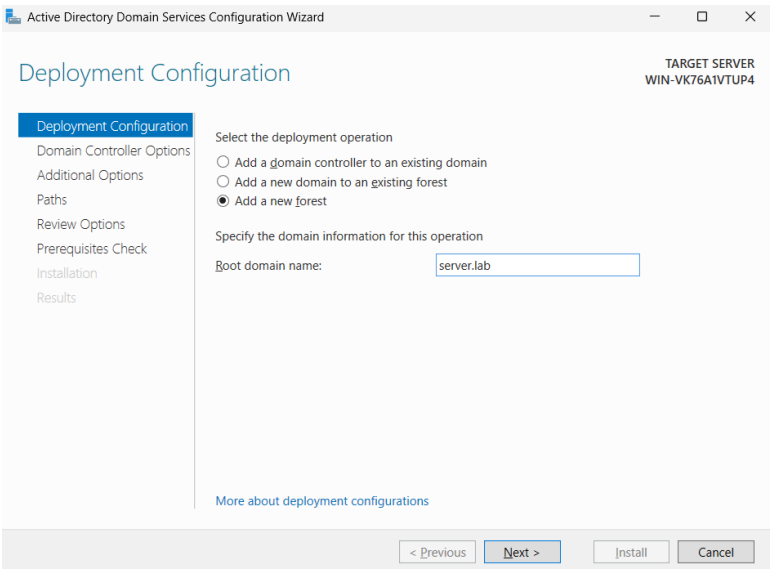

Рисунок 4.5 – Вибір «Додати новий ліс» та введення назви домену

В наступній вкладці вікна все залишаємо без змін, тільки вписуємо пароль для режиму відновлення служб каталогів (DSRM) (рис. 4.6).

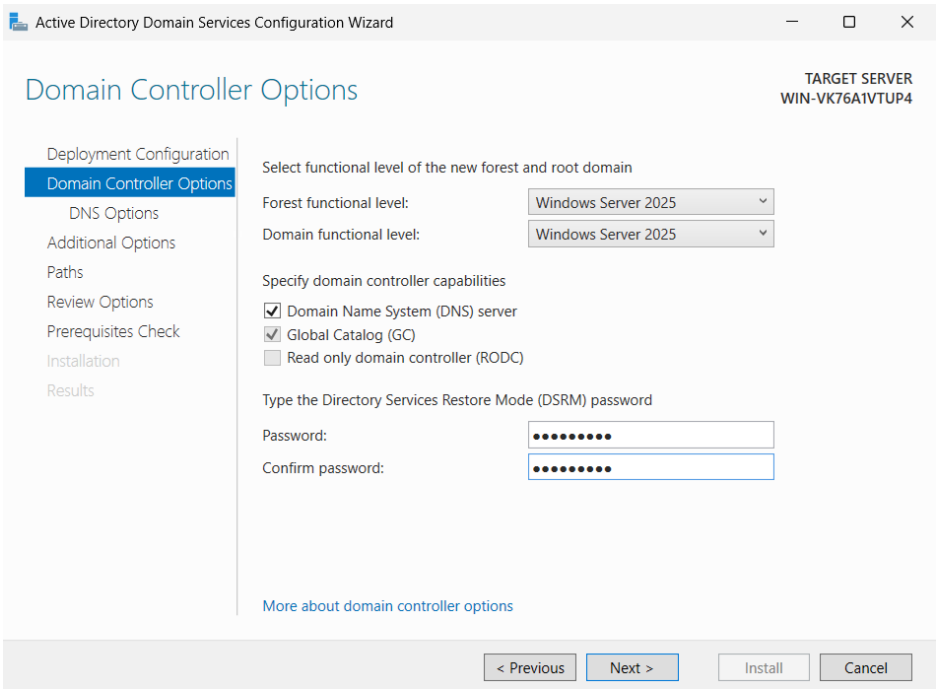

Рисунок 4.6 – «Параметри контролера домена»

У наступних вікнах «Параметри DNS» та «Додаткові параметри» просто натискаємо «Далі». На вкладці «Шляхи» теж залишаємо все без змін і з параметрами за-замовчуванням (рис. 4.7).

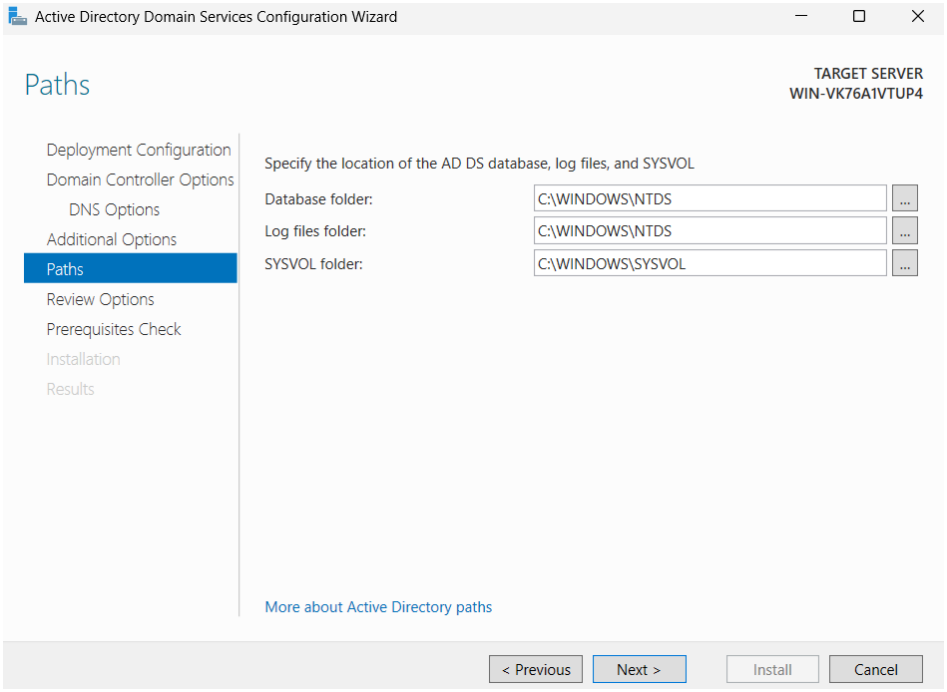

Рисунок 4.7 – Вкладка «Шляхи»

Після цього на вкладці «Переглянути параметри» перевіряємо введені дані. Якщо все вірно натискаємо «Далі». Після цього, якщо все відповідає вимогам, відбувається встановлення. За успішним встановленням слідує перезавантаження сервера (рис. 4.8).

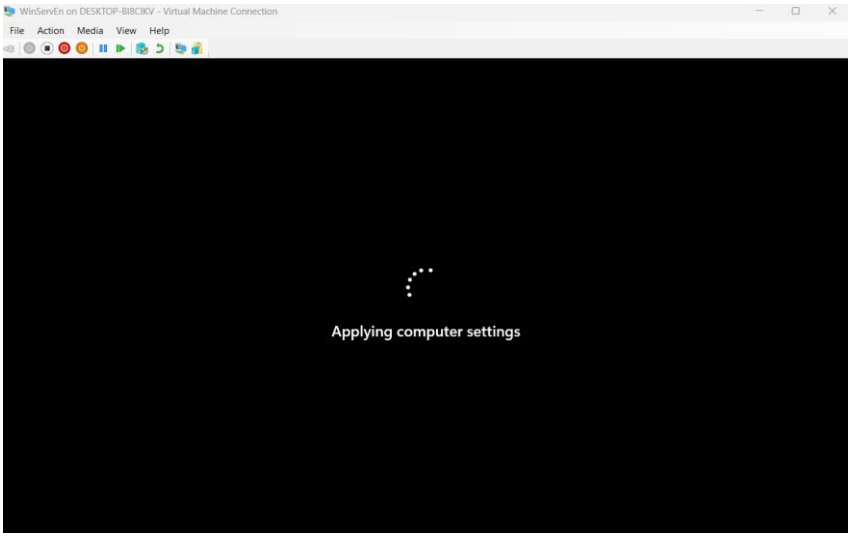

Рисунок 4.8 – Перезавантаження сервера

Після перезавантаження сервера, можемо зайти в «Диспетчер серверів», далі – «Інструменти», знайти там «Користувачі і комп'ютери Active Directory».

Якщо вікно відкривається і ми бачимо наш домен (наприклад, server.lab) з контейнерами – значить домен створений і сервер став контролером. Отже, створення та налаштування домену завершено.

Завдання 2. Додавання користувачів і груп

Для цього натискаємо «Диспетчер серверів» – «Інструменти» – «Користувачі та комп'ютери Active Directory» (рис. 4.9).

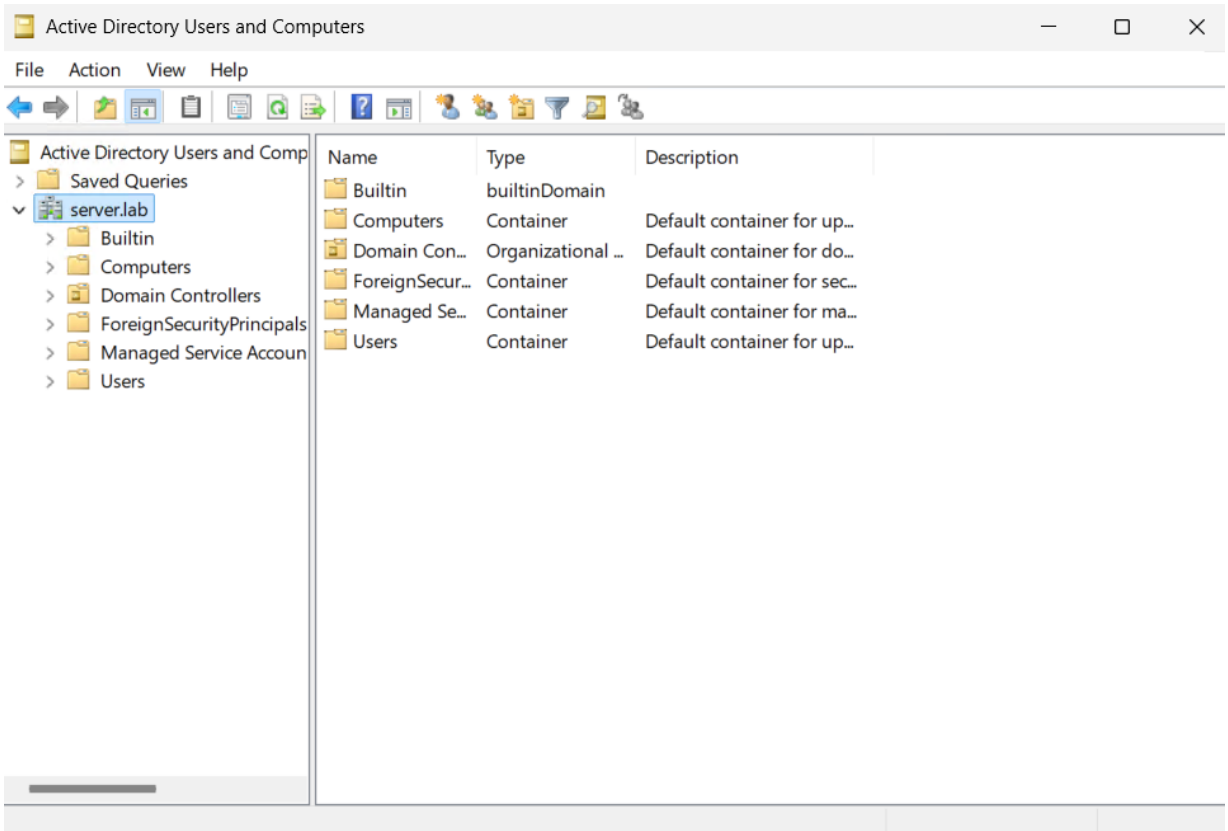

Рисунок 4.9 – Вікно «Користувачі та комп'ютери Active Directory»

Коли відкриється вікно, ми бачимо наш домен (server.lab) і стандартні контейнери:

Users (Користувачі) – тут знаходяться стандартні облікові записи та групи.

Computers (Комп'ютери) – сюди за замовчуванням потрапляють комп'ютери, приєднані до домену.

Domain Controllers (Контролери домена) – тут відображаються сервери з роллю контролера домену.

Щоб створити нового користувача можемо натиснути на піктограму «Створення нового користувача» або ж натиснути ПКМ по контейнеру «Users» – «Створити» – «Користувач» (рис. 4.10).

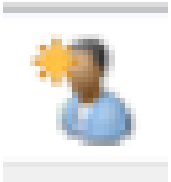

Рисунок 4.10 – Піктограма «Створення нового користувача»

Відкривається «Майстер створення нового користувача». Тут заповнюємо всі необхідні поля, такі, як «Ім'я», «Прізвище», «Ініціали» та найважливіше – «Ім'я входу користувача», коли це зроблено натискаємо «Далі» (рис. 4.11).

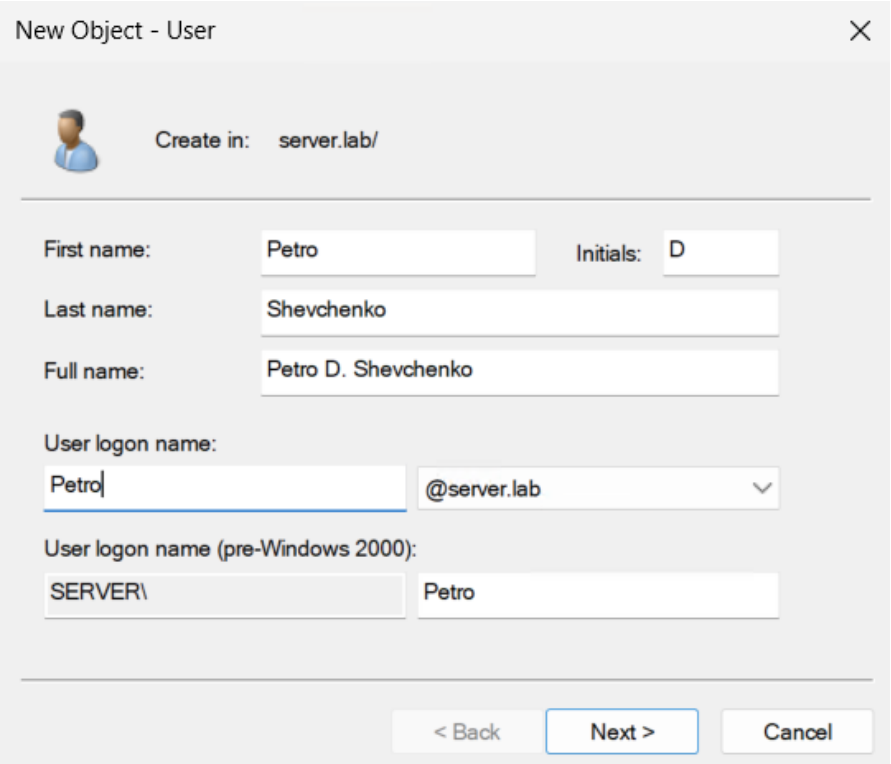

Рисунок 4.11 – Майстер створення нового користувача

На наступній вкладці відбувається налаштування пароля. Створюємо і записуємо новий пароль, повторюємо його та встановлюємо прапорець «Вимагати зміни пароля при наступному вході в систему» – це зумовлено

налаштуваннями безпеки. Інші прапорці залишаємо без змін в цьому випадку (рис. 4.12).

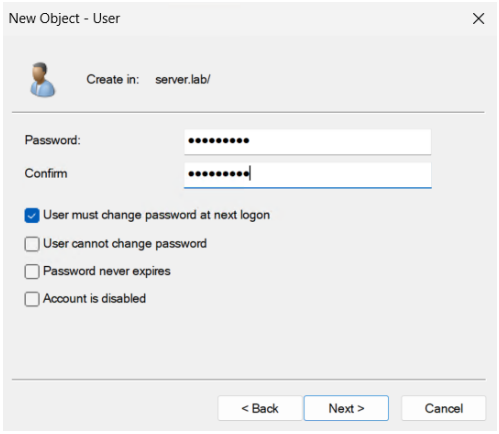

Рисунок 4.12 – Налаштування пароля для створюваного користувача

Далі натискаємо «Готово» – новий користувач створений.

Для створення групи користувачів алгоритм дій подібний – натискаємо відповідну піктограму або ПКМ по контейнеру «Users» – «Створити» – «Група» (рис. 4.13).

Рисунок 4.13 – Піктограма «Створення нової групи»

Відкривається «Майстер створення нової групи». Тут заповнюємо всі необхідні поля, такі, як «Ім’я групи», вибираємо область дій групи – «Локальна в домені» та тип групи – «Безпеки», коли це зроблено натискаємо «ОК» – нова група користувачів створена (рис. 4.14).

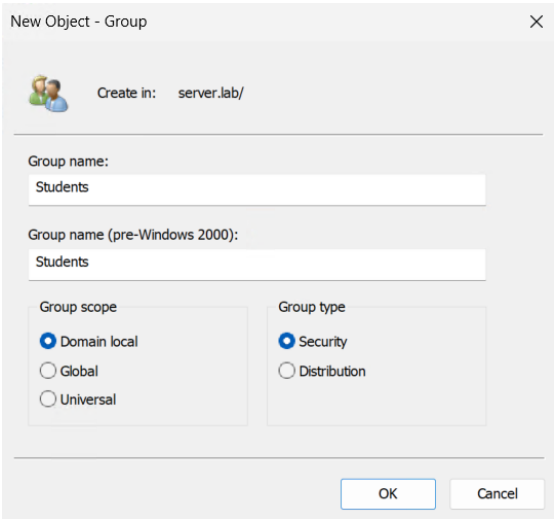

Рисунок 4.14 – Створення нової групи

Для того, щоб додати користувача до групи можна скористатися двома способами. Перший – натиснути на групу ПКМ, далі вибрати «Додати в групу» і у вікні, що відкрилося ввести ім'я користувача, що потрібно додати в цю групу і натиснути «ОК». Другий спосіб – зайти в контейнер «Користувачі», там знайти користувача, якого слід додати до групи, натиснути на нього ПКМ, вибрати «Властивості». У вікні властивостей, що відкрилося обрати «Член груп» – «Додати». Далі ввести назву групи і натиснути «ОК» (рис. 4.15).

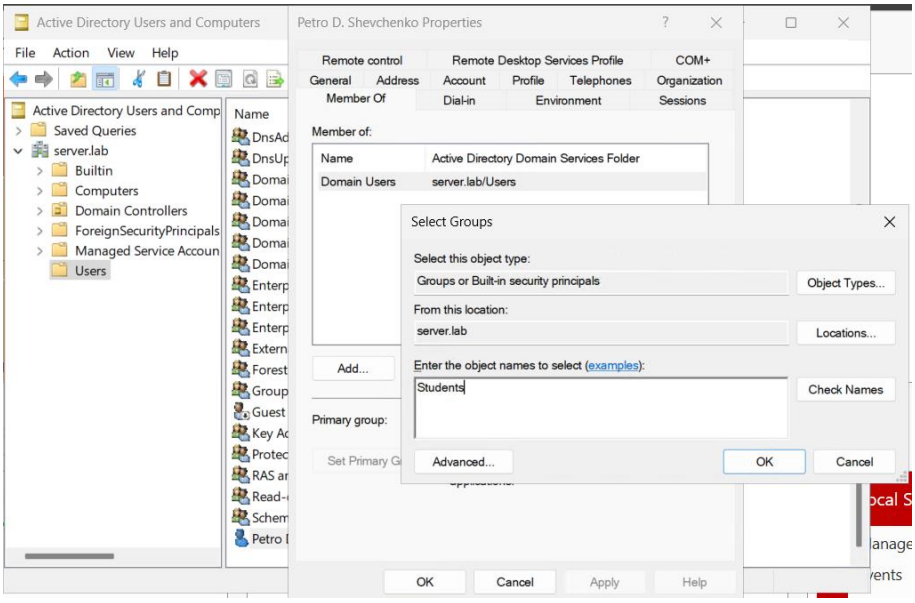

Рисунок 4.15 – Додавання користувача до групи

Після цього у вікні властивостей потрібно натиснути «Застосувати» і «ОК». В результаті цих дій користувач буде доданий до вказаної групи.

Завдання 3. Аналіз реплікації між контролерами домену

Для виконання цього завдання створюємо другу віртуальну машину Windows Server 2025, процес описаний в першій практичній роботі, додаємо роль Active Directory. Приєднуємо її до існуючого домену як додатковий контролер (опція Add a domain controller to an existing domain).

Після цього на основній (першій) машині відкриваємо «Диспетчер серверів», переходимо до «Інструменти» – «Сайти і служби Active Directory».

У дереві бачимо наш сайт за замовчуванням: Default-First-Site-Name (рис. 4.16).

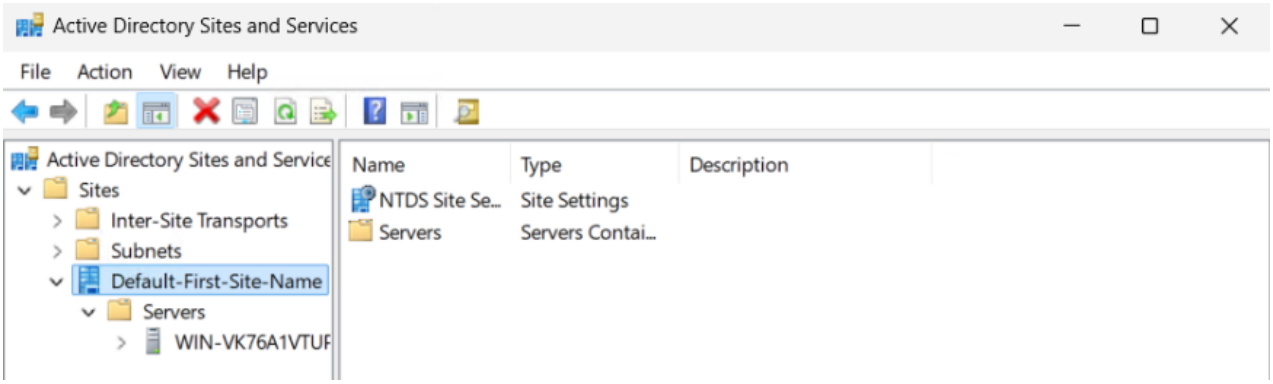

Рисунок 4.16 – Сайти і служби Active Directory

Розгортаємо вузол – «Servers» – бачимо список наших контролерів домену (DC1, DC2). Після цього для перегляду з’єднання реплікації розгортаємо сервер – «NTDS Settings». У правій частині бачимо автоматично створені з’єднання (зв’язки реплікації), це вказує, з ким контролер обмінюється даними.

Для детального аналізу виконуємо примусову реплікацію. Для цього натискаємо ПКМ на з’єднанні, потім «Виконати реплікацію зараз», підтверджуємо дію.

Якщо реплікація успішна, отримуємо повідомлення «Active Directory Domain Services has replicated the connections».

Лабораторна робота №5
Групові політики у Windows Server 2025

Мета роботи: ознайомитися з принципами функціонування та адміністрування групових політик у середовищі Windows Server 2025, набути практичних навичок налаштування політик безпеки, зокрема параметрів паролів та обмеження доступу до зовнішніх носіїв, а також опанувати методи діагностики і усунення помилок при застосуванні групових політик у доменній інфраструктурі [26-31].

Хід роботи

Завдання 1. Налаштування політик паролів

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена.

Далі відкриваємо «Диспетчер серверів». Натискаємо «Інструменти» – «Керування груповою політикою» – таким чином відкриваємо інструмент управління політиками (рис. 5.1).

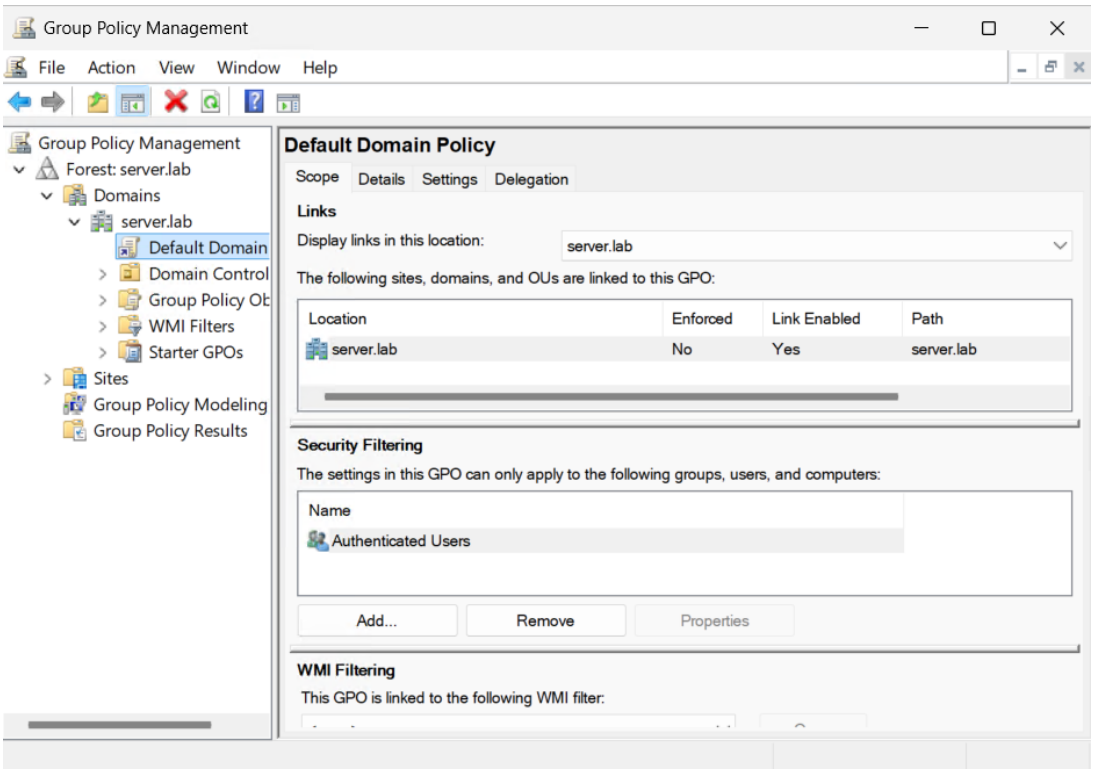

Рисунок 5.1 – Відкрите вікно «Керування груповою політикою»

Після цього відкриваємо дерево зліва: розгортаємо наш домен, вибираємо об’єкт Default Domain Policy (Політика за-замовчуванням для домена). Це саме та політика, яка застосовується для всіх користувачів домену, якщо ми її змінюємо. І далі, щоб налаштувати політику паролів клацаємо правою кнопкою миші по «Default Domain Policy» – «Змінити». Внаслідок цього відкривається редактор групових політик (рис. 5.2).

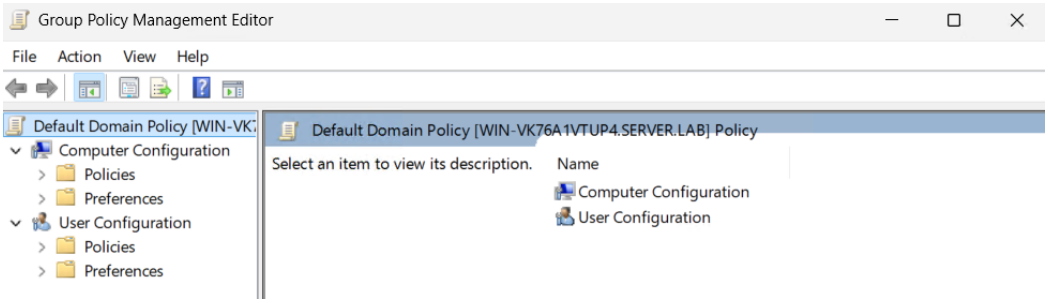

Рисунок 5.2 – Відкрите вікно «Редактор управління груповими політиками»

Далі у редакторі вибираємо «Конфігурація комп'ютера», в наступній вкладці редактора обираємо пункт «Політики» (рис. 5.3).

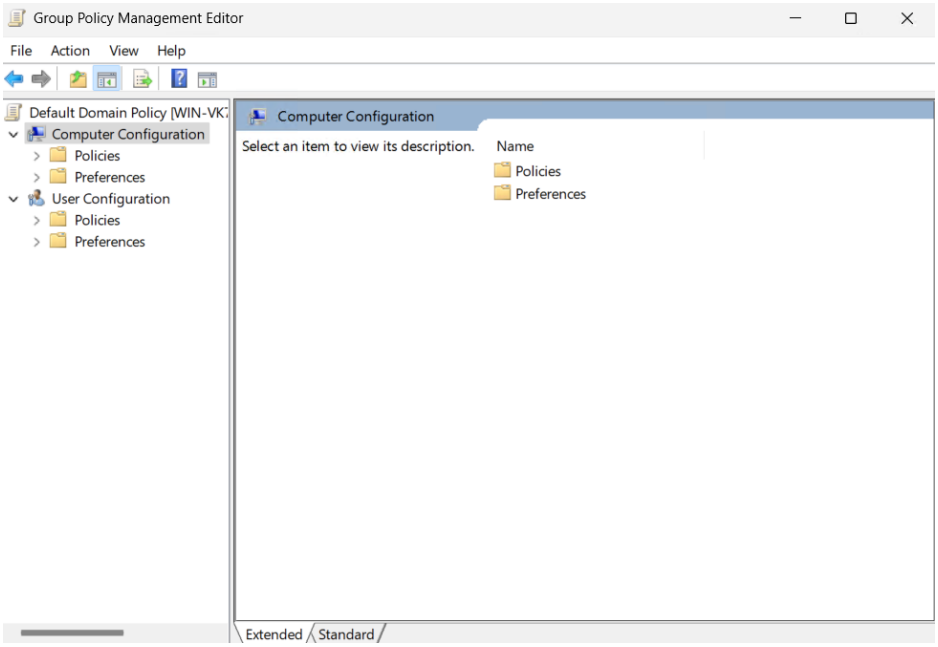

Рисунок 5.3 – Вибір пункту меню «Політики»

Згодом, у новій вкладці обираємо «Конфігурація Windows» (рис. 5.4).

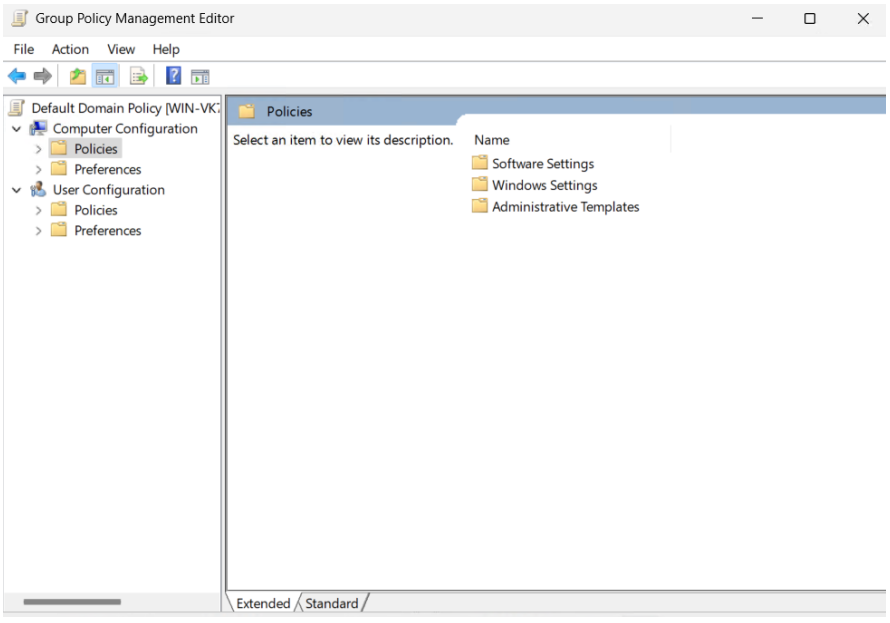

Рисунок 5.4 – Вибір пункту меню «Конфігурація Windows»

Після цього, у вкладці, що відрилася обираємо «Параметри безпеки» (рис. 5.5).

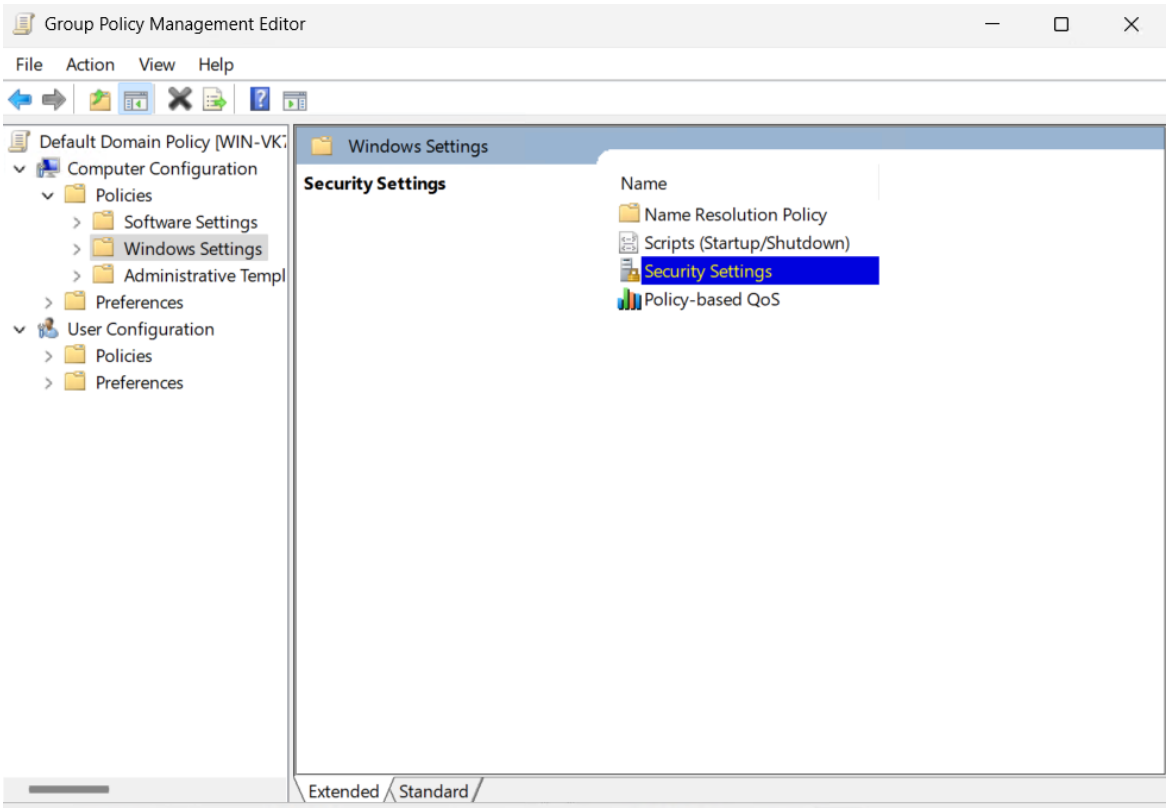

Рисунок 5.5 – Вибір пункту меню «Параметри безпеки»

Далі вибираємо пункт «Політики облікових записів» (рис. 5.6).

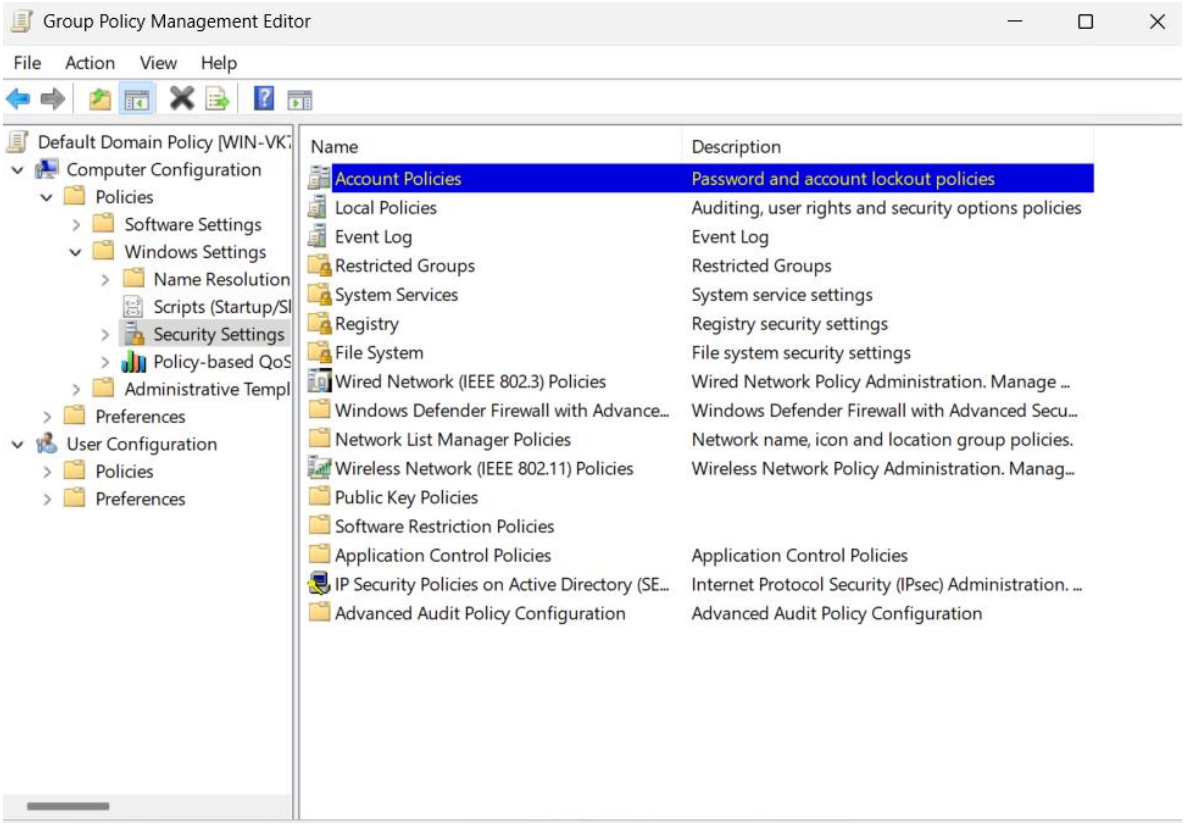

Рисунок 5.6 – Вибір пункту меню «Політики облікових записів»

Після цього відкривається вкладка з потрібним нам для налаштування пунктом меню і видом політик – «Політика паролів» (рис. 5.7-5.8).

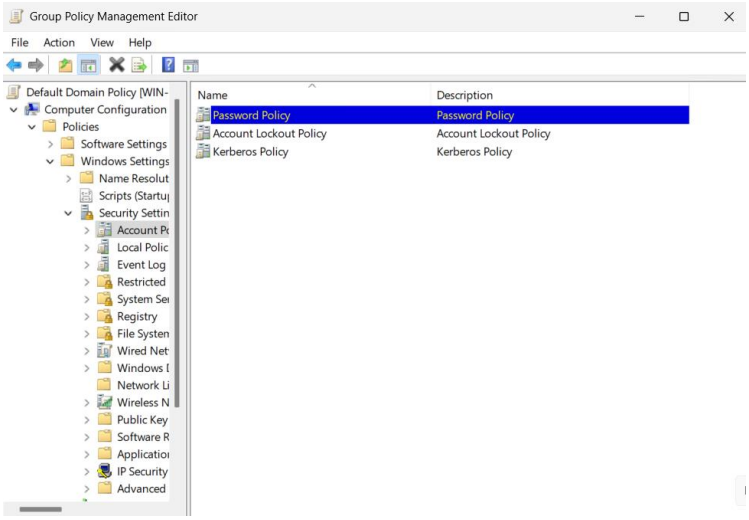

Рисунок 5.7 – Вибір пункту меню «Політика паролів»

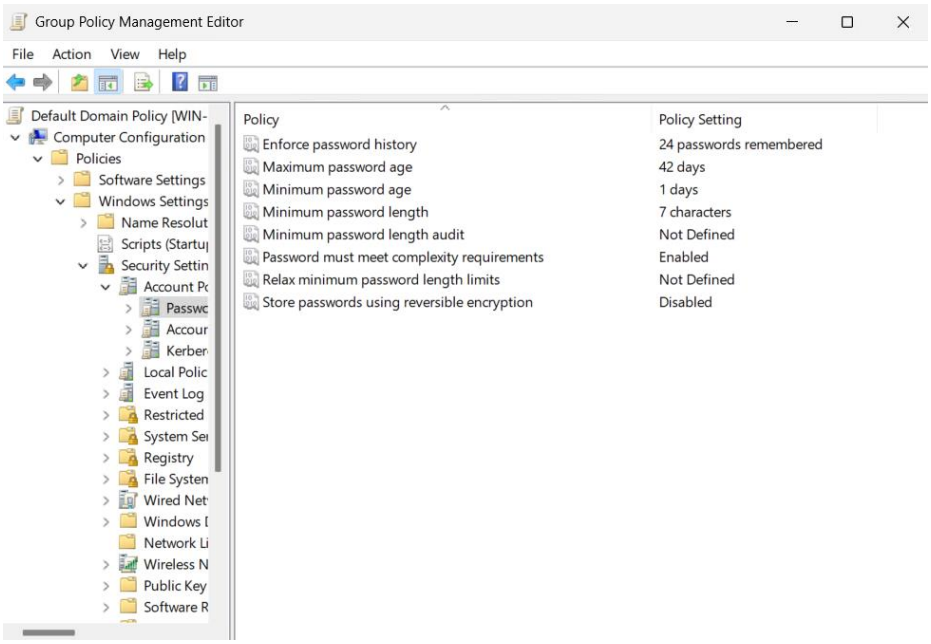

Рисунок 5.8 – Вікно налаштування політики паролів

Тут ми бачимо кілька ключових параметрів:

Вести журнал паролів – скільки паролів зберігається.

Максимальний термін дії пароля – як часто потрібно міняти пароль.

Мінімальний термін дії пароля – через який час після зміни пароль можна змінити знову.

Мінімальна довжина пароля – мінімальна кількість символів.

Пароль повинен відповідати вимогам – вимагає використання великих, малих літер, цифр та символів.

Зберігати паролі використовуючи реверсивне шифрування – даний параметр стосується безпеки та типу шифрування паролів.

Налаштування політики паролів, наприклад, здійснюємо наступним чином: мінімальна довжина пароля – 8 символів; термін дії пароля – 30 днів; вести журнал паролів – 5 останніх; складність пароля – Вимкнено.

Для налаштування певного пункту політики два рази натискаємо на нього лівою кнопкою миші (рис. 5.9-5.10).

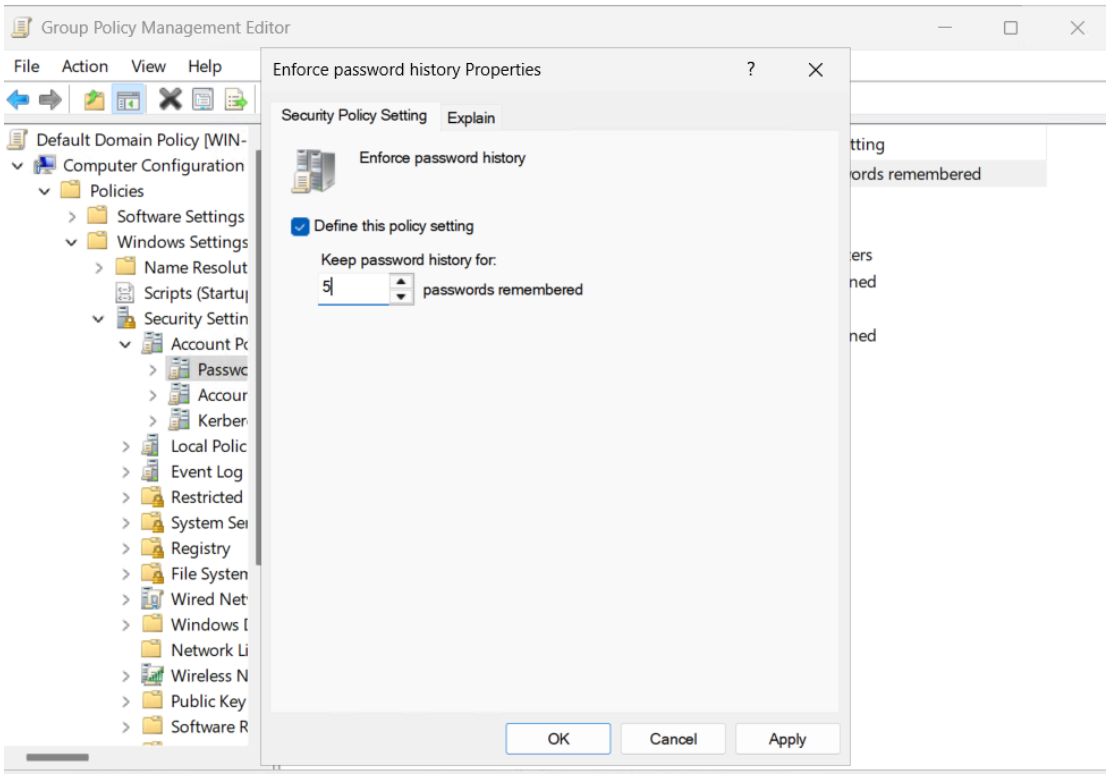

Рисунок 5.9 – Редагування значення пункту «Вести журнал паролів» в редакторі політик

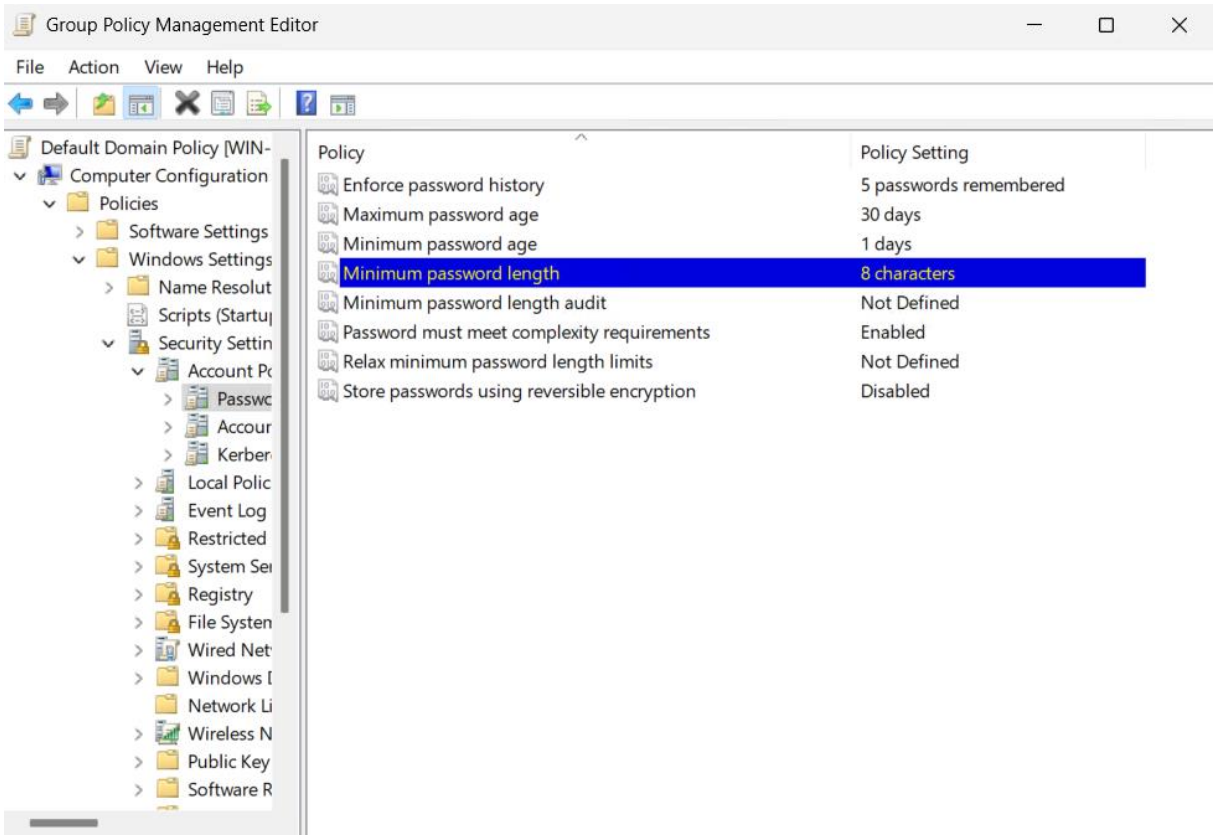

Рисунок 5.10 – Налаштована згідно завдання політика паролів

Коли налаштування проведено закриваємо «Редактор управління груповими політиками». Далі у середовищі Windows PowerShell запускаємо gpupdate /force, щоб зміни вступили в силу (рис. 5.11).

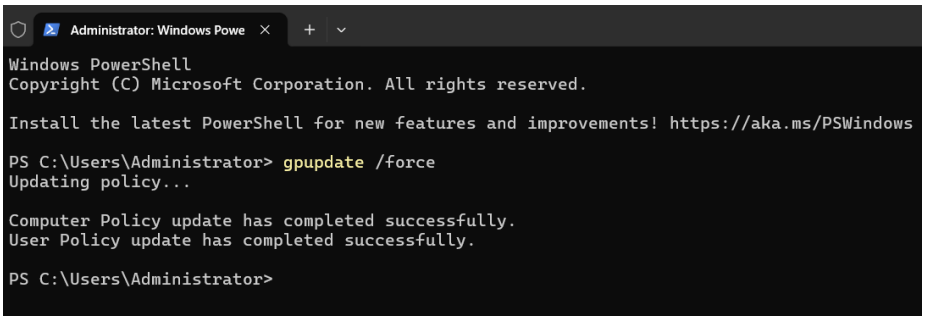

Рисунок 5.11 – Застосування gpupdate /force в середовищі Windows PowerShell

Для того, щоб переконатися в тому, що зміни вступили в силу знову відкриваємо налаштування політики паролів та перевіряємо значення відповідних параметрів. В результаті перевірки переконуємось у правильності здійснених налаштувань.

Завдання 2. Обмеження доступу до USB-носіїв

Для налаштування цієї опції також слід скористатися редактором групових політик. Для цього, як і в попередньому завдання заходимо в нього.

Якщо ми хочемо застосувати обмеження для всіх користувачів домену – редагуємо Default Domain Policy.

Якщо для певної групи або OU (організаційного підрозділу) – створюємо нову політику (натискаємо на назву домену ПКМ та вибираємо «Створити об’єкт групової політики в цьому домені та зв’язати його…») та прив’язуємо її до OU та дотримуємося подальших інструкцій майстра.

У редакторі політик йдемо шляхом: «Конфігурація комп’ютера» – «Політики» – «Адміністративні шаблони» – «Система» – «Доступ до знімних запам’ятовуючих пристроїв» (рис. 5.12-5.13).

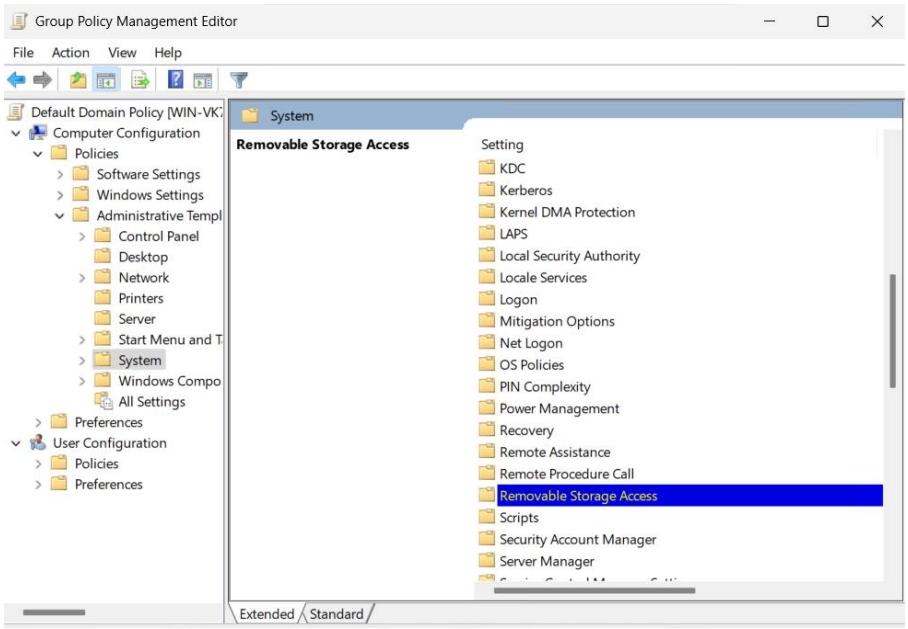

Рисунок 5.12 – Вибір пункту меню «Доступ до знімних запам’ятовуючих пристроїв»

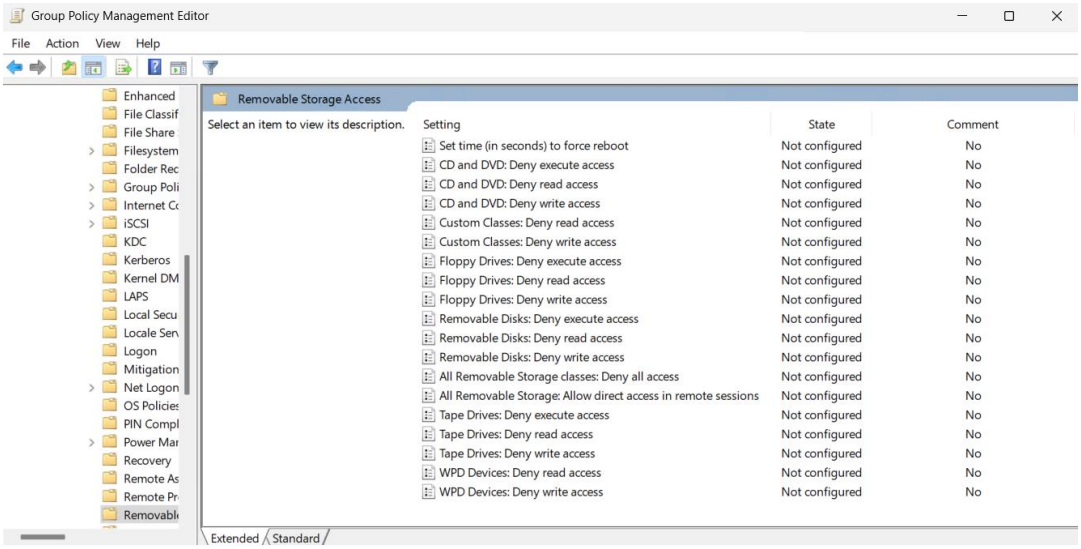

Рисунок 5.13 – Вікно налаштування політик щодо знімних запам’ятовуючих пристроїв

У вікні налаштування політик щодо знімних запам’ятовуючих пристроїв бачимо список параметрів для різних типів пристроїв: CD/DVD, USB-носії, зовнішні диски та інші подібні пристрої.

Ми можемо керувати як читанням, так і записом, вмикаючи та вимикаючи ці параметри для конкретного типу знімних пристроїв.

Для обмеження доступу до USB-носіїв вмикаємо політику «Знімні диски: заборонити читання» – «Увімкнути», а також вмикаємо політику «Знімні диски: заборонити запис» – «Увімкнути». Це означає, що користувачі не зможуть ані читати, ані записувати дані з USB-носіїв (рис. 5.14-5.15).

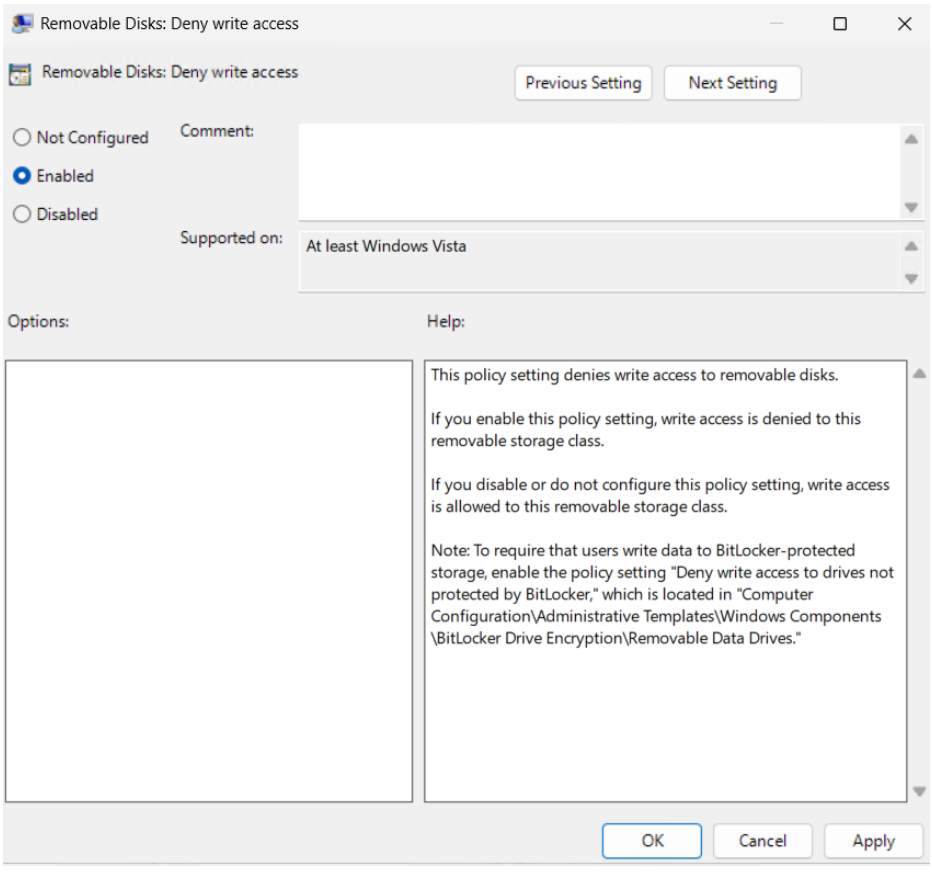

Рисунок 5.14 – Ввімкнення політики «Знімні диски: заборонити запис»

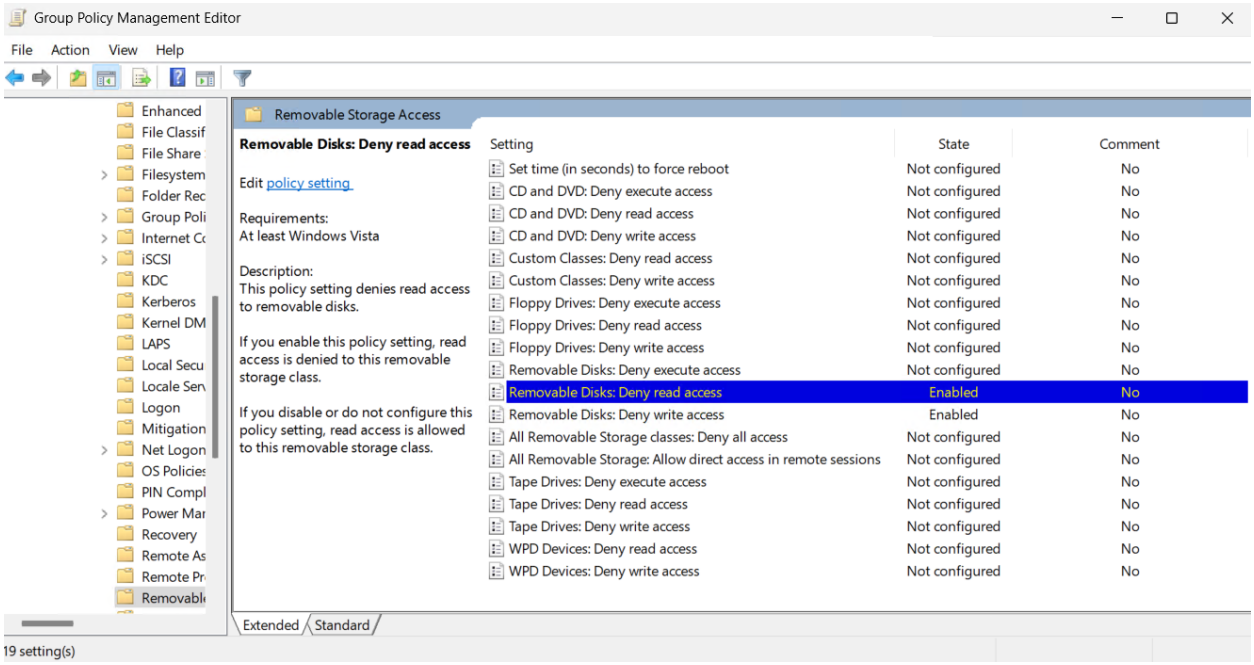

Рисунок 5.15 – Налаштована політика щодо знімних пристроїв для обмеження доступу до USB-носіїв

Коли налаштування проведено закриваємо «Редактор управління груповими політиками». Далі у середовищі Windows PowerShell запускаємо gpupdate /force, щоб зміни вступили в силу.

Для того, щоб переконатися в тому, що зміни вступили в силу знову відкриваємо налаштування політики знімних запам'ятовуючих пристроїв та перевіряємо значення відповідних параметрів політики. В результаті перевірки переконуємось у виконанні здійснених налаштувань.

Завдання 3. Діагностика помилок групових політик

Для діагностики, аналізу та перевірки групових політик є кілька інструментів, які можна застосувати.

Перше – це використання оснастки RSoP (Resultant Set of Policy). Для того, щоб застосувати її натискаємо Win + R та вводимо rsop.msc, натискаємо Enter. В результаті відкривається вікно Resultant Set of Policy (рис. 5.16).

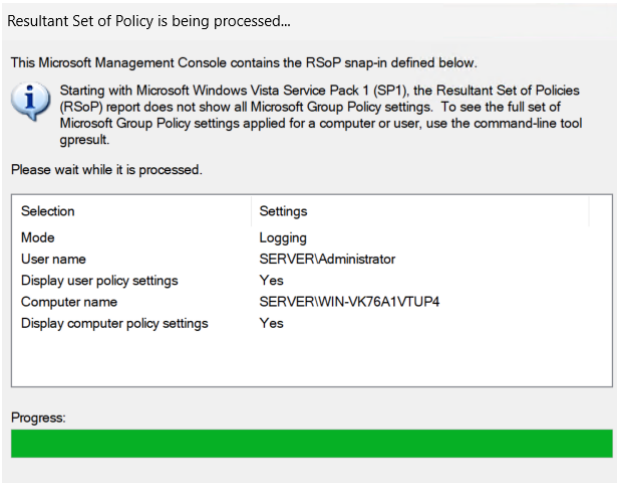

Рисунок 5.16 – Вікно «Resultant Set of Policy»

Система проводить збір інформації та показує нам, які саме політики застосувалися до користувача та комп'ютера та які параметри політик активні. Якщо політика не застосувалася, біля неї буде відображено помилку або попередження.

Наступний інструмент – «Результати групових політик» у «Менеджері управління груповими політиками». Ми відкриваємо «Керування груповими політиками» у «Менеджері серверів». Далі у дереві ліворуч розгортаємо вузол нашого домену. Клацаємо правою кнопкою миші на «Результати групової політики», вибираємо «Майстер результатів групових політик». Запускається майстер, де ми обираємо комп'ютер і користувача, для яких хочемо перевірити застосування політик.

Після завершення майстер формує звіт, про те, які політики застосовані, які були заблоковані та, що найважливіше чи виникли конфлікти між політиками (рис. 5.17-5.19).

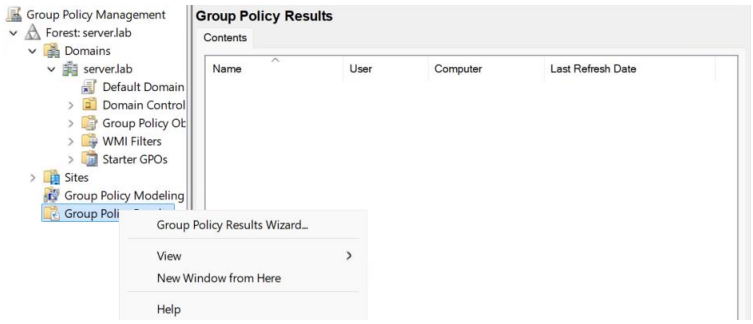

Рисунок 5.17 – Відкриття «Майстра результатів групових політик»

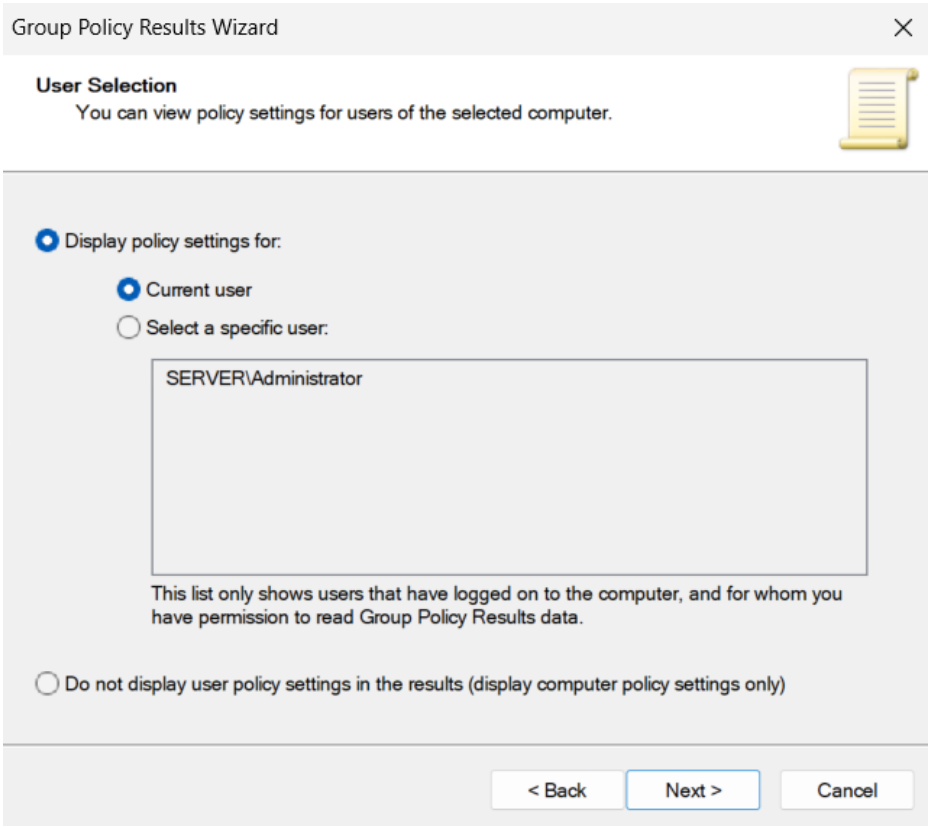

Рисунок 5.18 – Вибір користувача, щодо якого буде створено звіт використання групових політик

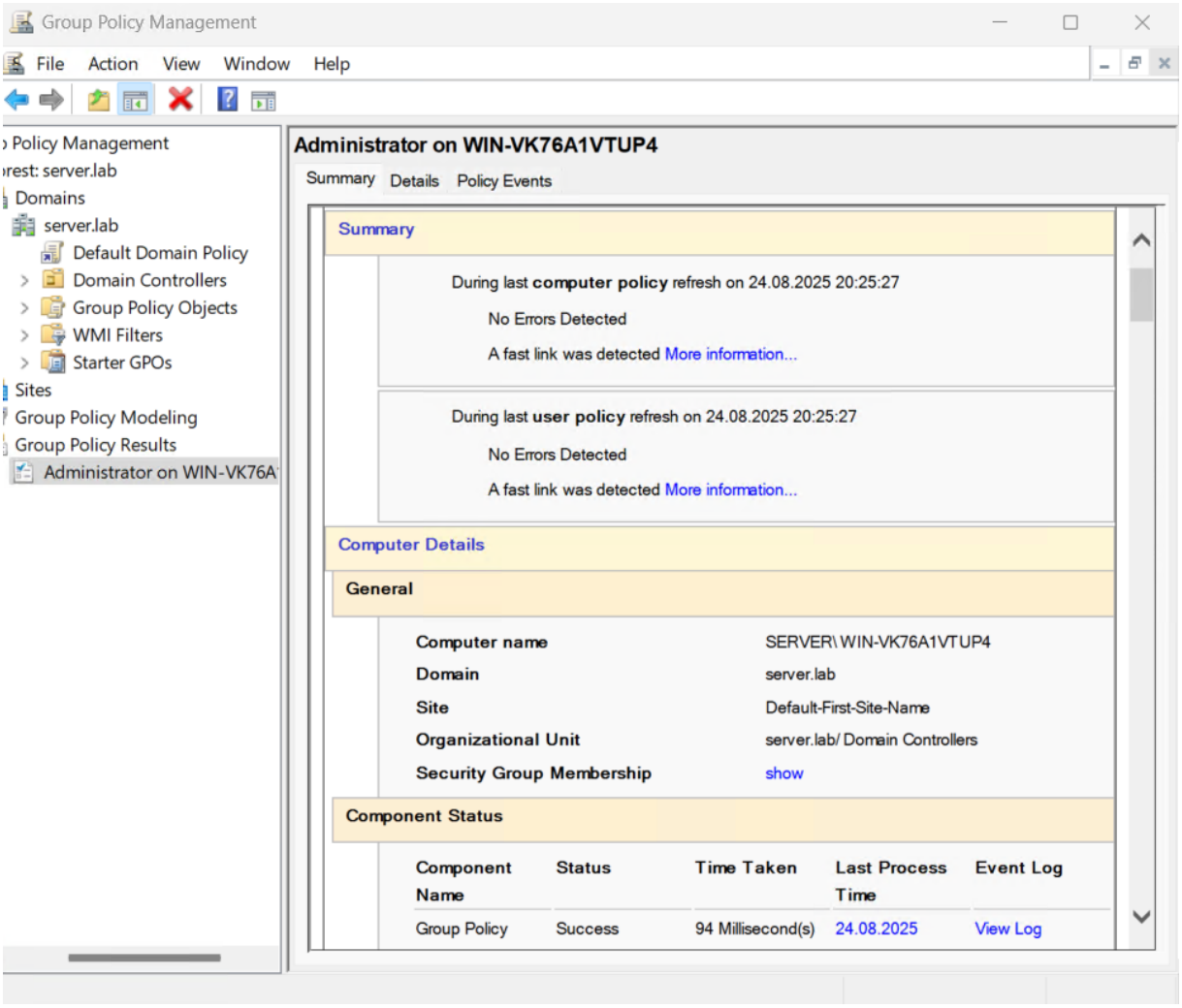

Рисунок 5.19 – Створений звіт використання групових політик

Також можна застосувати «Журнал подій» («Event Viewer») для діагностики роботи та помилок групових політик. Ми відкриваємо «Пуск» – «Адміністративні інструменти» – «Журнал подій» (рис. 5.20).

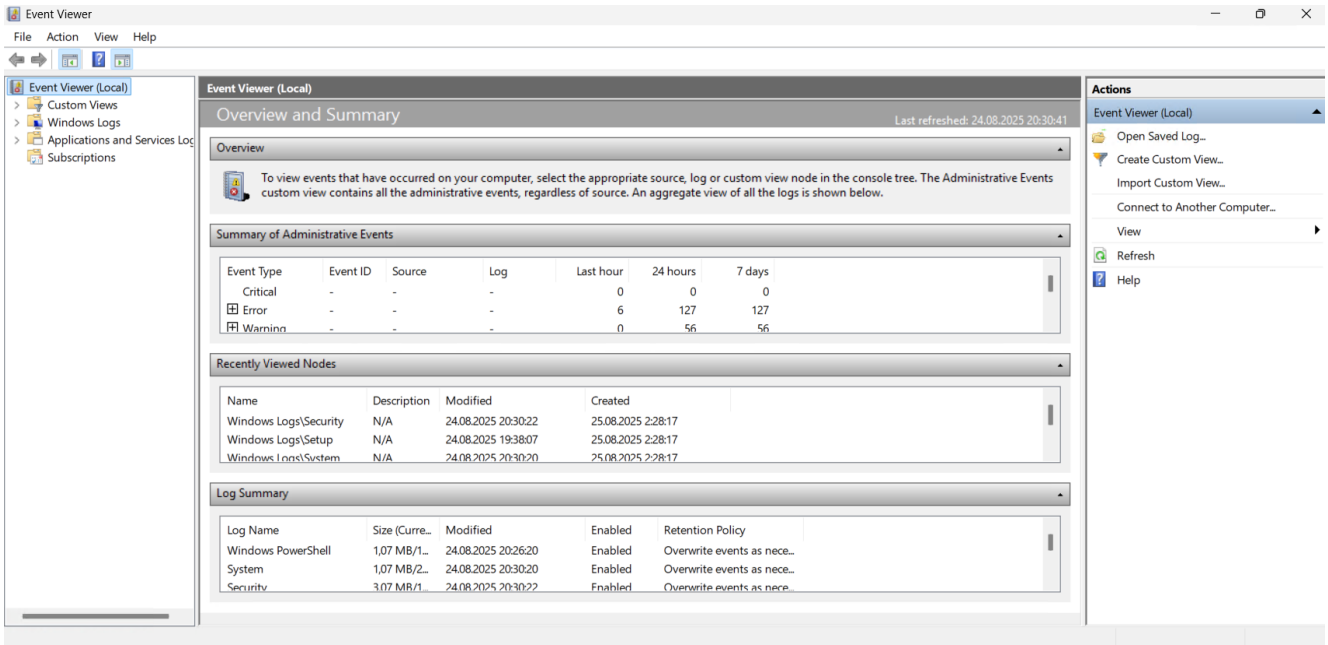

Рисунок 5.20 – Відкритий «Журнал подій»

У дереві ліворуч йдемо шляхом: «Журнали додатків та сервісів» – «Microsoft» – «Windows» – «GroupPolicy» – «Operational» (рис. 5.21).

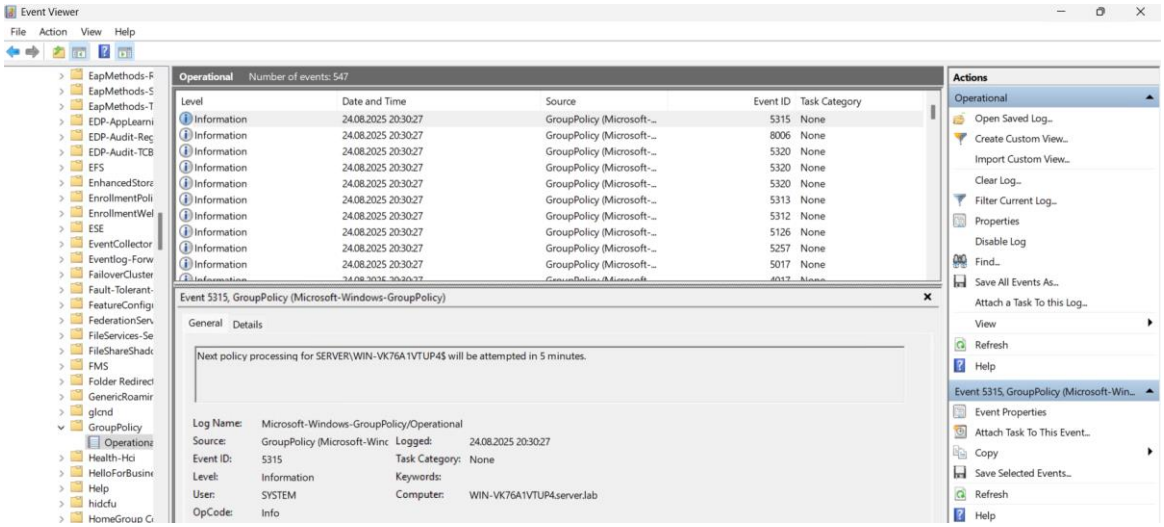

Рисунок 5.21 – Відкритий «Журнал подій» – «Operational»

У цьому журналі бачимо: час і спроби застосування політик, чи успішно вони застосувалися, а також точні повідомлення про помилки (наприклад, «немає доступу до контролера домену» або «політика не знайдена») чи попередження (рис. 5.22).

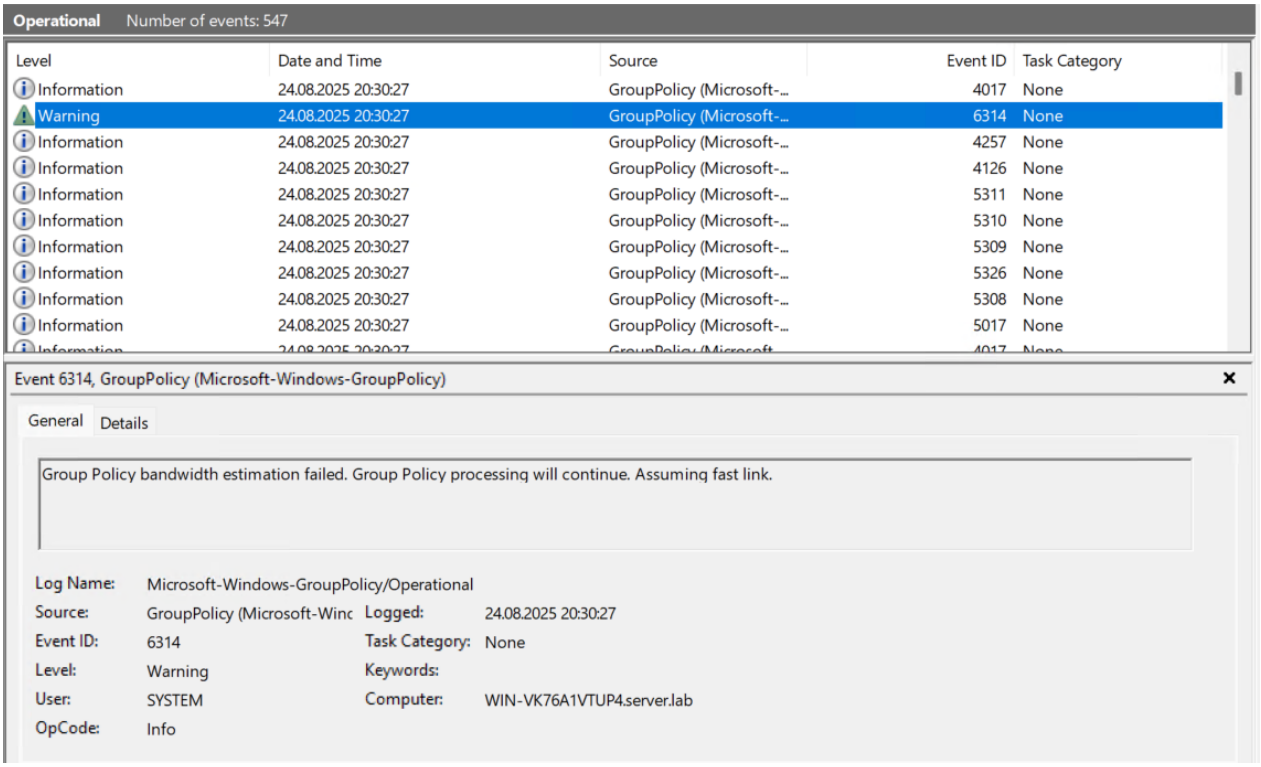

Рисунок 5.22 – Приклад попередження в журналі «Operational» щодо застосування групових політик

Для того, щоб точно знайти помилки, варто скористатися фільтром поточного журналу, вибравши відповідні категорії подій – «Помилка» та «Критичне» (рис. 5.23).

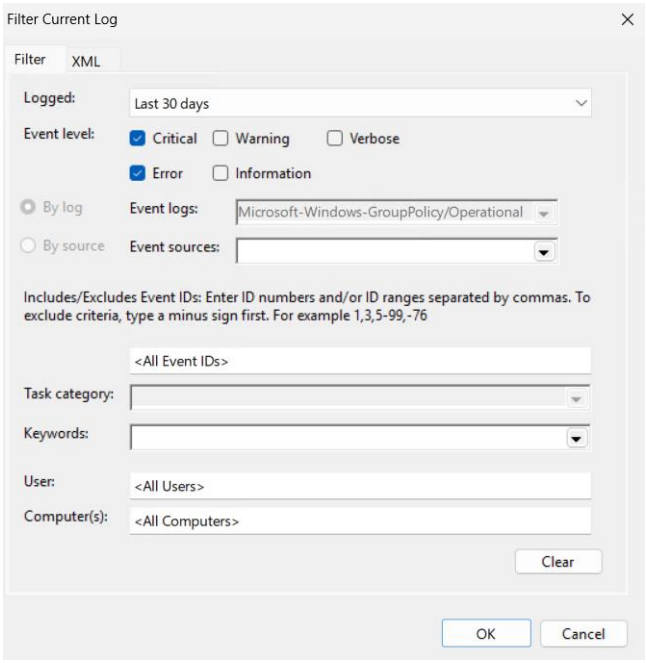

Рисунок 5.23 – Створення фільтру для пошуку та діагностики помилок політик

Якщо в результаті журнал буде пустий, це означає, що помилок немає. В іншому випадку будуть показані помилки та їхні властивості, які і слід детально проаналізувати та виправити.

Також для діагностики та перевірки помилок групових політик можна виконати перевірку послідовності застосування політик. Для цього переходимо в «Управління груповою політикою», там можемо відкрити потрібний OU (організаційний підрозділ). Далі вибираємо вкладку «Наслідування групових політик» (рис. 5.24).

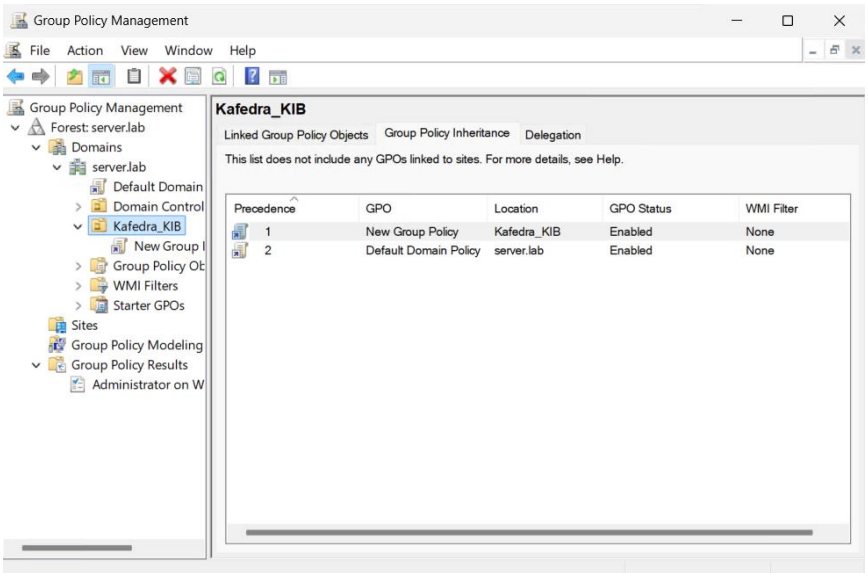

Рисунок 5.24 – Вкладка «Наслідування групових політик»

Тут бачимо порядок застосування політик: яка з них має вищий пріоритет і яка може перекривати інші. Якщо політика не працює – перевіряємо, чи не перекривається вона іншою, адже це може бути однією з причин помилки групової політики.

Лабораторна робота №6
Налаштування DNS у Windows Server 2025

Мета роботи: ознайомитися з принципами роботи служби доменних імен (DNS) у середовищі Windows Server 2025, набути практичних навичок зі створення та налаштування прямої та зворотної зони DNS, дослідити механізми кешування DNS-запитів, а також виконати діагностику та усунення можливих помилок у функціонуванні служби [33].

Хідроботи

Завдання 1. Створення прямої та зворотної зони DNS

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань першої практичної роботи.

Для роботи з DNS та створення прямої та зворотної зони DNS відкриваємо «Диспетчер DNS», який попередньо встановлюємо через «Додавання ролей та компонентів» – додавання ролі «DNS-сервер». Вікдриття робиться наступним чином: відкриваємо «Диспетчер серверів», переходимо до пункту меню «Інструменти» і там шукаємо та вибираємо «DNS» (рис. 6.1).

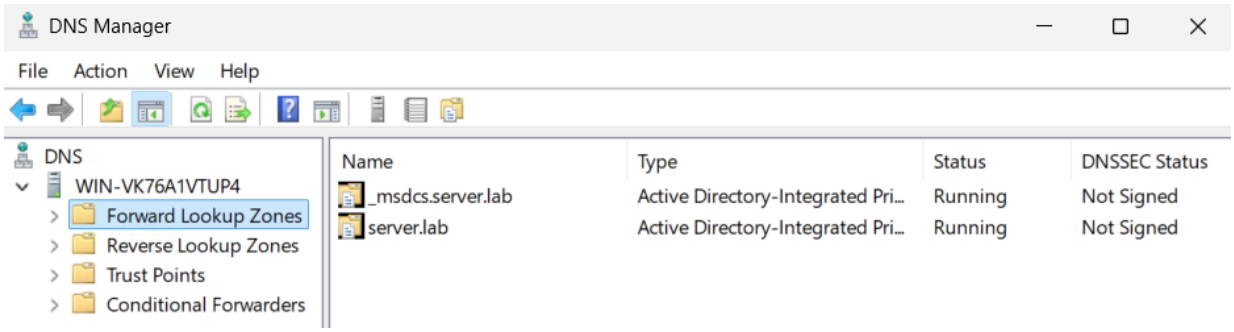

Рисунок 6.1 – Відкритий «Диспетчер DNS»

Після цього створюємо пряму зону DNS. Для цього у дереві зліва розгортаємо наш сервер DNS. Клацаємо правою кнопкою миші на «Прямі зони пошуку» – обираємо «Створити нову зону…» (рис. 6.2).

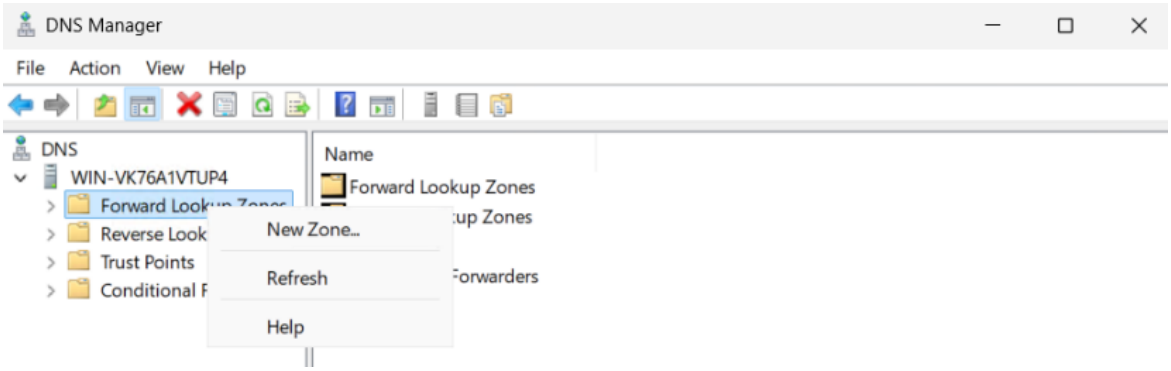

Рисунок 6.2 – Початок створення прямої зони DNS

Внаслідок цих дій запускається «Майстер створення нової зони», у вікні, що відкрилося натискаємо «Далі» (рис. 6.3).

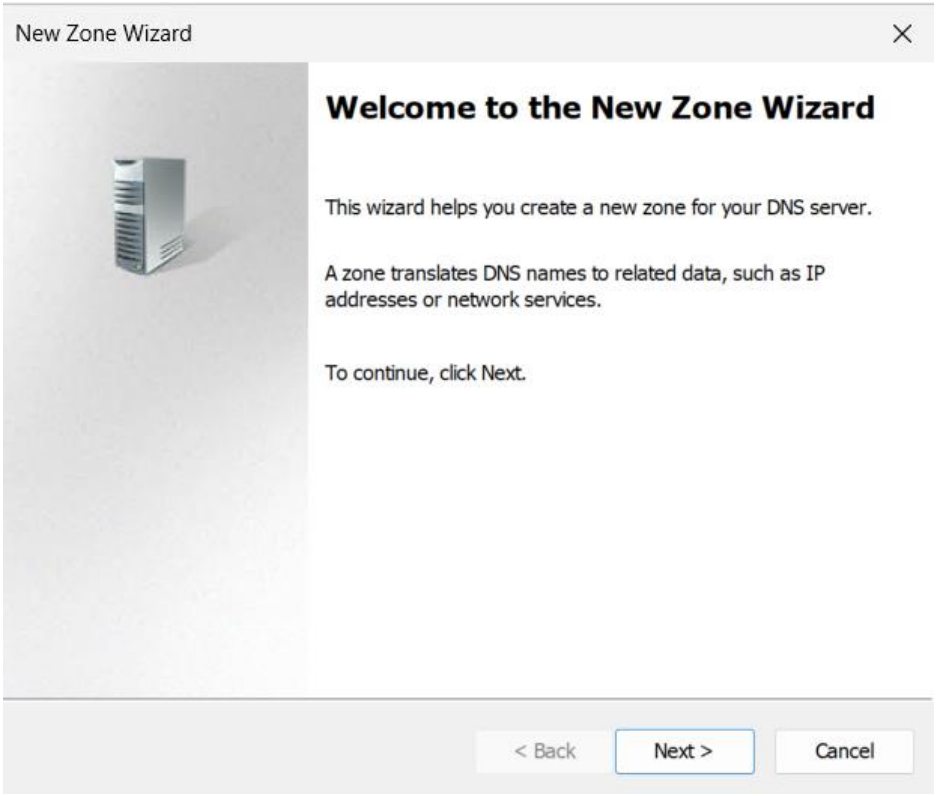

Рисунок 6.3 – «Майстер створення нової зони»

В наступній вкладці «Майстра створення нової зони» обираємо тип зони – «Основна зона». Якщо сервер є частиною домену, залишаємо галочку «Зберігати зону в Active Directory» (а в нашому випадку це так і є) і тиснемо «Далі» (рис. 6.4).

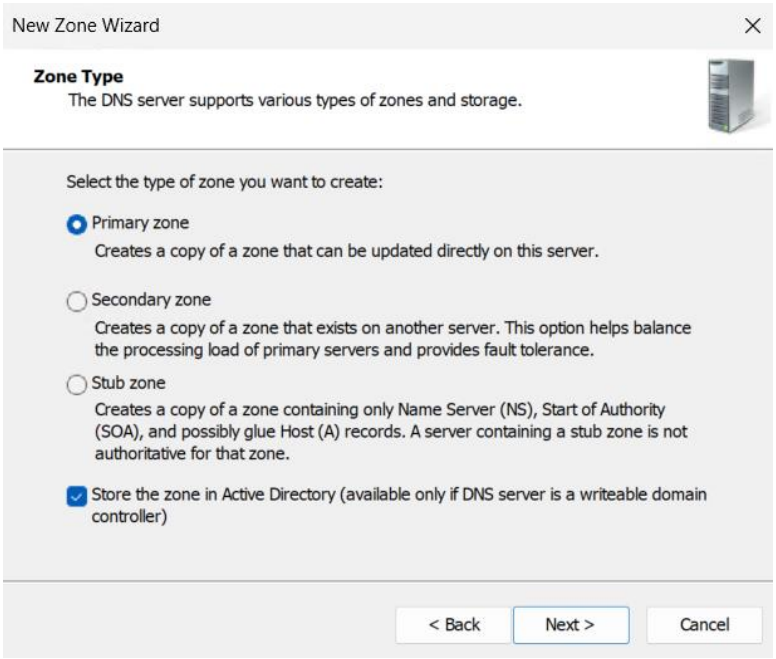

Рисунок 6.4 – Вибір типу зони DNS

Після цього, в іншій вкладці обираємо область реплікації – «Для всіх серверів DNS у домені» і тиснемо «Далі» (рис. 6.5).

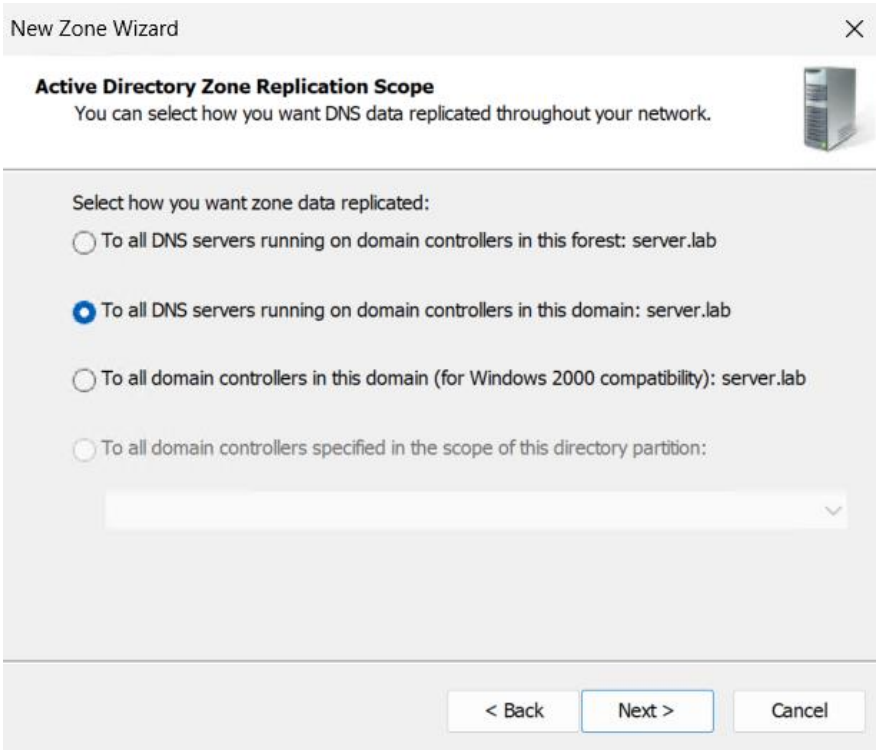

Рисунок 6.5 – Вибір області реплікації зони DNS

Коли вибір області реплікації виконано, вводимо ім’я зони, наприклад, «server_dns_forward_zone» і натискаємо «Далі» (рис. 6.6).

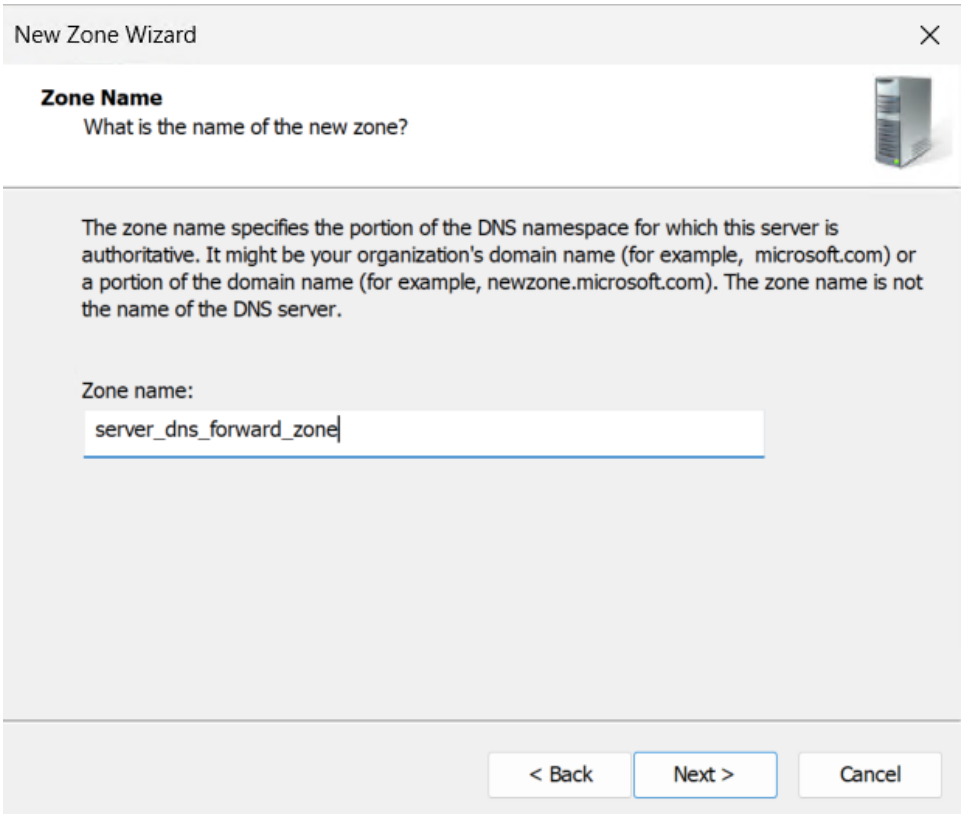

Рисунок 6.6 – Надання імені прямій зоні DNS

Коли надано ім’я, вибираємо спосіб оновлення зони DNS – «Дозволити лише захищені динамічні оновлення» – це оптимальний вибір з точки зору безпеки та функціональності і натискаємо «Далі» (рис. 6.7).

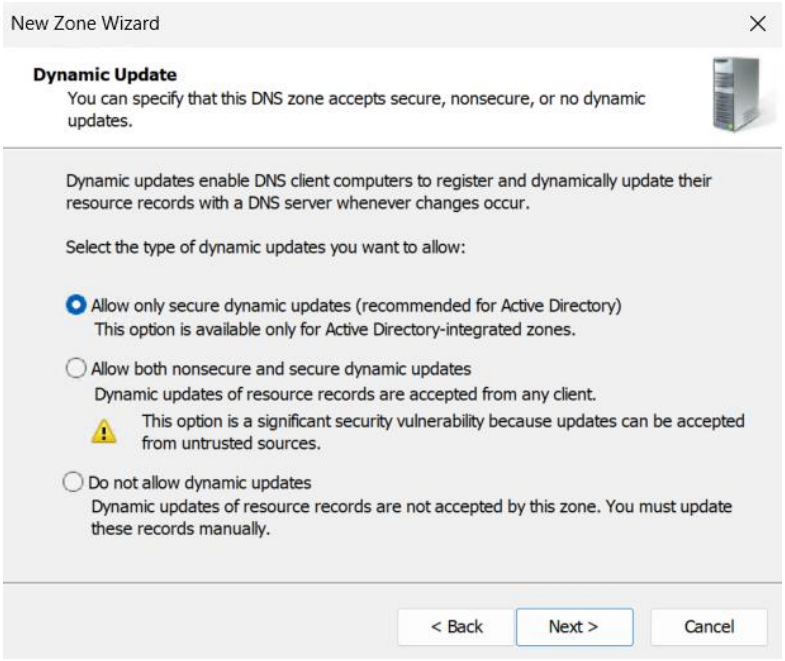

Рисунок 6.7 – Вибір способу оновлення прямої зони DNS

Далі на останній вкладці «Майстра створення нової зони» натискаємо «Готово» і в результаті цього пряма зона DNS створена (рис. 6.8).

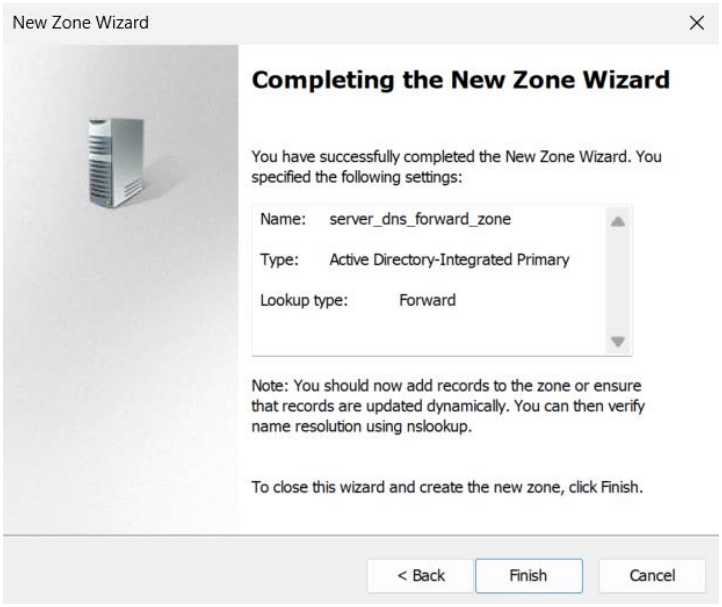

Рисунок 6.8 – Завершення створення прямої зони DNS

Щоб створити зворотну зону DNS здійснюємо подібні дії. У дереві зліва розгортаємо наш сервер DNS. Клацаємо правою кнопкою миші на «Зворотні зони пошуку», далі обираємо «Створити нову зону». Відкривається «Майстер створення нової зони», в першій вкладці натискаємо «Далі». Потім обираємо тип зони – «Основна зона» – «Далі». Далі обираємо реплікацію (як у прямій зоні). Після цього починаються деякі відмінності від прямої зони DNS, оскільки у наступній вкладці з'являється вибір «Зона зворотного пошуку IPv4» або «Зона зворотного пошуку IPv6». Ми обираємо IPv4 та натискаємо «Далі» (рис. 6.9).

Рисунок 6.9 – Вибір типу IP-адрес для створюваної зворотної зони DNS

Після цього, вводимо ідентифікатор мережі. Наприклад, якщо мережа, в якій працює сервер – 172.30.243.0 /24, то вводимо «172.30.243.» і тиснемо «Далі» (рис. 6.10).

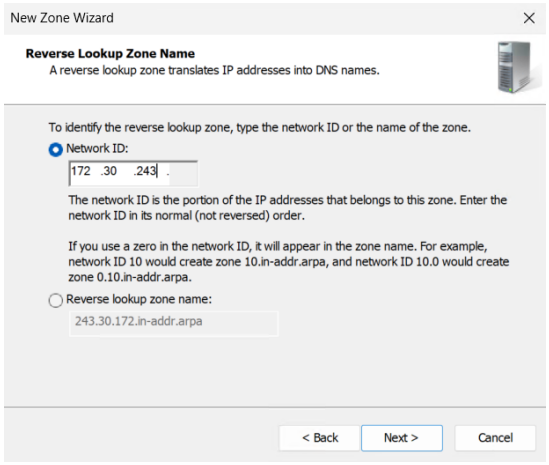

Рисунок 6.10 – Надання ідентифікатора мережі для зворотної зони DNS

Після цього вибираємо тип оновлень. Залишаємо «Дозволити лише захищені динамічні оновлення» (рис. 6.11).

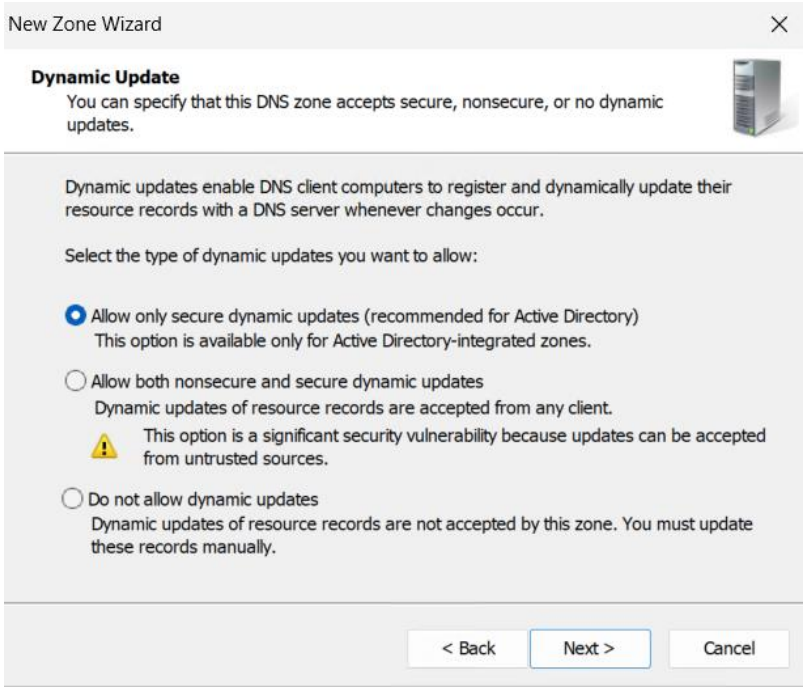

Рисунок 6.11 – Вибір типу оновлень для зворотної зони DNS

В останній вкладці тиснемо «Готово» і як наслідок зворотна зона DNS створена (рис. 6.12).

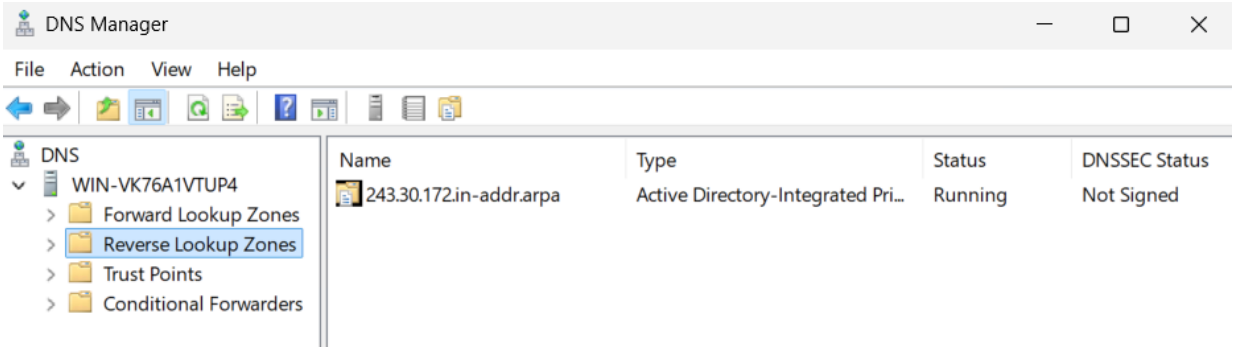

Рисунок 6.12 – Створена зворотна зона DNS

Завдання 2. Аналіз роботи кешування DNS

Для аналізу кешування DNS на сервері запускаємо «Диспетчер DNS». У лівій панелі обираємо наш сервер. Розгортаємо вузол «Кеш-пам'ять DNS». Тут бачимо записи, які сервер тимчасово зберіг після звернення до зовнішніх ресурсів. Кеш дозволяє швидше відповідати на повторні запити, не звертаючись щоразу до зовнішніх DNS-серверів.

Для перевірки кешування на сервері відкриваємо «Командний рядок» і виконуємо команду: «nslookup google.com». В результаті цього DNS-сервер отримає IP-адресу від зовнішнього DNS і збереже її у кеші. Далі виконуємо ту саму команду ще раз і тепер відповідь прийде значно швидше, бо сервер бере дані з кешу. Повертаємось у «Диспетчер DNS» – «Кеш-пам'ять DNS». Тут має з'явитися домен google.com та його підзаписи. Щоб не заходити в «Командний рядок» можна в «Диспетчер DNS» натиснути «Дії» – «Запустити NSLOOKUP» (рис. 6.13).

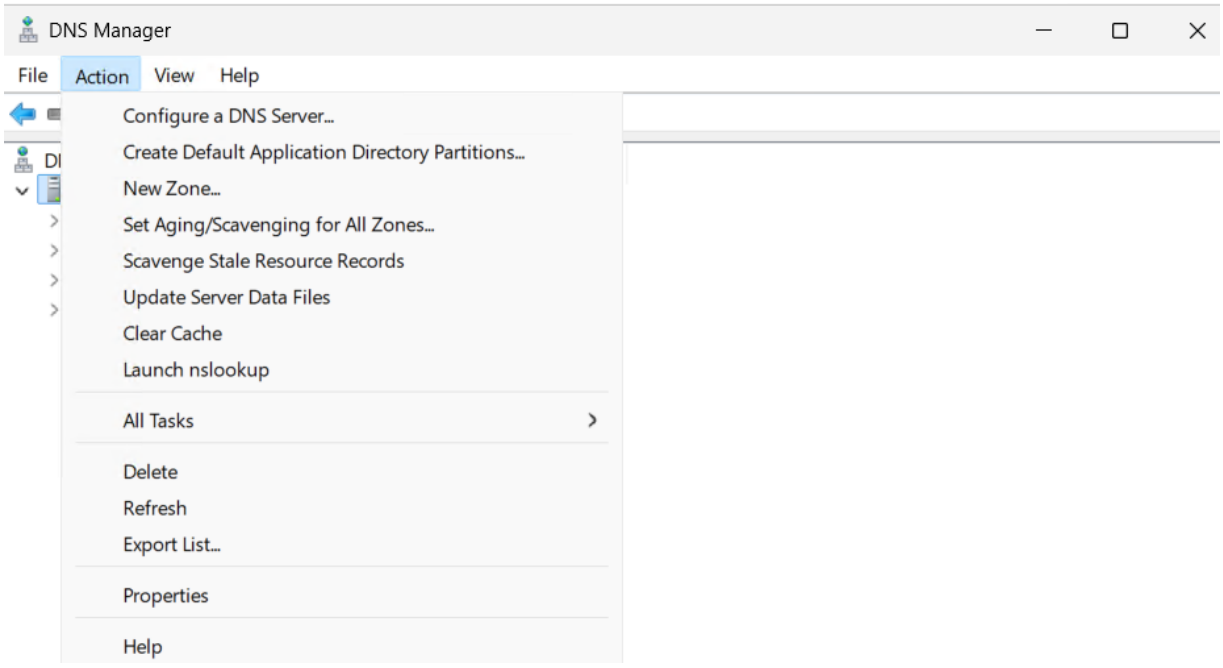

Рисунок 6.13 – «Запустити NSLOOKUP»

Після цього проводимо очищення кешу DNS. Щоб це виконати у DNS-менеджері натискаємо правою кнопкою миші на сервер та обираємо «Очистити кеш». Після цього кеш у вікні «Кеш-пам'ять DNS» очиститься (рис. 6.14).

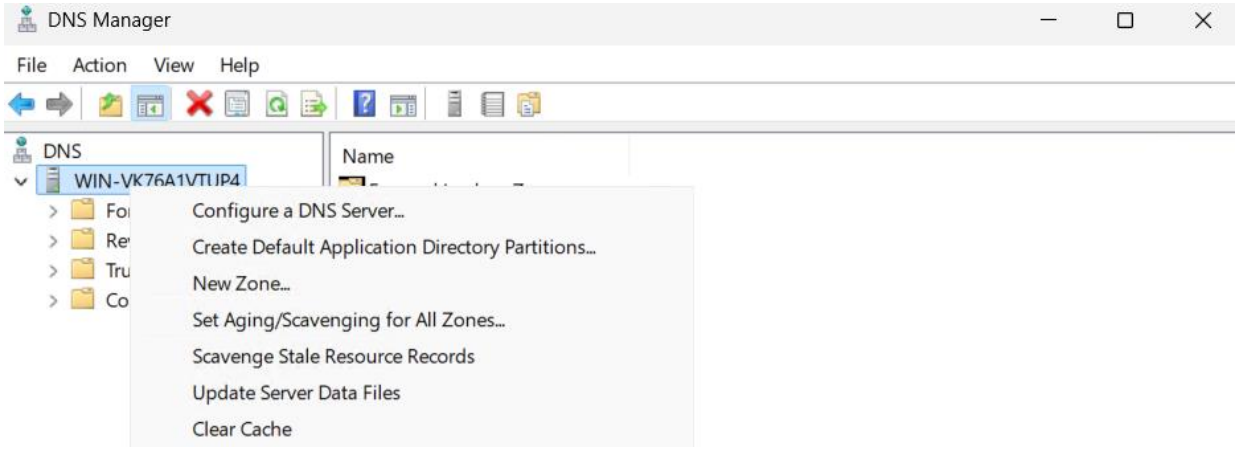

Рисунок 6.14 – «Очистити кеш»

Варто зазначити, що в кожного запису кешу DNS є параметр TTL (Time To Live) – це час, протягом якого він зберігається в кеші. Коли TTL закінчується, запис автоматично видаляється і при наступному запиті оновлюється.

Завдання 3. Діагностика та усунення помилок DNS

Для початку перевіряємо стан служби DNS. Відкриваємо «Диспетчер серверів». Переходимо у розділ «Служби». Переконуємось, що служба «DNS» має стан «Запущено». Якщо служба не працює – запускаємо її через натиснення на «Пуск».

Наступне, що варто виконати – це перевірка резолюції імен. Для цього відкриваємо «Командний рядок», виконуємо команду «nslookup google.com» Якщо бачимо IP-адресу, то резолюція працює. Якщо отримуємо помилку «Server failed» або «Request timed out», потрібно перевіряти далі та змінювати налаштування (рис. 6.15).

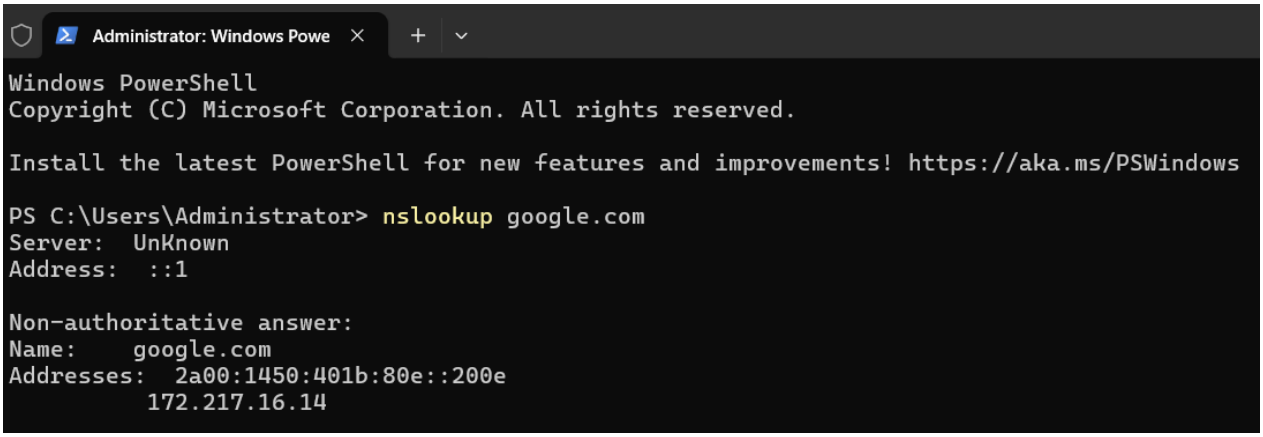

Рисунок 6.15 – Приклад успішного виконання команди «nslookup google.com»

Для діагностики налаштувань DNS виконуємо також перевірку клієнтських налаштувань. Відкриваємо «Центр управління мережами і спільним доступом» (рис. 6.16).

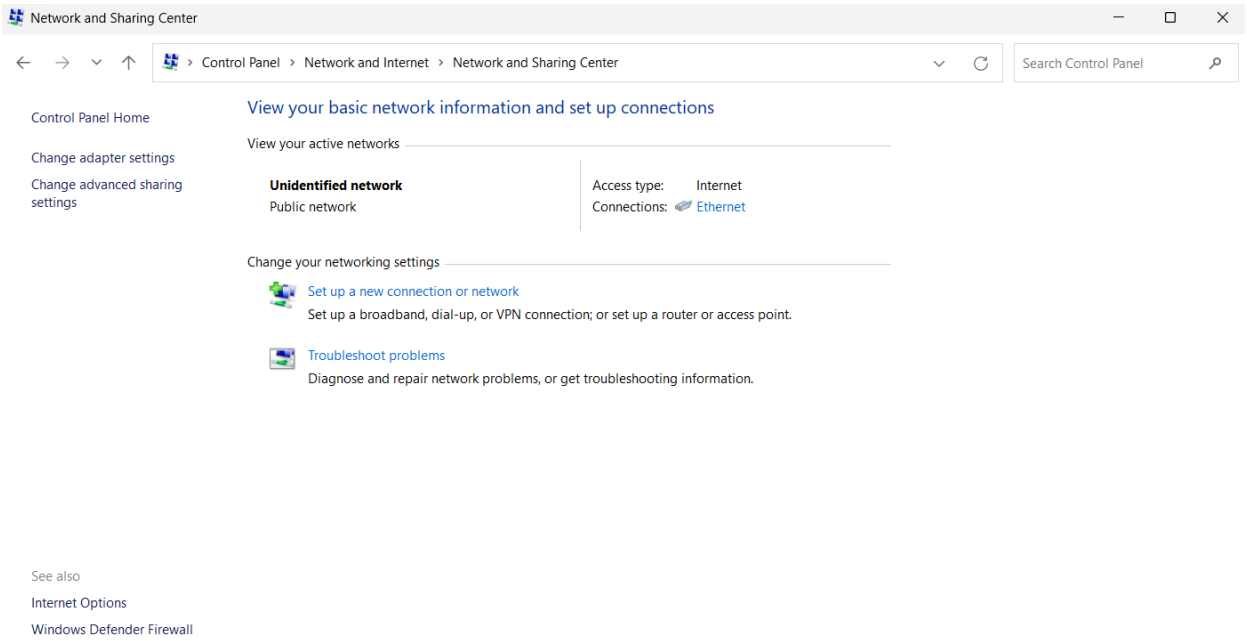

Рисунок 6.16 – «Центр управління мережами і спільним доступом»

Натискаємо на «Ethernet» та у вікні, що відкрилося заходимо у «Властивості». Вибираємо «Протокол TCP/IPv4» та натискаємо «Властивості». Переконуємось, що у полі «DNS-сервер» вказана IP-адреса нашого DNS-сервера (рис. 6.17).

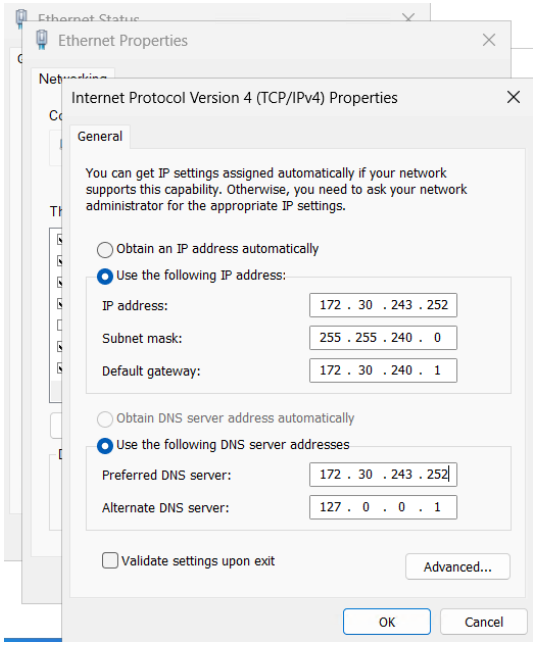

Рисунок 6.17 – Властивості IPv4 сервера та значення параметрів DNS-сервера

Також для діагностики проводиться перевірка зон DNS. Відкриваємо «Диспетчер DNS». Переглядаємо «Зони прямого перегляду» та «Зони зворотного перегляду».

Переконуємось, що: існує зона для домену (наприклад, server.lab). Є записи A (хост) для серверів і клієнтів. У зворотній зоні створені записи PTR. Якщо записи відсутні – створюємо їх вручну (натискаємо ПКМ по назві типу

зони та вибираємо «Новий вузол (A або AAAA)», «Новий вказівник (PTR)») (рис. 6.18).

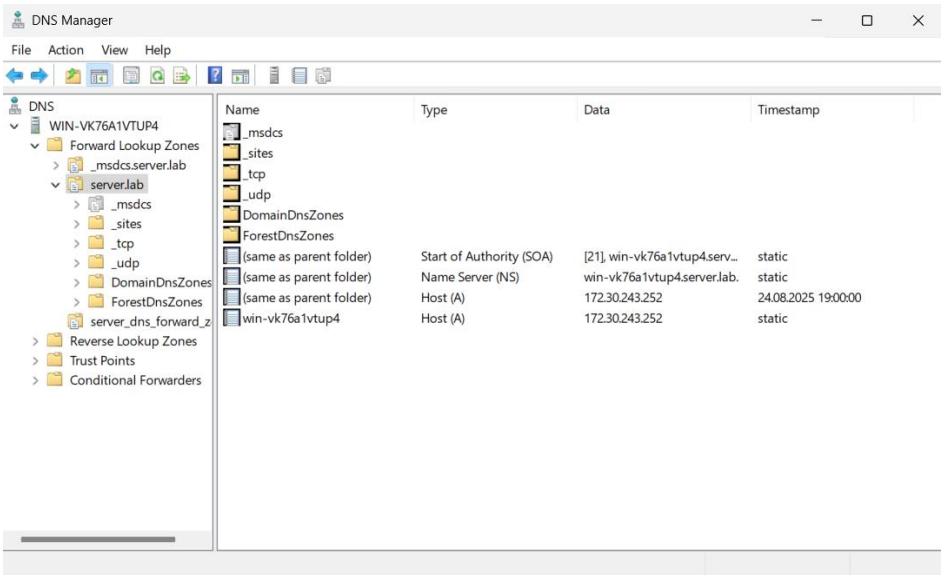

Рисунок 6.18 – Перевірка зон DNS

Також для діагностики роботи DNS та перевірки на наявність помилок застосовується утиліта «nslookup». Для її застосування у командному рядку вводимо «nslookup» – з'явиться консоль утиліти. Далі перевіряємо наш конкретний DNS-сервер – вводимо команду «server <ip address DNS-server>», в даному випадку «server 172.30.247.252». Після цього запитуємо будь-який домен, наприклад, google.com. Якщо є відповідь, то сервер працює. Якщо помилка, то проблема у зоні або маршруті (рис. 6.19).

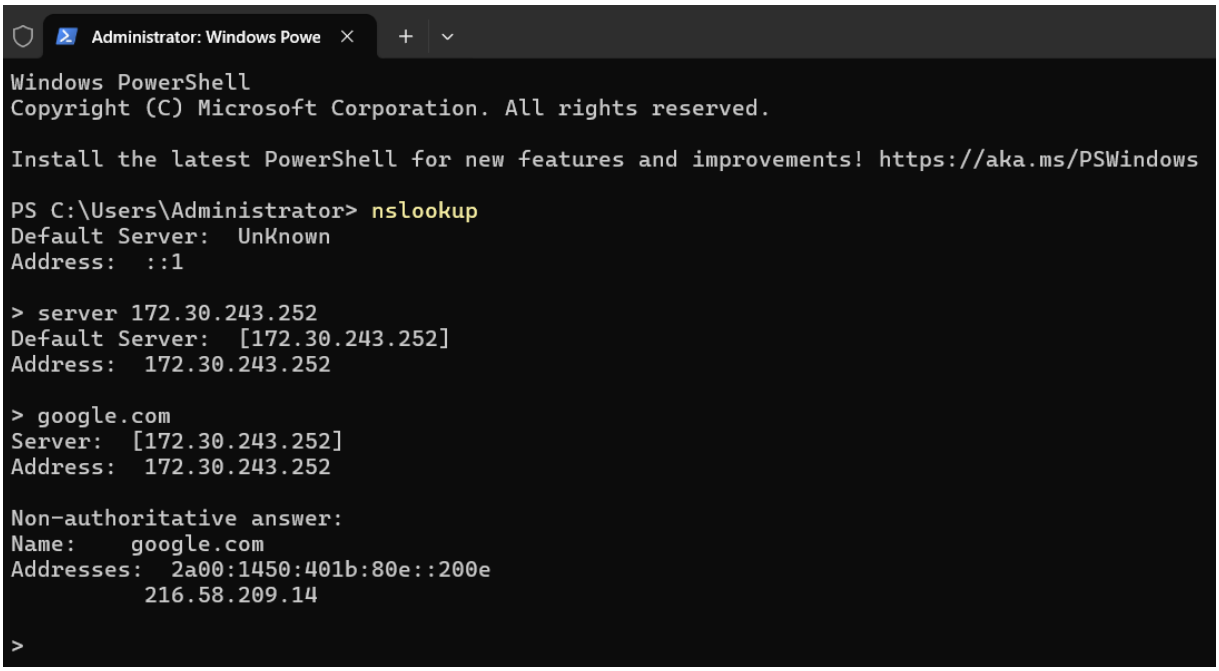

Рисунок 6.19 – Використання утиліти «nslookup» для діагностики роботи DNS

Лабораторна робота №7
DHCP у Windows Server 2025

Мета роботи: ознайомитися з принципами функціонування служби DHCP у середовищі Windows Server 2025, набути практичних навичок з інсталяції та конфігурації DHCP-сервера, створення та налаштування діапазонів IP-адрес, перевірки автоматичної видачі мережевих параметрів клієнтам, а також аналізу журналів роботи служби та усунення типових помилок [34-37].

Хідроботи

Завдання 1. Розгортання DHCP-сервера

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань першої практичної роботи.

Для розгортання DHCP-сервера, потрібно встановити для цього локального сервера роль «DHCP-сервер». Як, додавати ролі та компоненти опрацьовано в попередніх практичних роботах. Тому, відкриваємо «Диспетчер серверів». У верхньому правому меню обираємо «Керування» – «Додати ролі та компоненти». У майстрі додаємо роль «Ролі серверів» – «Сервер DHCP» (рис. 7.1).

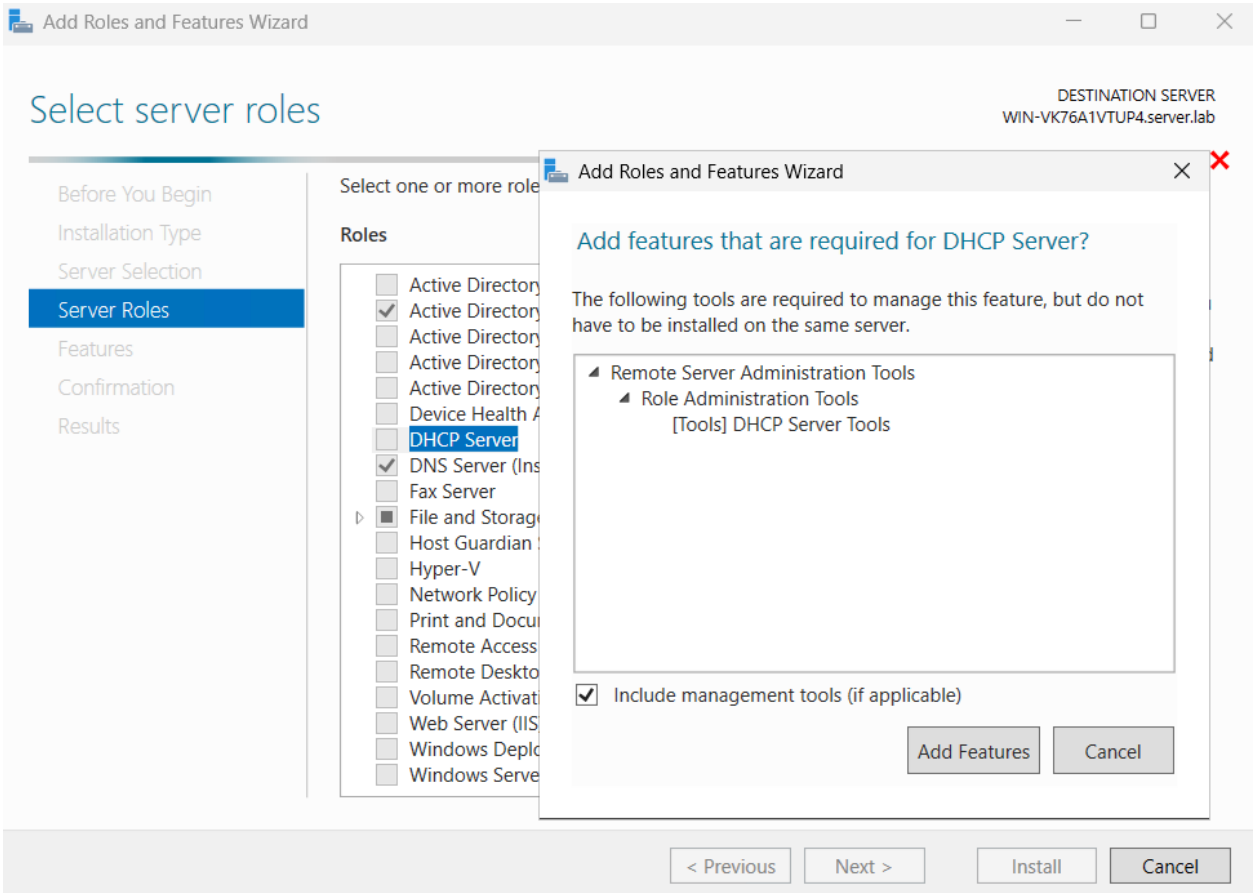

Рисунок 7.1 – Додавання ролі «Сервер DHCP»

Після вибору ролі, підтверджуємо вибір та чекаємо завершення інсталяції. Після завершення – натискаємо «Закрити» (рис. 7.2).

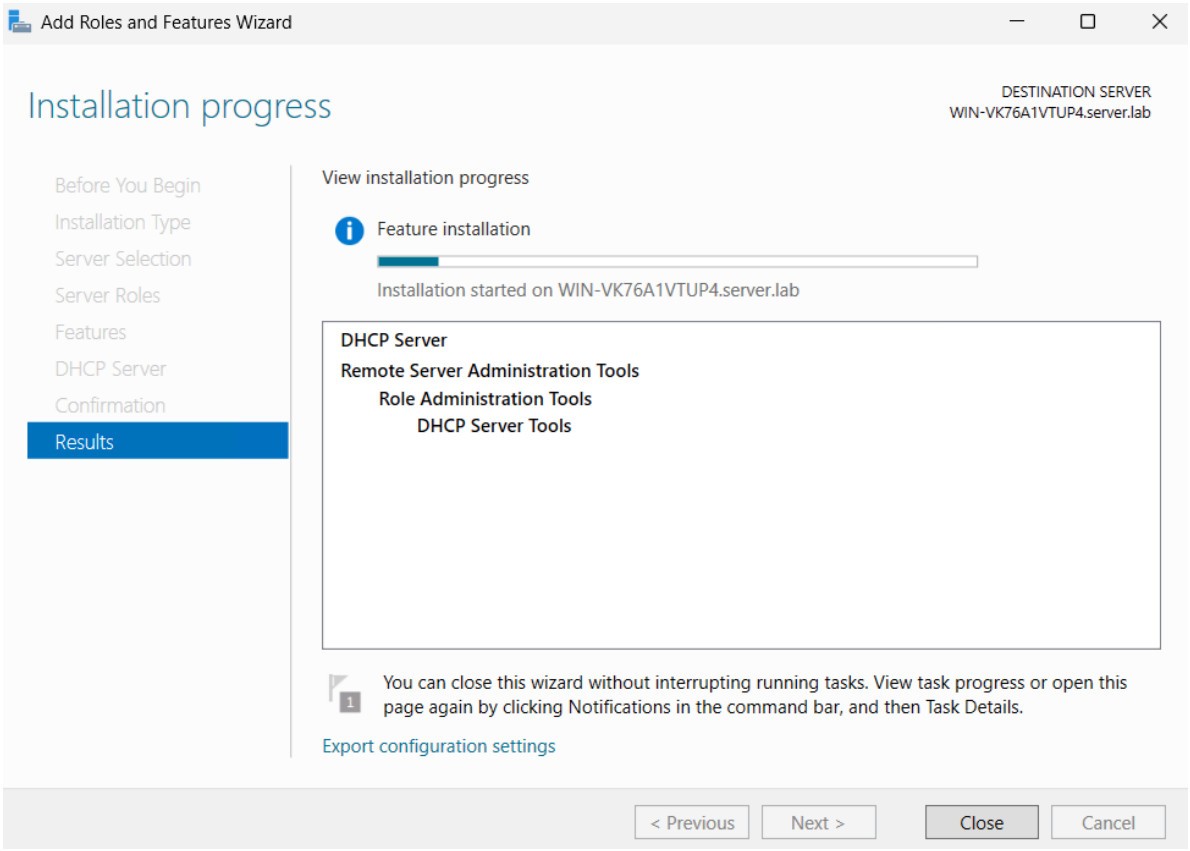

Рисунок 7.2 – Встановлення ролі «Сервер DHCP»

Після інсталяції у «Диспетчері серверів» з’явиться повідомлення про необхідність виконати початкову конфігурацію DHCP(рис. 7.3).

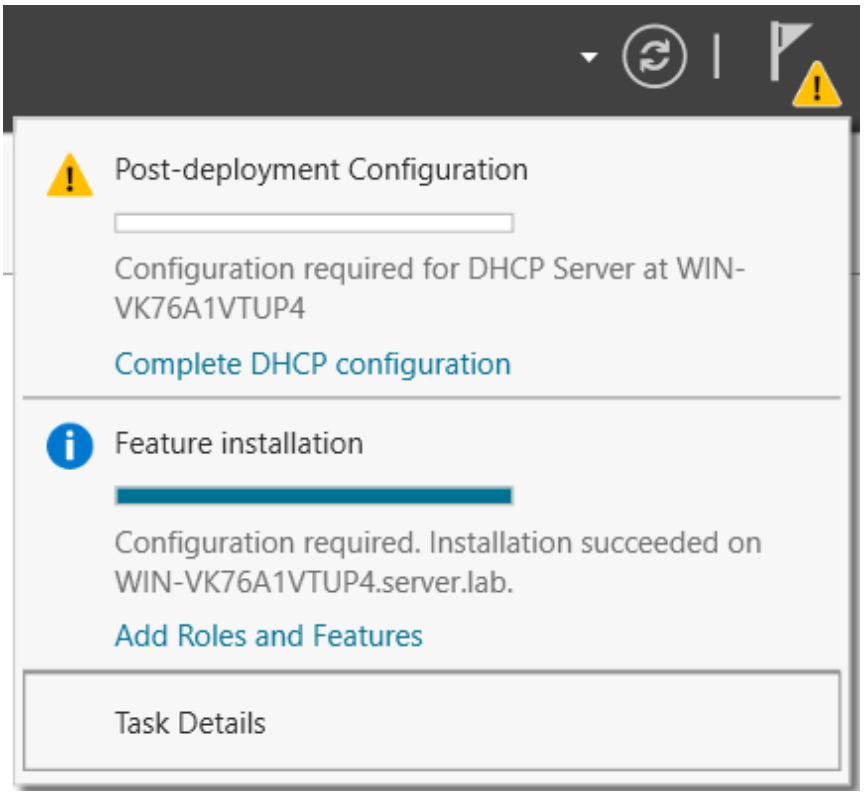

Рисунок 7.3 – Повідомлення про необхідність виконати конфігурацію DHCP

Натискаємо «Завершити конфігурацію DHCP», відкривається «Майстер налаштування DHCP після встановлення», на першій вкладці натискаємо «Далі» (рис. 7.4).

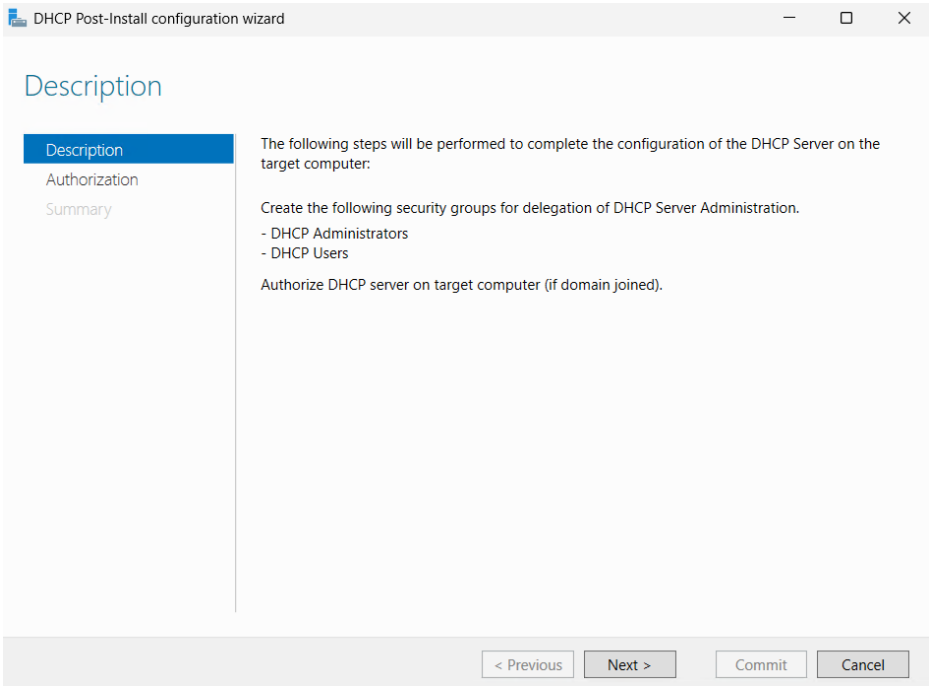

Рисунок 7.4 – Перша вкладка «Майстра налаштування DHCP після встановлення»

У наступному вікні майстра підтверджуємо використання облікового запису адміністратора для авторизації. Завершуємо налаштування та натискаємо «Закрити» (рис. 7.5-7.6).

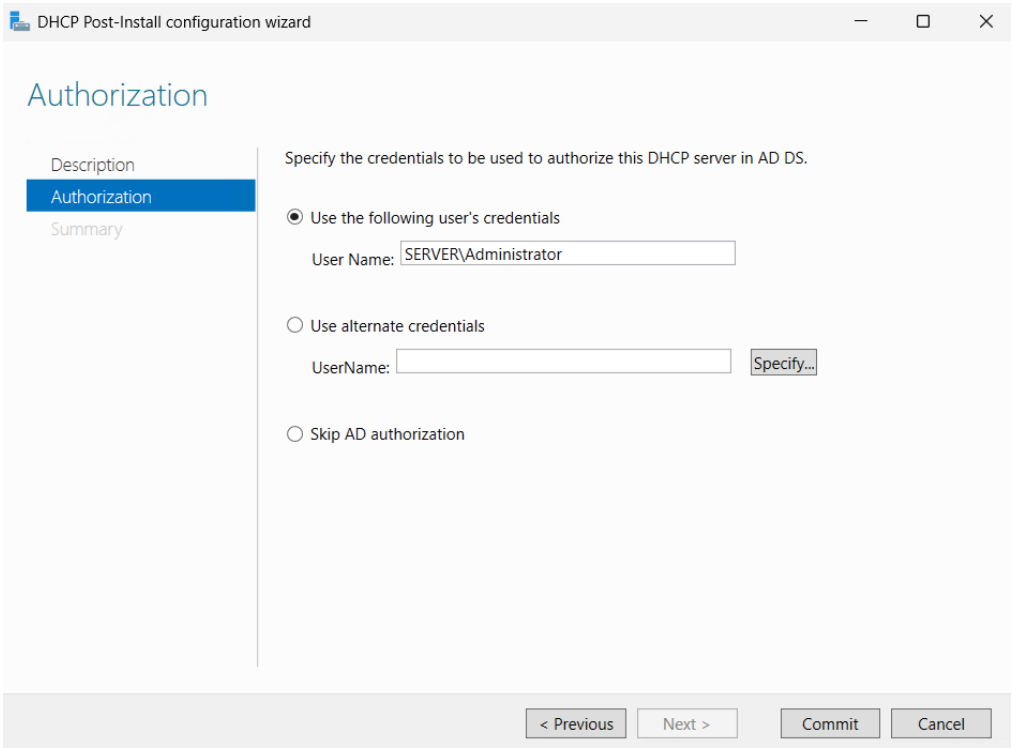

Рисунок 7.5 – Підтвердження використання облікового запису адміністратора

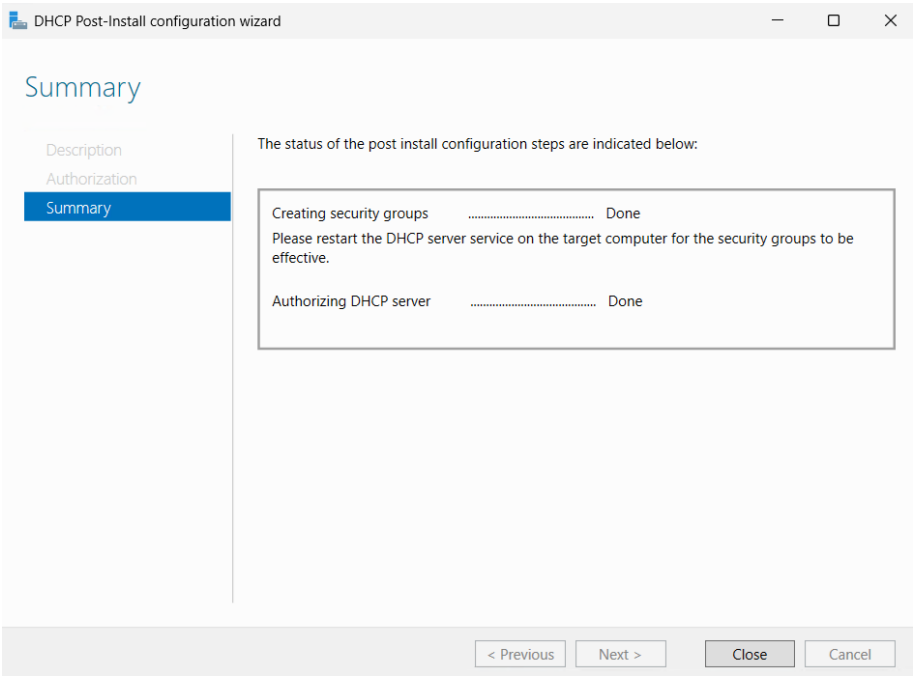

Рисунок 7.6 – Завершення початкового налаштування DHCP

Завдання 2. Налаштування діапазону IP-адрес

Подальшим етапом налаштування DHCP-сервера є налаштування діапазону IP-адрес, який цей сервер використовуватиме та видаватиме клієнтським пристроям. Для створення нового діапазону IP-адрес відкриваємо «DHCP», щоб це виконати «Диспетчері серверів» переходимо до «Інструменти» – «DHCP». Відкривається вікно «Менеджера DHCP» (рис. 7.7).

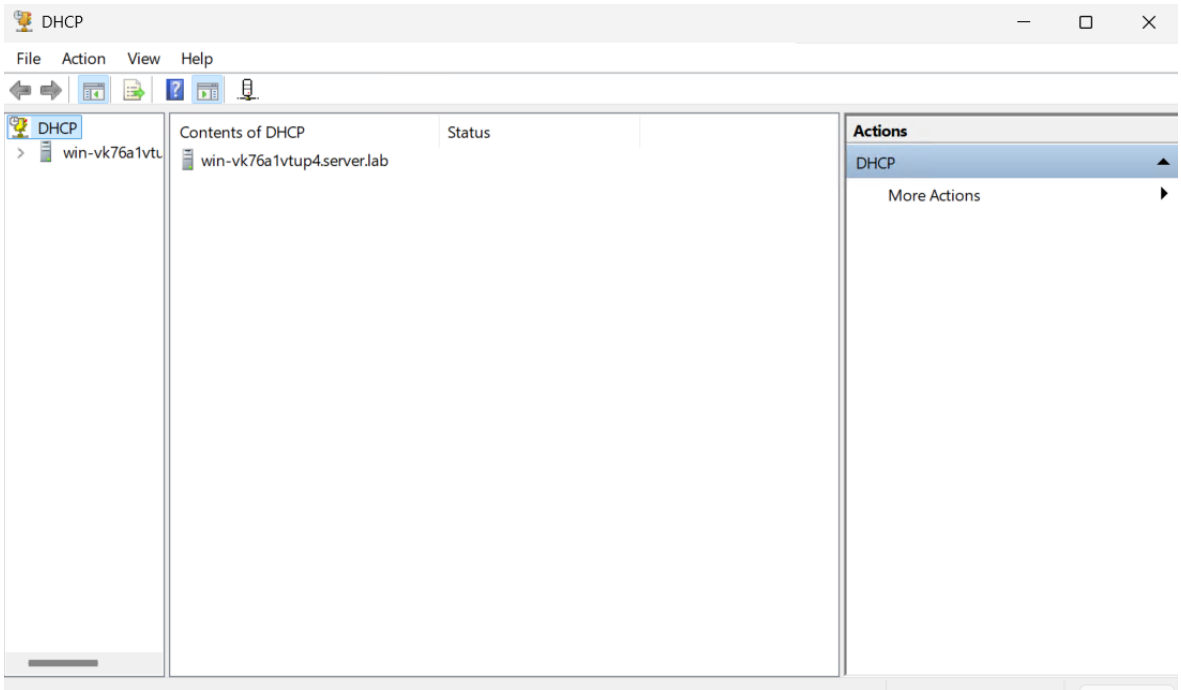

Рисунок 7.7 – Вікно «Менеджера DHCP»

У дереві зліва обираємо свій сервер, натискаємо на нього. Далі клацаємо правою кнопкою миші на «IPv4» та вибираємо «Створити область». В результаті цих дій відкривається «Майстер створення області» (рис. 7.8).

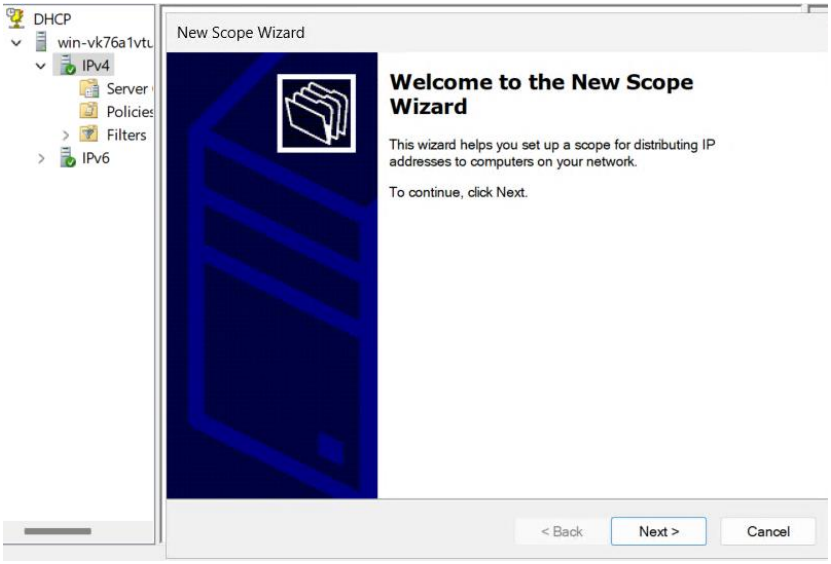

Рисунок 7.8 – Вікно «Майстер створення області»

На першій вкладці даного «Майстра…» натискаємо «Далі». Після цього починаються власне налаштування створюваного діапазону IP-адрес. Спочатку налаштовуємо ім'я діапазону (вводимо наприклад «DHCP-M1»). За необхідності можна додати опис, це корисно, якщо існує кілька DHCP-пулів для різних мереж і пристроїв(рис. 7.9).

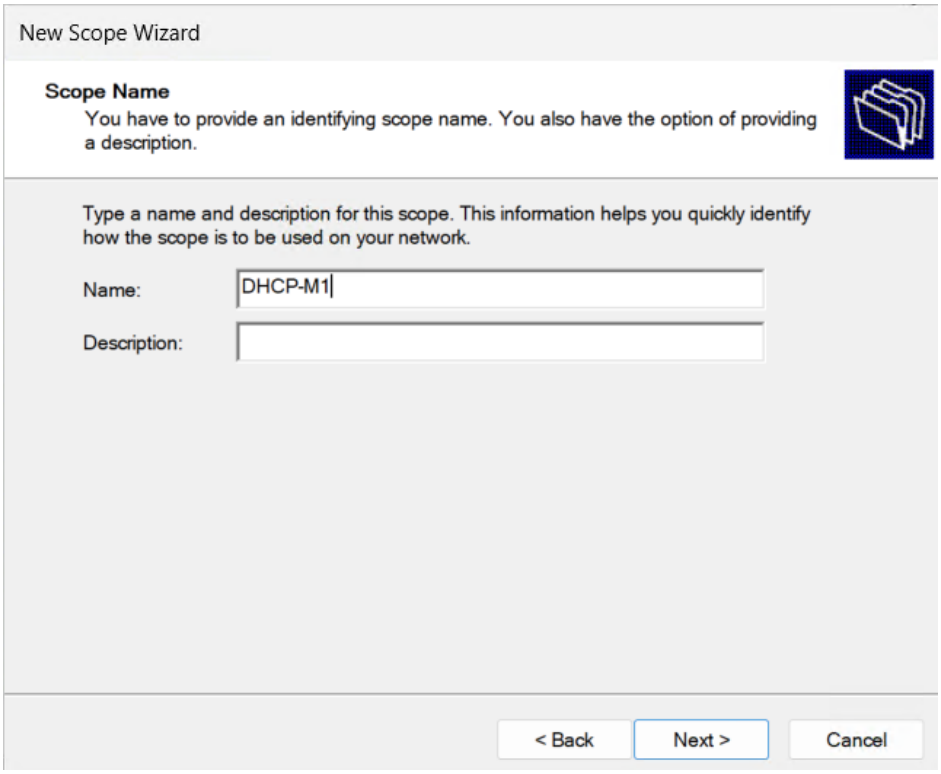

Рисунок 7.9 – Надання імені DHCP-діапазону

В наступній вкладці налаштовуємо найважливіші параметри: початкова IP-адреса (наприклад: 172.30.243.80); кінцева IP-адреса (наприклад: 172.30.243.160). Маска підмережі (наприклад: 255.255.240.0). Після заповнення всіх полів натискаємо «Далі» (рис. 7.10).

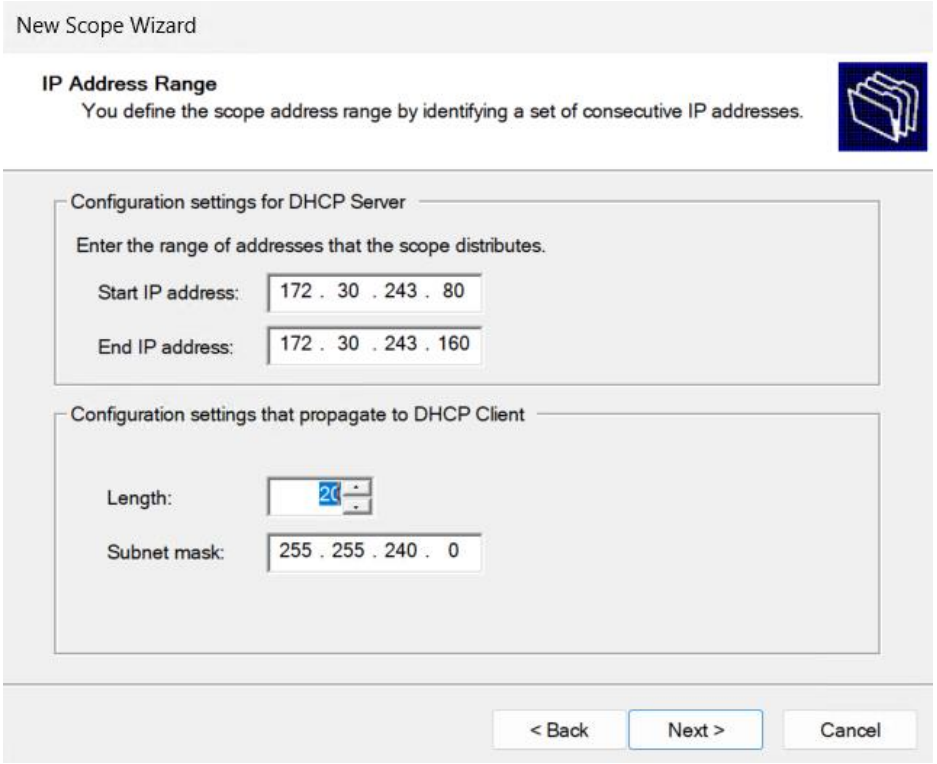

Рисунок 7.10 – Налаштування IP-параметрів DHCP-діапазону

В наступній вкладці, якщо є IP-адреси, які не повинні видаватися клієнтам, додаємо їх у «Виключення» та знову тиснемо «Далі» (рис. 7.11).

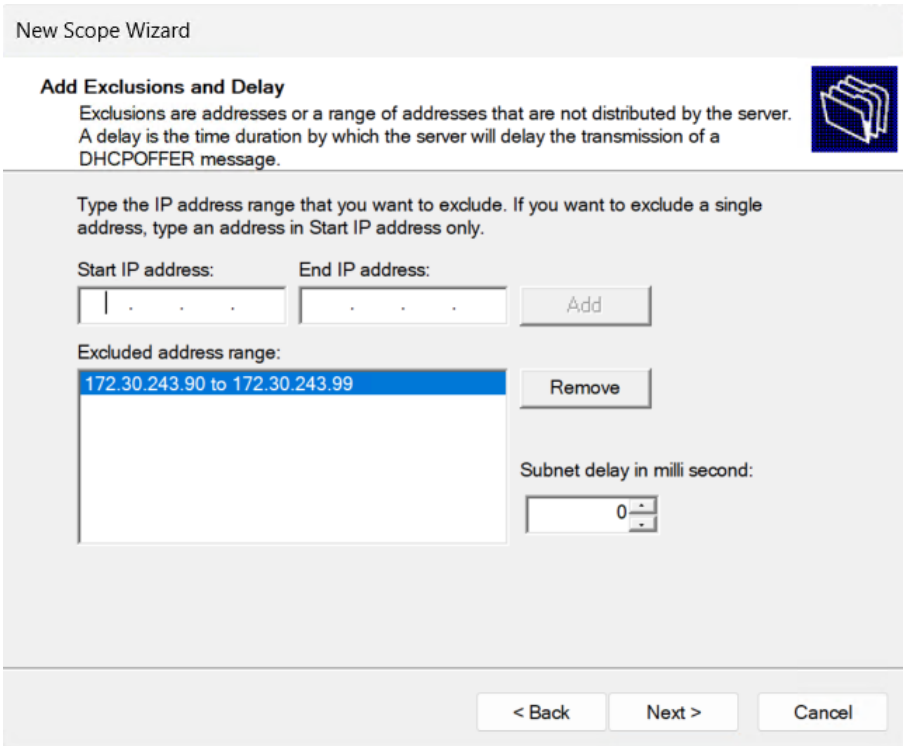

Рисунок 7.11 – Налаштування IP-адрес, які будуть виключені з DHCP-діапазону

Після цього налаштовуємо час оренди (наприклад, 30 днів) і натискаємо «Далі» (рис. 7.12).

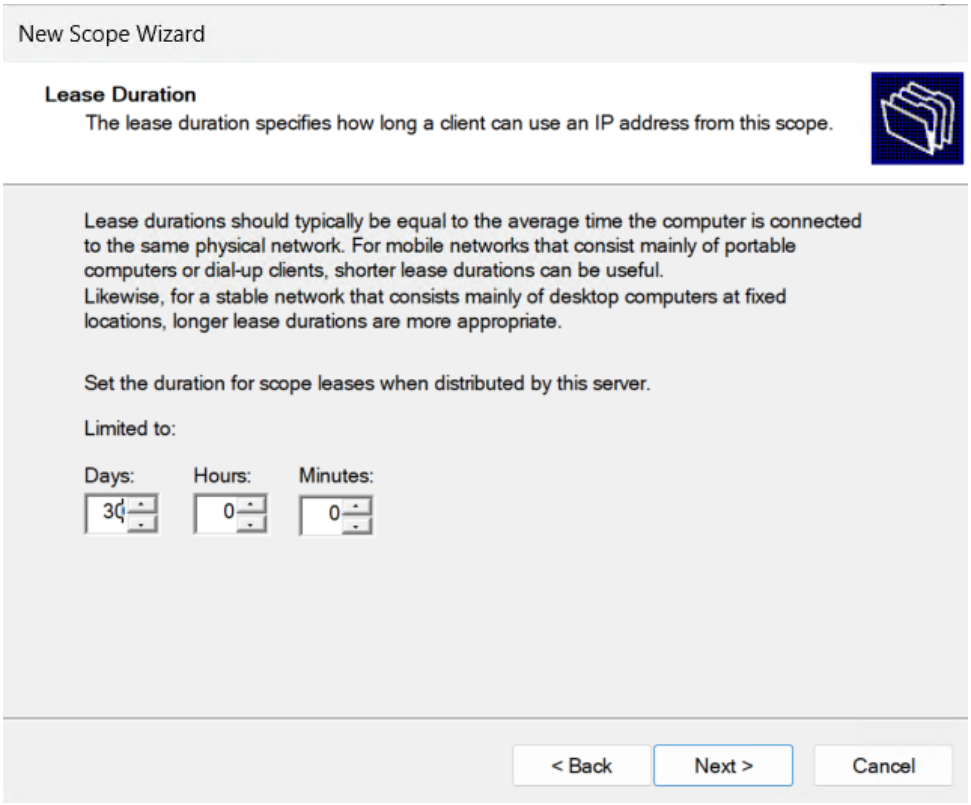

Рисунок 7.12 – Налаштування часу оренди для DHCP-діапазону

Далі, в наступній вкладці, вибираємо «Так, налаштувати ці параметри зараз». тиснемо «Далі». Потім вказуємо шлюз за замовчуванням (IP-адреса порту маршрутизатора) – наприклад: 172.30.240.1 (рис. 7.13).

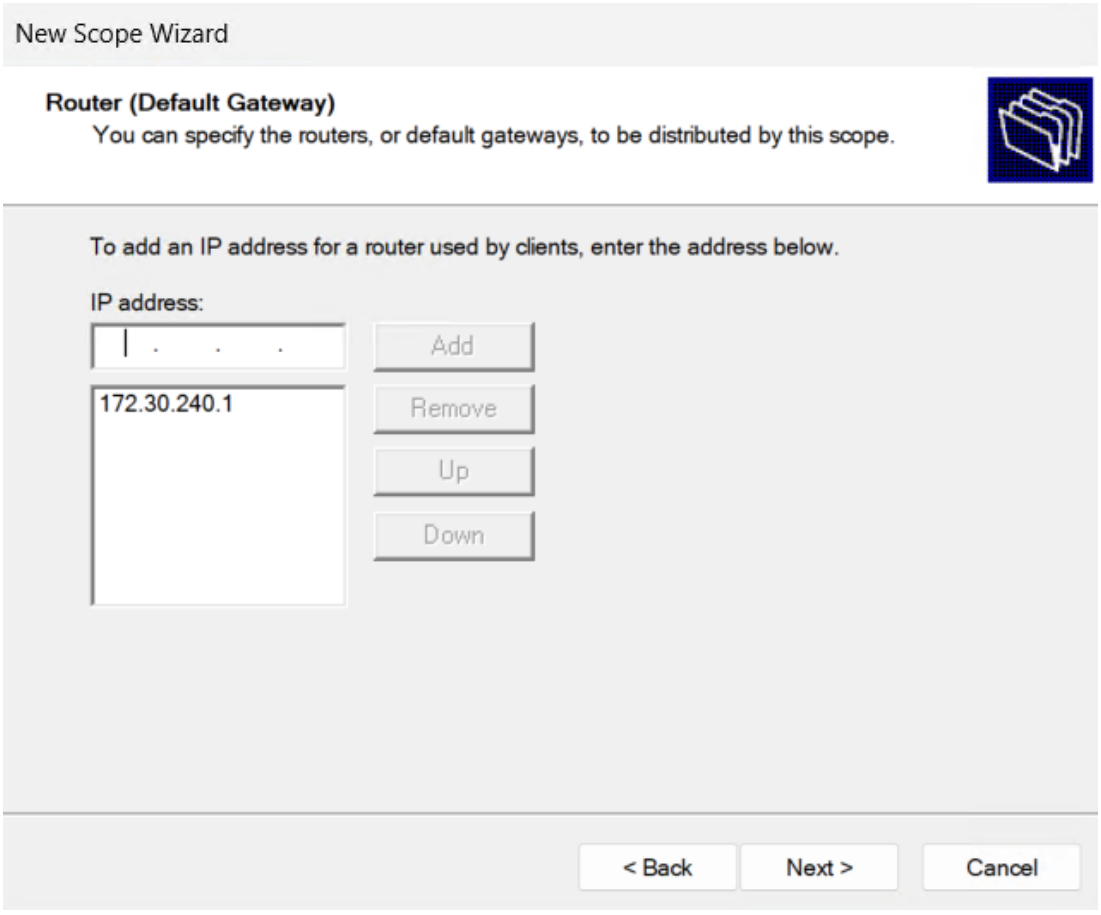

Рисунок 7.13 – Налаштування шлюзу за замовчуванням для DHCP-діапазону

Після цього виконуємо налаштування DNS-сервера для створюваного DHCP-діапазону, вказуємо IP-адресу нашого DNS (наприклад: 172.30.243.252). Якщо налаштування DNS, вже було виконано, то IP-адреса DNS-сервера буде записана автоматично і додаткового введення на цьому етапі не потребуватиме (рис. 7.14).

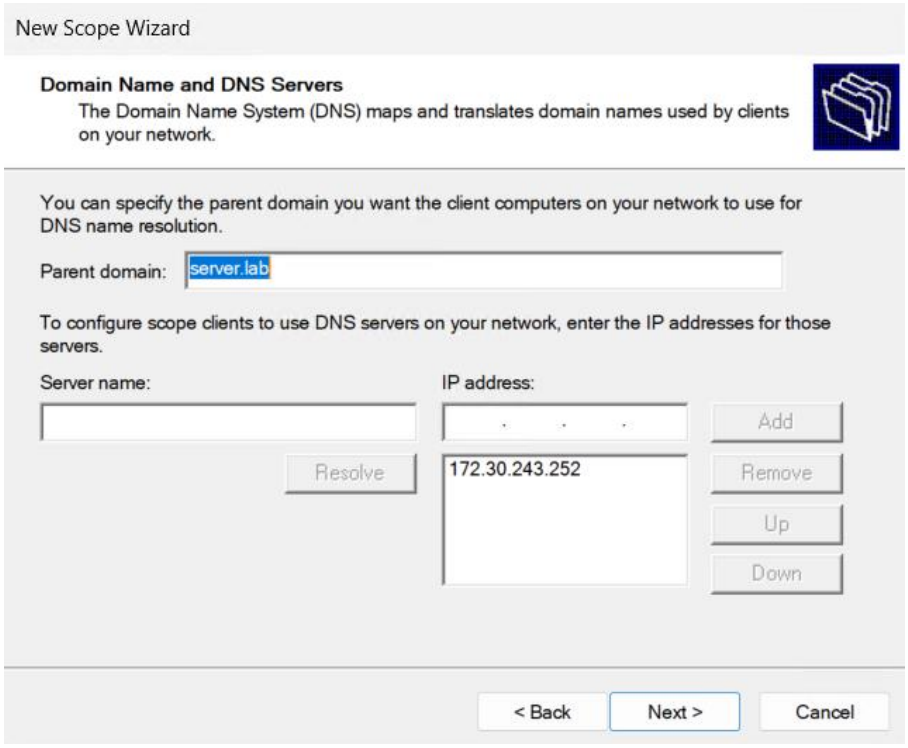

Рисунок 7.14 – Налаштування DNS-сервера для DHCP-діапазону

Згодом натискаємо «Далі» в цій вкладці і у наступній також. При виборі часу активації DHCP-області обираємо варіант «Так, я хочу активувати цю область зараз» і тиснемо «Далі» (рис. 7.15).

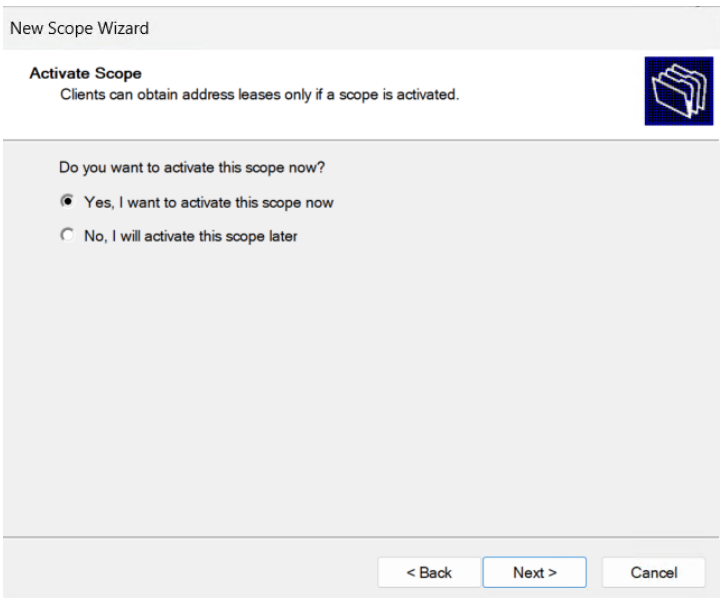

Рисунок 7.15 – Вибір часу активації DHCP-області

Далі натискаємо «Готово» і завершуємо створення та налаштування DHCP-діапазону (рис. 7.16).

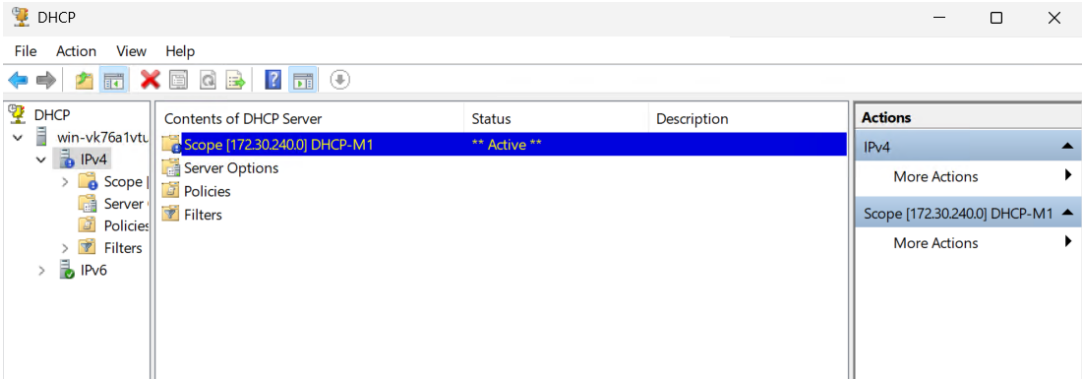

Рисунок 7.16 – Створена та активована DHCP-область

Щоб перевірити функціонування DHCP-сервера запускаємо іншу віртуальну машину у Hyper-V (наприклад, клієнт з Windows 10/11). Налаштовуємо мережеву карту цієї ВМ так, щоб вона отримувала IP-адресу автоматично.

У командному рядку клієнтської ВМ вводимо команди «ipconfig /renew» (оновлення IP) та «ipconfig /all» (перегляд виданої IP-адреси). Переконуємось, що клієнт отримав адресу з діапазону, який ми створили.

Завдання 3. Аналіз логів DHCP-сервера

Аналіз логів DHCP-сервера передбачає використання журналів Windows для аналізу функціонування DHCP. Для цього відкриваємо «Переглядач подій» (Event Viewer). У дереві ліворуч переходимо: «Журнали програм та служб» – «Microsoft» – «Windows» – «DHCP-Server» та аналізуємо журнали, що присутні для цього DHCP-сервера (рис. 7.17).

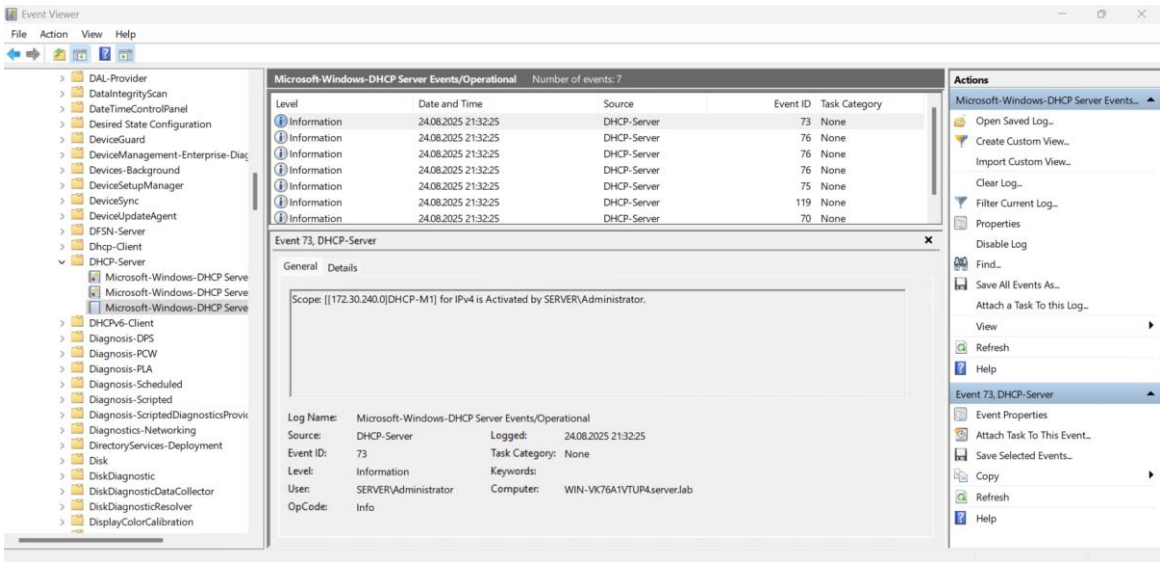

Рисунок 7.17 – Аналіз журналів DHCP-сервера

Аналізуємо записи в журналі за кодом події. Успішна видача IP-адреси – Event ID 10. Відмова через відсутність вільних IP-адрес – Event ID 20. Конфлікт IP-адрес – Event ID 30. Можна профільтрувати журнал для знаходження помилок для їх подальшого виправлення.

Логи DHCP також зберігаються у файлах на диску за адресою «C:\Windows\System32\dhcp». Файли мають назви DhcpSrvLog-XXX.log, де XXX – це день тижня написаний англійською мовою (Mon, Tue, Wed…). Відкриваємо файл за допомогою Блокнота (Блокнот / Notepad) або іншого текстового редактора (рис. 7.18).

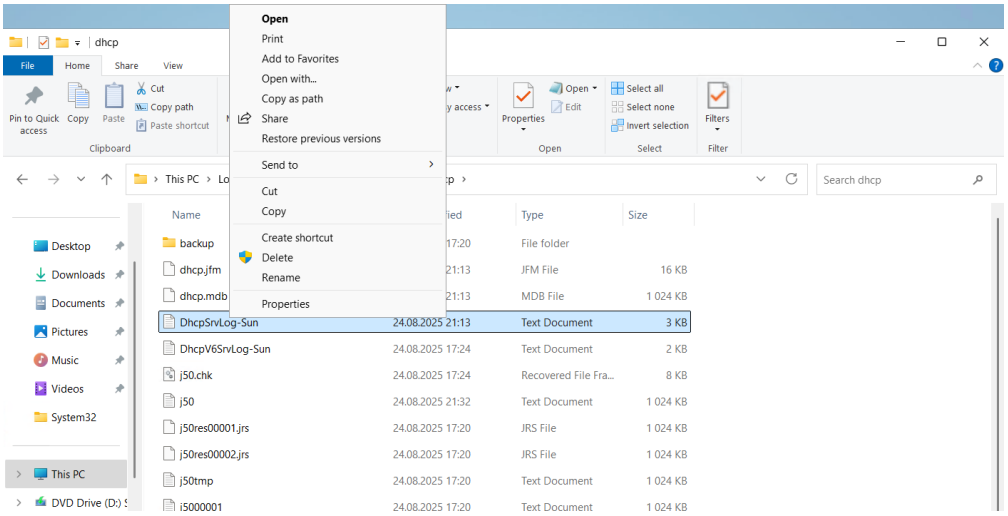

Рисунок 7.18 – Приклад текстового журналу DHCP-сервера на диску

У цих логах можна знайти записи: DHCPDISCOVER – клієнт шукає сервер, DHCPOFFER – сервер пропонує IP, DHCPREQUEST – клієнт запитує IP, DHCPACK – сервер підтверджує видачу, DHCPNACK – відмова у видачі адреси.

Щодо виправлення помилок, то типові помилки – це якщо клієнти не отримують IP-адреси – перевіряємо чи є вільні адреси у діапазоні; якщо є конфлікти – перевіряємо Event ID 30 (конфлікт) та уточнюємо, чи немає статичних IP в межах діапазону; якщо DHCP не запускається – перевіряємо службу у Службах (Services.msc).

Лабораторна робота №8
Захист Windows Server 2025

Мета роботи: ознайомитися з механізмами забезпечення безпеки у Windows Server 2025, набути практичних навичок зі створення та налаштування правил брандмауера для вхідних і вихідних з'єднань, здійснювати моніторинг активних правил і підключень, а також проводити аналіз журналів безпеки для виявлення та запобігання несанкціонованим діям [38].

Хід роботи

Завдання 1. Налаштування вхідних і вихідних правил

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань першої практичної роботи.

Для захисту сервера використовується брендмауер, що працює но основі правил вхідного і вихідного трафіку. Тому, потрібно ці правила налаштувати. Для цього переходимо до «Диспетчера серверів». У верхньому меню обираємо «Інструменти» – «Монітор брандмауера Windows в режимі підвищеної безпеки» (рис. 8.1).

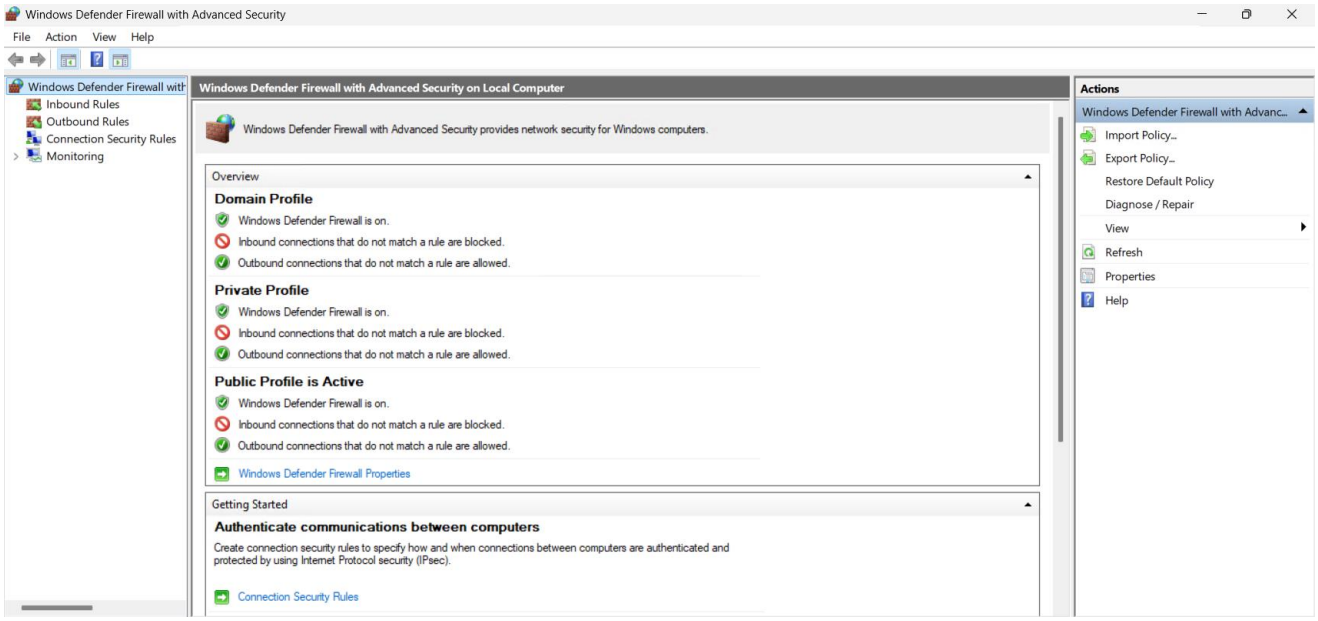

Рисунок 8.1 – Вікно «Монітора брандмауера Windows в режимі підвищеної безпеки»

У вікні бачимо три головні категорії: вхідні правила, що визначають, який трафік може заходити на сервер; вихідні правила, які визначають, який трафік може виходити із сервера; правила безпеки підключень – додатково налаштовують IPSec.

Для створення нового вхідного правила у лівій панелі обираємо «Правила для вхідних підключень» і після цього у правій панелі натискаємо «Створити правило…» (рис. 8.2-8.3).

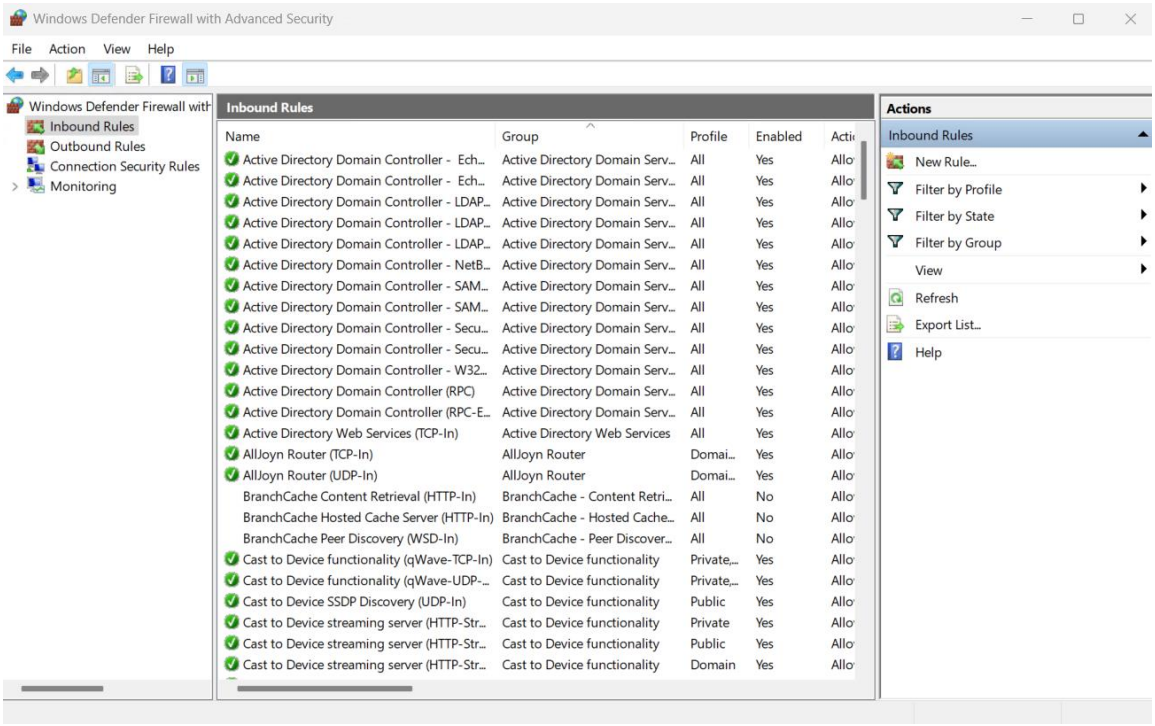

Рисунок 8.2 – «Правила для вхідних підключень»

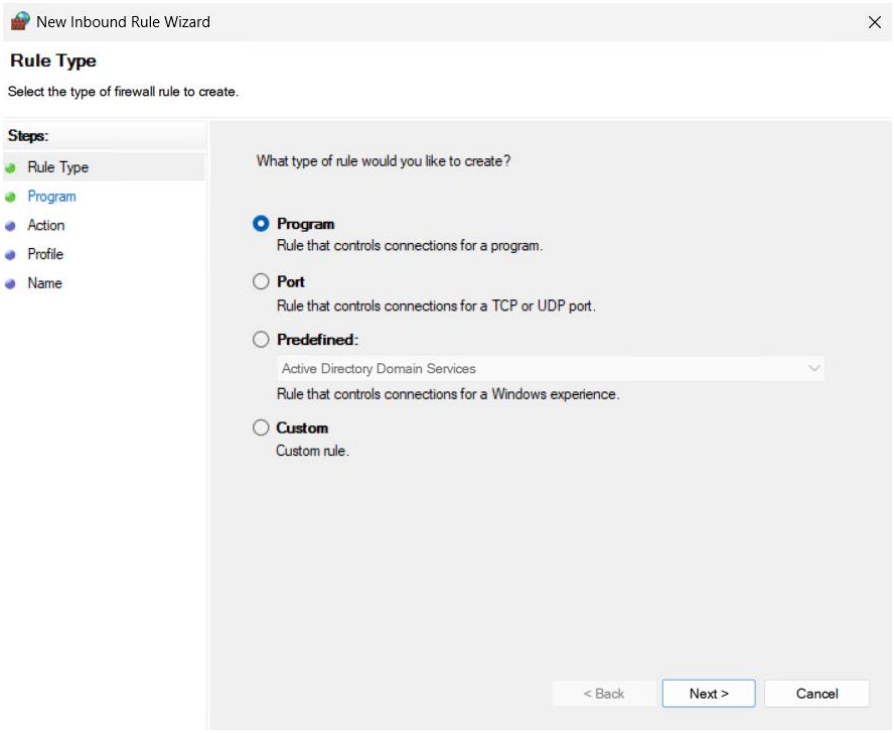

Рисунок 8.3 – Початок створення нового вхідного правила

У цьому вікні «Майстра створення правил для нового вхідного підключення» вибираємо тип правила.

Для програми – якщо хочемо дозволити або заблокувати конкретну програму.

Для порту – якщо треба обмежити доступ по TCP/UDP портах.

Для попередньо визначеного – для вбудованих сервісів Windows.

Користувацьке – власне правило користувача.

В цьому випадку, наприклад, обираємо тип правила «Для порту» та натискаємо «Далі» (рис. 8.4).

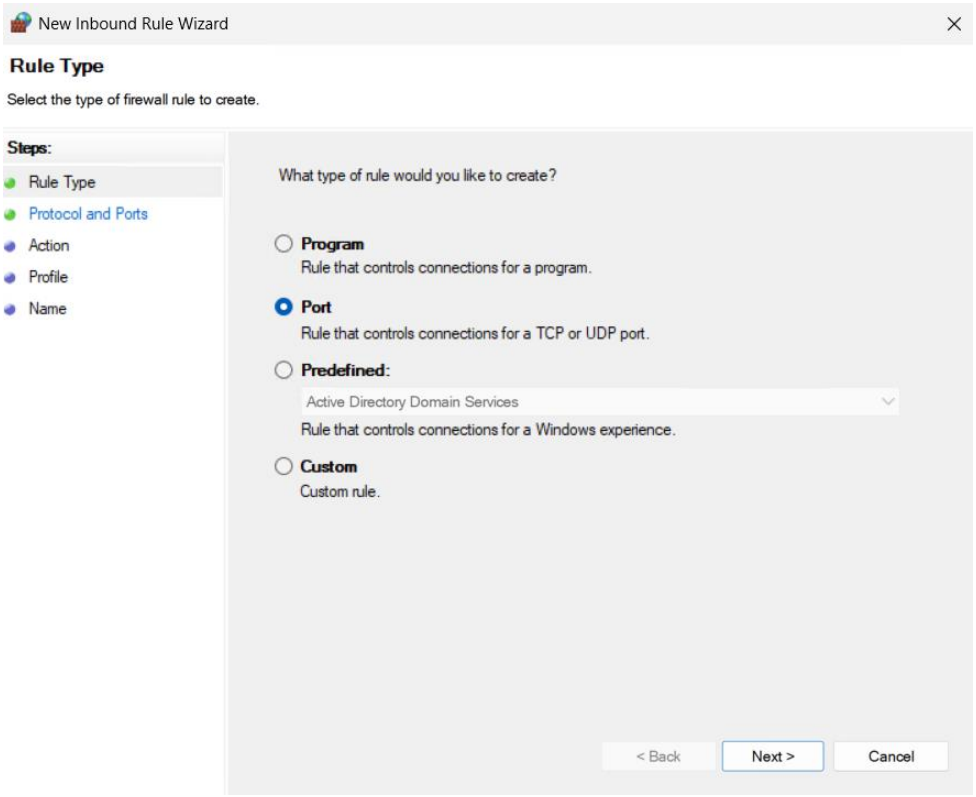

Рисунок 8.4 – Вибір типу нового вхідного правила

Після обрання типу правила – «Для порту», вказуємо протокол «TCP» та порт «3389» (RDP) та натискаємо «Далі» (рис. 8.5).

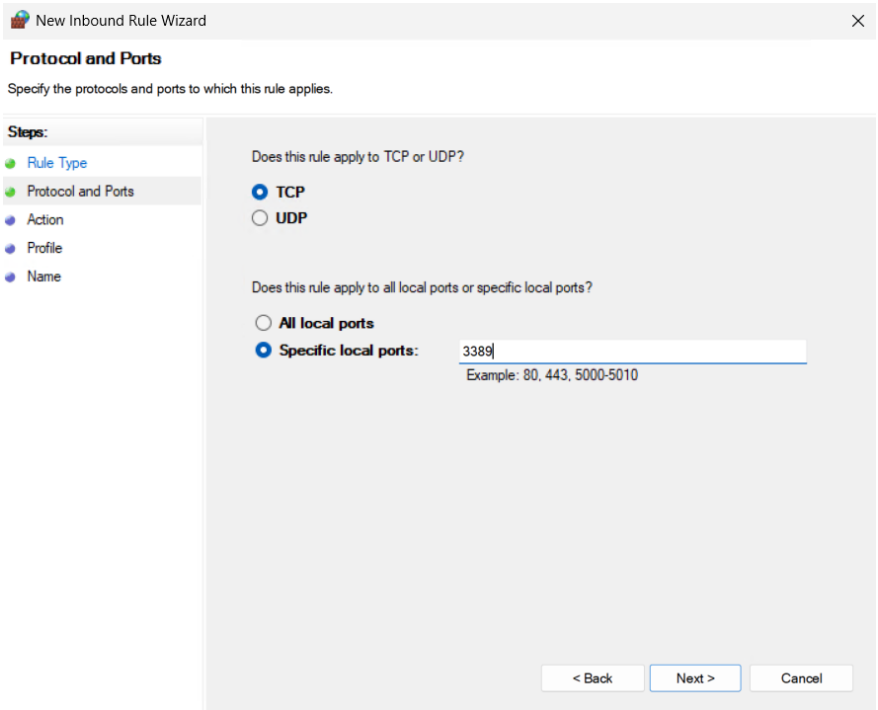

Рисунок 8.5 – Вибір типу протоколу та вказівка порту для вхідного правила

В наступній вкладці вікна вибираємо дію, яка застосовуватиметься до порту, що ми вказали раніше: «Дозволити з’єднання» або «Блокувати з’єднання». Обираємо блокувати (рис. 8.6).

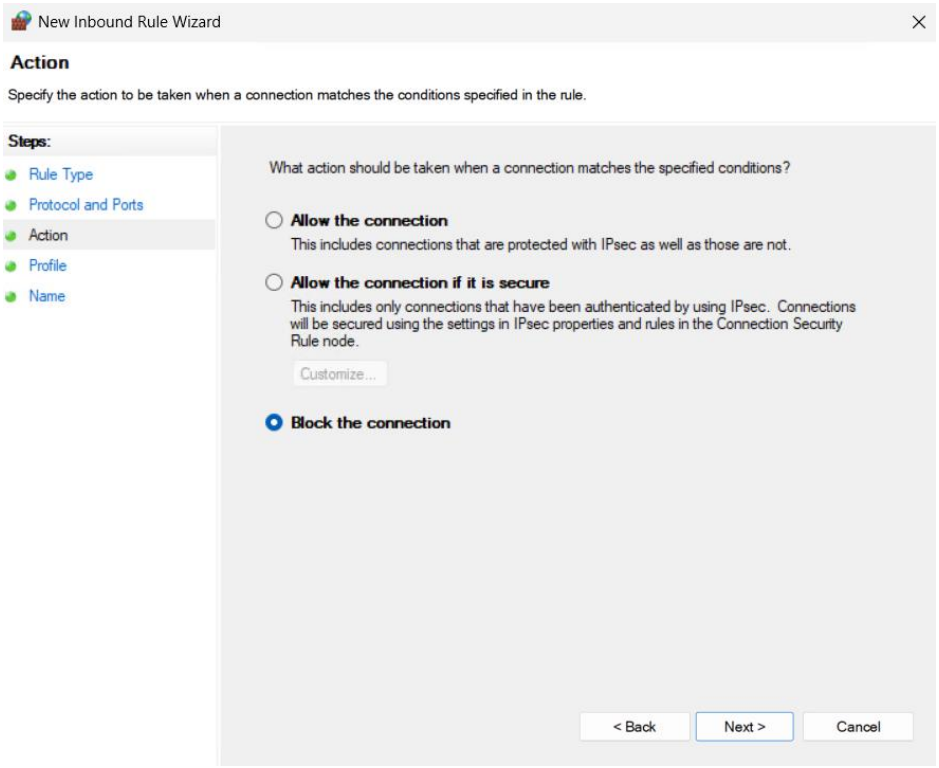

Рисунок 8.6 – Вибір дії для нового вхідного правила

Після цього обираємо профіль, для якого або яких застосовуватиметься нове правило. Варіанти: «Домен», «Приватний», «Публічний». Вибираємо для всіх і натискаємо «Далі» (рис. 8.7).

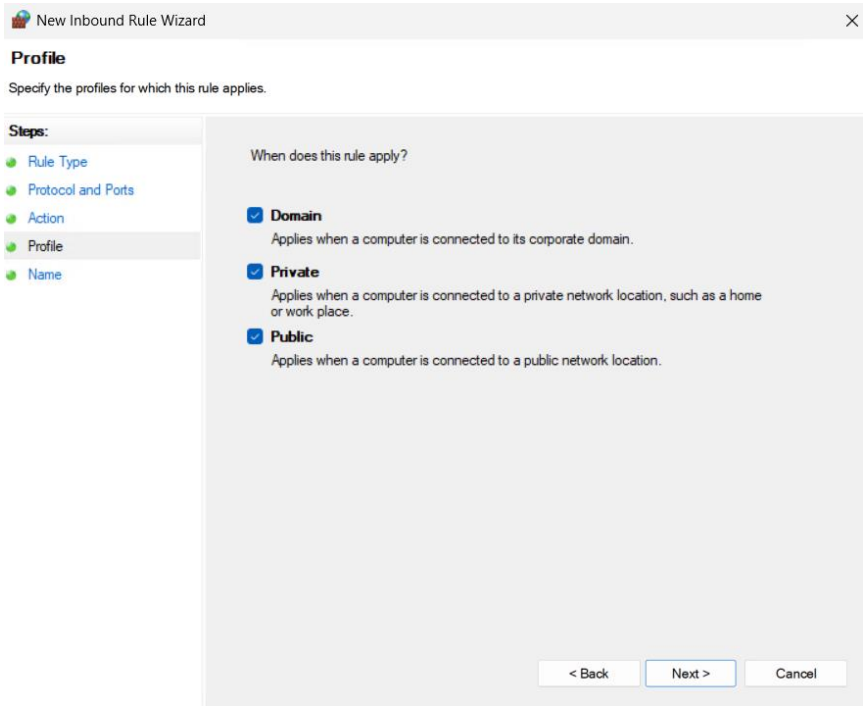

Рисунок 8.7 – Вибір профіля для нового вхідного правила

На останній вкладці вказуємо ім’я для створеного вхідного правила, наприклад, в даному випадку, «Блокування RDP», після цього тиснемо «Готово» і вхідне правило створене (рис. 8.8).

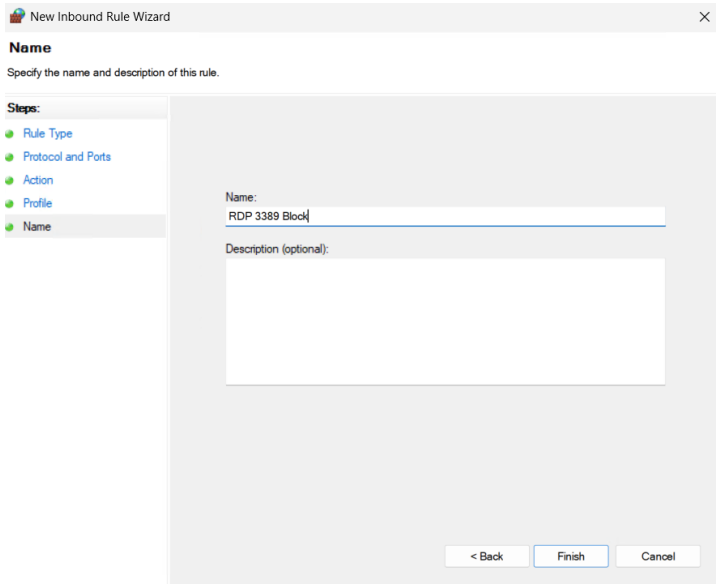

Рисунок 8.8 – Надання імені для нового вхідного правила

Створення вихідного правила відбувається за подібним алгоритмом. У лівій панелі обираємо «Правила для вихідного підключення». В правій частині вікна натискаємо «Створити правило…». Аналогічно задаємо параметри. Наприклад, блокуємо доступ програми Microsoft Edge до Інтернету. Для цього вибираємо тип правила «Для програми», далі вказуємо шлях до виконуваного файлу Microsoft Edge, а саме – «C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe» (рис. 8.9).

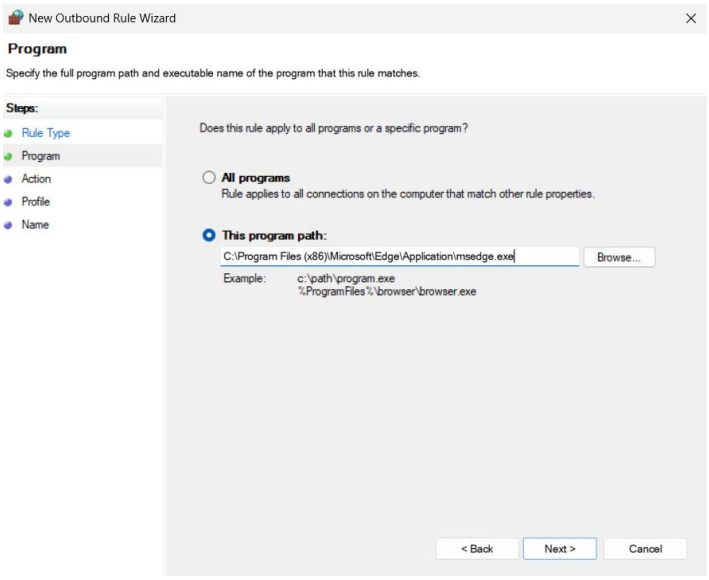

Рисунок 8.9 – Вказівка шляху до виконуваного файлу для вихідного правила

Перейшовши далі у вкладці «Дії» обираємо «Блокувати з’єднання». Далі виконуємо налаштування профіля для вихідного правила. Після цього даємо ім’я новому вихідному правилу «Блокування MsEdge» та натискаємо «Готово». В результаті цих дій вихідне правило створено (рис. 8.10).

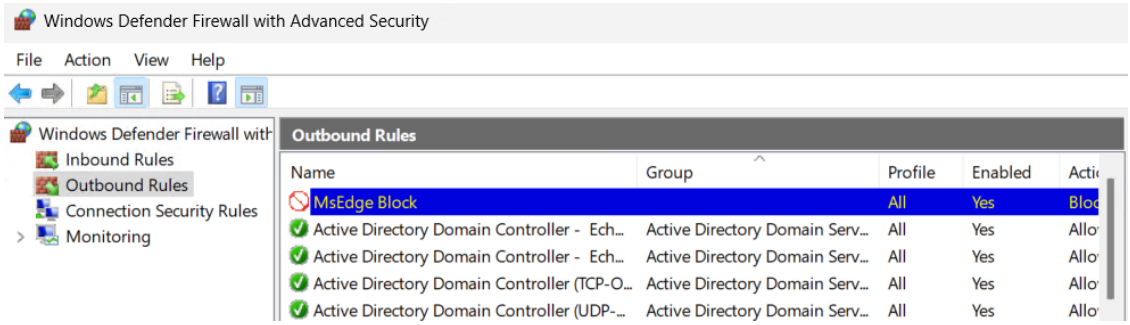

Рисунок 8.10 – Створене вихідне правило

Для перевірка роботи правила на клієнтській ВМ у Hyper-V пробуємо підключитися до сервера по RDP (3389). Якщо правило на блокування діє, то відповідно з'єднання не встановиться. Запускаємо заблоковану програму (наприклад Microsoft Edge) і перевіряємо, що вона не має виходу в Інтернет. Повертаємося до серверної ВМ, відкриваємо консоль брандмауера і переконуємось, що правила застосувалися.

Кожне правило брендмауера (як вхідне, так і вихідне) можна увімкнути/вимкнути або видалити (рис. 8.11).

Рисунок 8.11 – Меню дій, що можна робити з створеним правилом

Щоб змінити будь-яке правило слід натиснути на нього два рази лівою кнопкою миші – відкриються його властивості і далі можна проводити редагування. Наприклад, дозволимо підключення по RDP та змінимо ім'я правила (рис. 8.12).

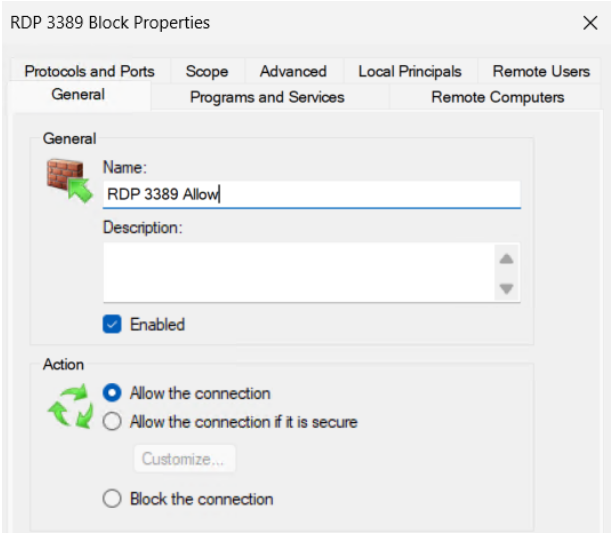

Рисунок 8.12 – Зміна налаштувань правила

Завдання 2. Моніторинг роботи брандмауера

Для моніторингу роботи брендмауера та з'єднань є вкладка «Моніторинг». Вона використовується для: перегляду активних правил (і вхідних, і вихідних), які застосовуються на сервері; відображення ефективних правил – тобто тих, що реально працюють, навіть якщо є конфлікти між кількома політиками; перевірки активних з'єднань та їх відповідності правилам; швидкого аналізу, чи спрацювало конкретне правило без необхідності перевіряти вручну всю колекцію. Ця вкладка зручна для діагностики, коли є сумніви: правило створене, але невідомо, чи воно реально застосовується (рис. 8.13).

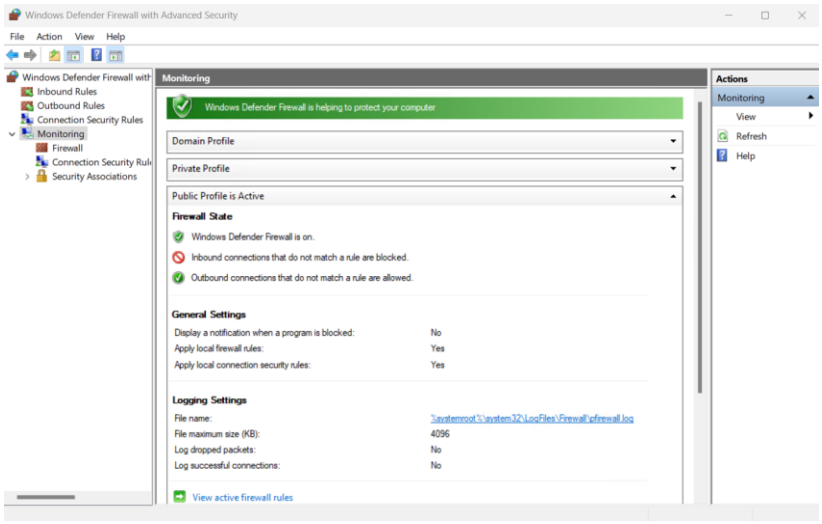

Рисунок 8.13 – Вкладка «Моніторинг»

Для перевірка конкретного правила, наприклад, якщо ми раніше створювали правило для блокування доступу до певного порту, воно має з'явитися у списку активних правил. Для цього у вікні вкладки «Моніторинг» натискаємо «Перегляд активних правил брендмауера» та у новому вікні шукаємо створені нами правила (рис. 8.14).

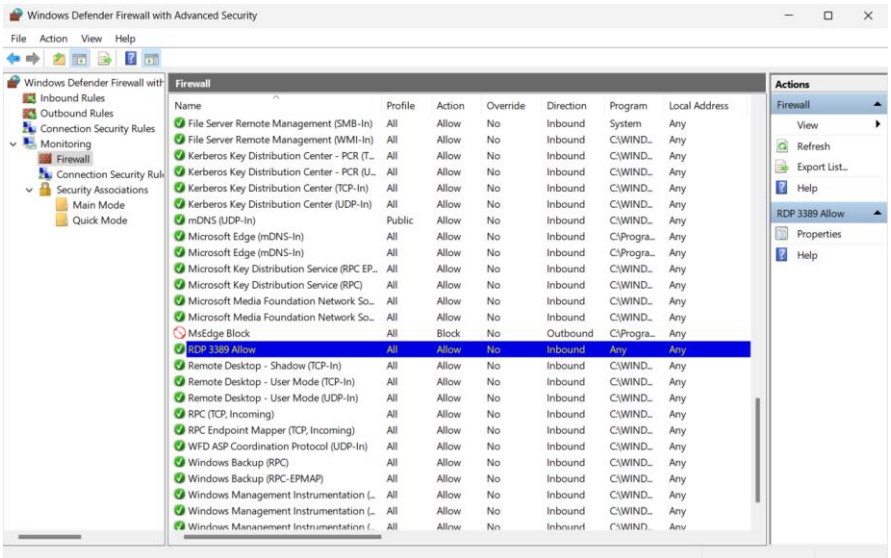

Рисунок 8.14 – Перегляд активних правил брендмауера

Для перевірки активних з’єднань, у розділі «Моніторинг» – «Правила безпеки підключень» переглядаємо, які з’єднання зараз захищені або заблоковані. Це дозволяє зрозуміти, чи працює IPsec або інші налаштування захисту (рис. 8.15).

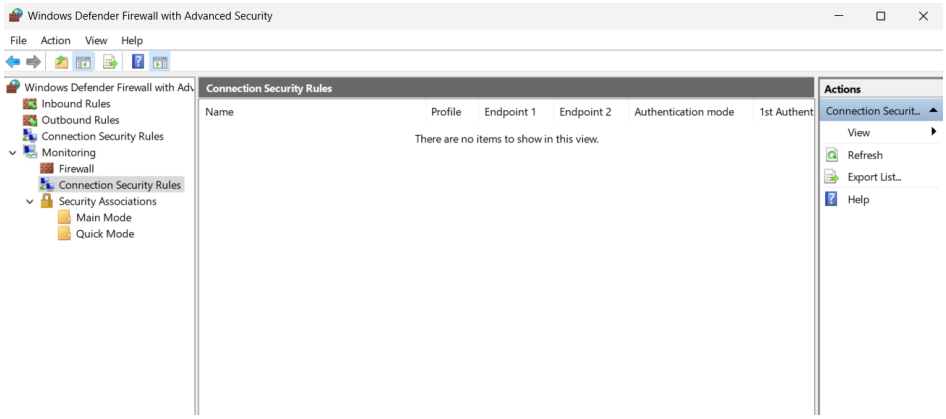

Рисунок 8.15 – Приклад не налаштованого IPsec

В загальному, завдяки вкладці «Моніторинг» адміністратор сервера може швидко перевірити, які правила реально діють. Це зручно для пошуку конфліктів між різними наборами політик і для діагностики проблем доступу.

Завдання 3. Аналіз журналів безпеки Windows Server 2025

Для аналізу та роботи з журналами безпеки Windows Server 2025 на сервері відкриваємо «Диспетчер серверів». У меню «Інструменти», обираємо «Перегляд подій». У вікні, що відкрилося переходимо до журналів безпеки. Для цього у лівій панелі розгортаємо: «Журнали Windows» – «Безпека». У центральному вікні бачимо список подій, пов’язаних із безпекою системи (рис. 8.16).

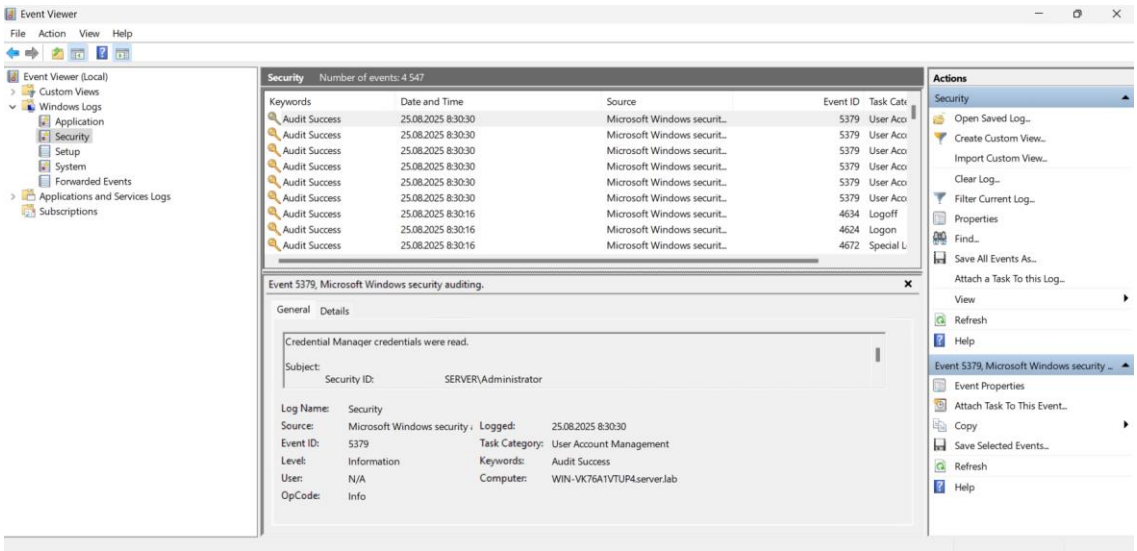

Рисунок 8.16 – Журнал «Безпека»

Для зручності аналізу та ефективного підходу до його здійснення варто використати фільтрацію подій. У правій панелі натискаємо «Фільтр поточного журналу». У полі «Ідентифікатор подій» вводимо потрібний номер, наприклад «4625», щоб побачити всі невдалі спроби входу та вибираємо час за, який

бажаємо побачити ці спроби. Це допоможе швидко виявити можливі атаки підбору паролю та те коли вони були здійснені (рис. 8.17-8.18).

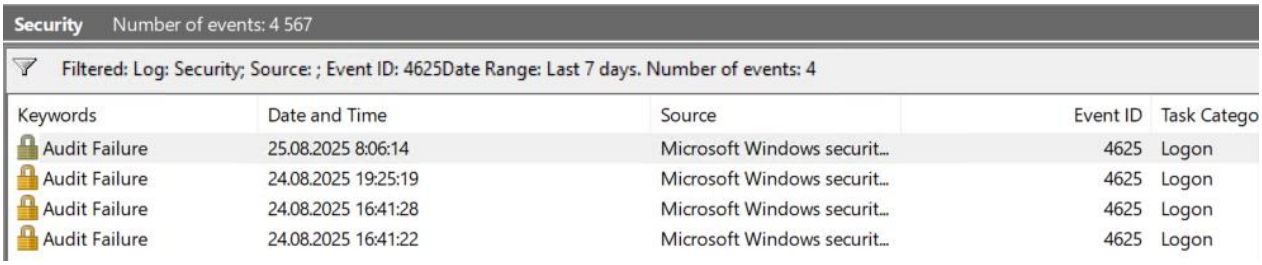

Рисунок 8.17 – Результати фільтрації по коду події «4625»

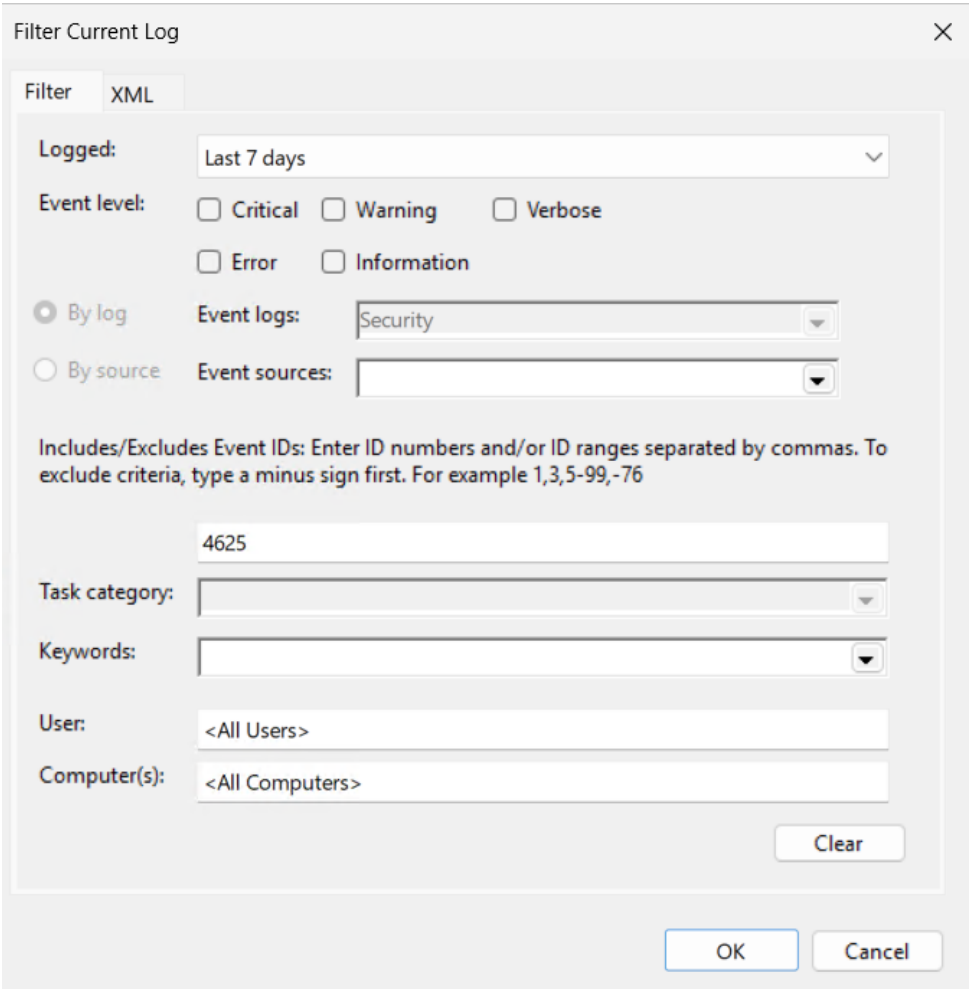

Рисунок 8.18 – Фільтрація подій, для пошуку спроб підбору пароля

Щоб детальніше проаналізувати певну подію безпеки слід скористатися переглядом властивостей події. Для цього двічі натискаємо на потрібну подію у списку і після цього у вікні бачимо дату й час події, ім’я користувача, комп’ютер або IP-адресу джерела. Це дозволяє визначити, хто і звідки намагався увійти, якщо обрати властивості події з кодом «4625» (рис. 8.19).

Рисунок 8.19 – Властивості події безпеки

Аналіз подій журналу безпеки в контексті може вказати, чи відбувалися зловмисні дії по відношенню до сервера. Наприклад, якщо бачимо багато подій «4625» з однієї IP-адреси – це може свідчити про атаку типу «Brute force». Якщо ж бачимо часті події «4648», слід перевірити, чи не використовує хтось скомпрометовані облікові дані.

Для експорту відфільтрованої частини журналу для пізнішого аналізу у правій панелі вибираємо «Зберегти вибрані події як...», зберігаємо у форматі «.evtx», щоб можна було переглядати пізніше або надсилати для аналізу (рис. 8.20).

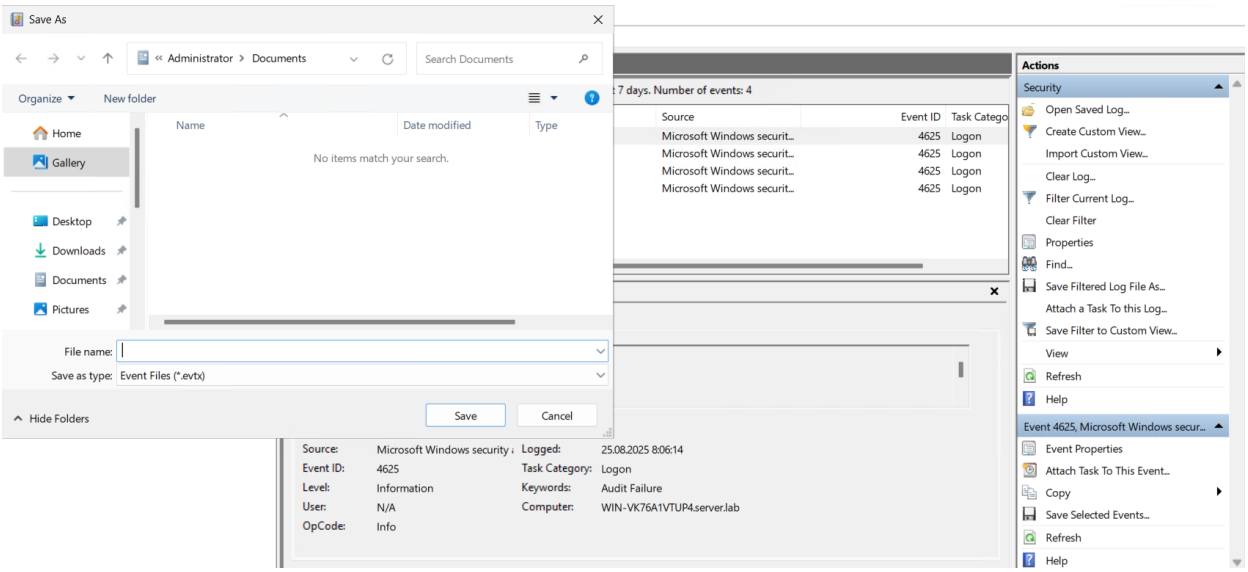

Рисунок 8.20 – Збереження вибраних подій з журналу безпеки

Отож, журнали безпеки є ключовим інструментом для моніторингу підозрілої активності. Їх регулярний аналіз дозволяє вчасно виявити спроби несанкціонованого доступу та запобігти зламу та втраті даних.

Лабораторна робота №9
Налаштування веб-сервера IIS у Windows Server 2025

Мета роботи: закріпити практичні навички встановлення та базового налаштування веб-сервера IIS у середовищі Windows Server 2025, навчитися створювати та конфігурувати сайти й віртуальні директорії, а також опанувати методи ведення та аналізу журналів IIS. Виконання роботи спрямоване на формування розуміння принципів функціонування веб-сервера, його основних компонентів та параметрів, необхідних для розгортання і підтримки веб-додатків у корпоративних інформаційних системах [38-39].

Хід роботи

Завдання 1. Встановлення IIS та базові налаштування

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань першої практичної роботи.

Для встановлення IIS у «Диспетчері серверів» натискаємо «Керування» – «Додати ролі та компоненти». У вікні «Майстра додавання ролей і компонентів» обираємо: тип інсталяції – Інсталяція ролей та компонентів, тиснемо «Далі». Сервер – залишаємо за замовчуванням (наш локальний сервер). У списку ролей ставимо прапорець на «Веб-сервер (IIS)» – потрібній для нас в цій роботі ролі, натискаємо «Додати компоненти» (рис. 9.1).

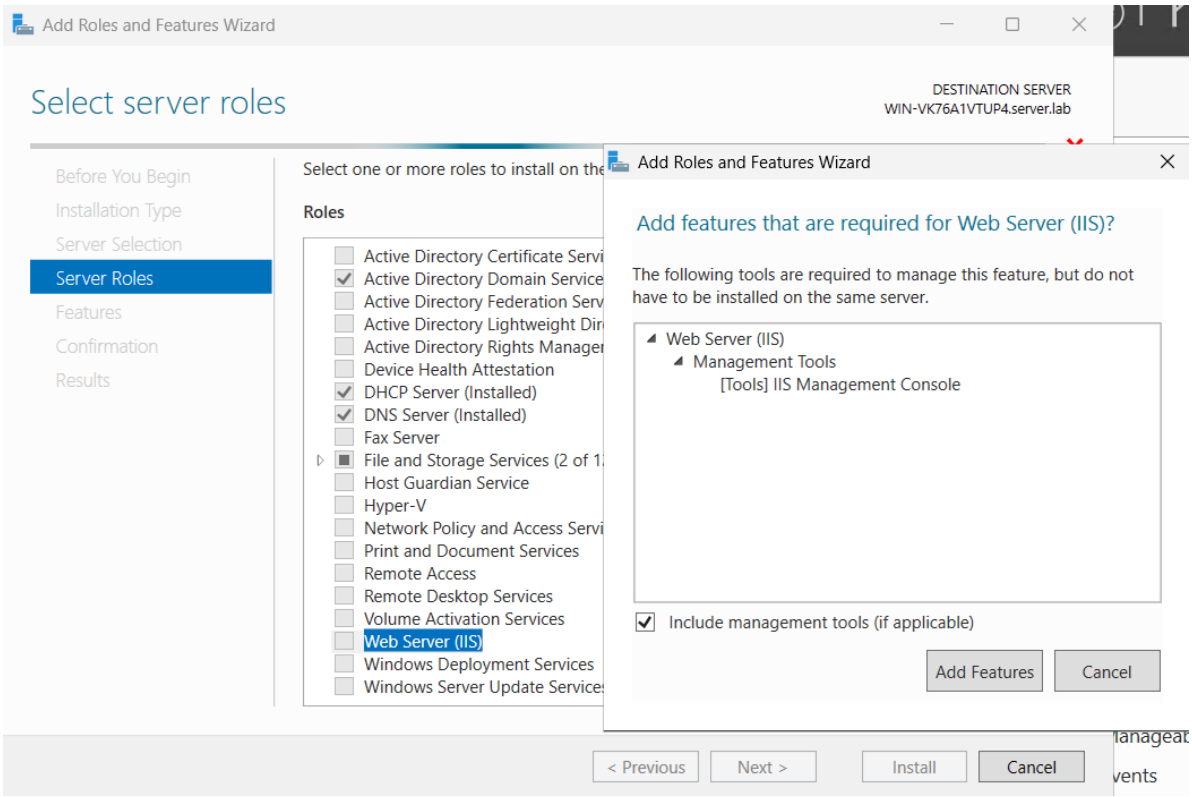

Рисунок 9.1 – Додавання ролі «Веб-сервер (IIS)»

Продовжуємо натискаючи «Далі» на наступних вкладках, поки не з’явиться вкладка «Підтвердження встановлення компонентів», там натискаємо «Встановити» (рис. 9.2).

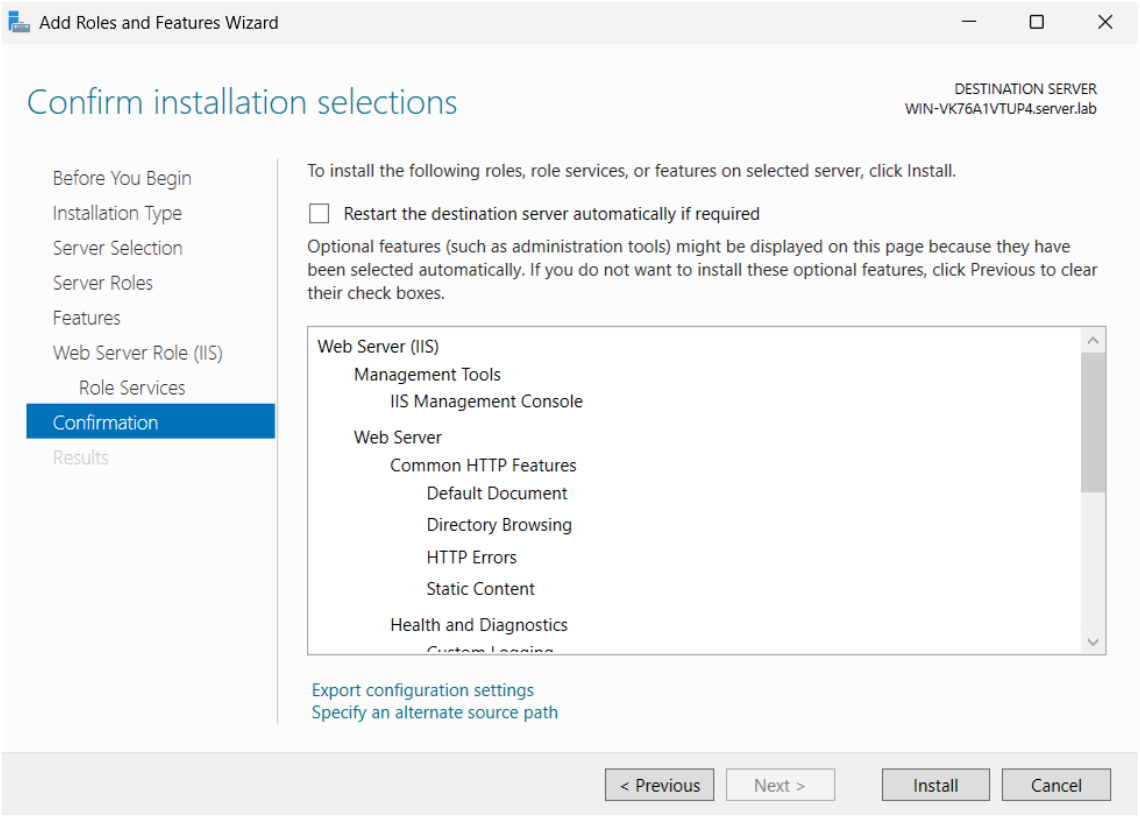

Рисунок 9.2 – Підтвердження встановлення ролі «Веб-сервер (IIS)»

Після цього відбувається процес встановлення, чекаємо його успішного завершення (рис. 9.3).

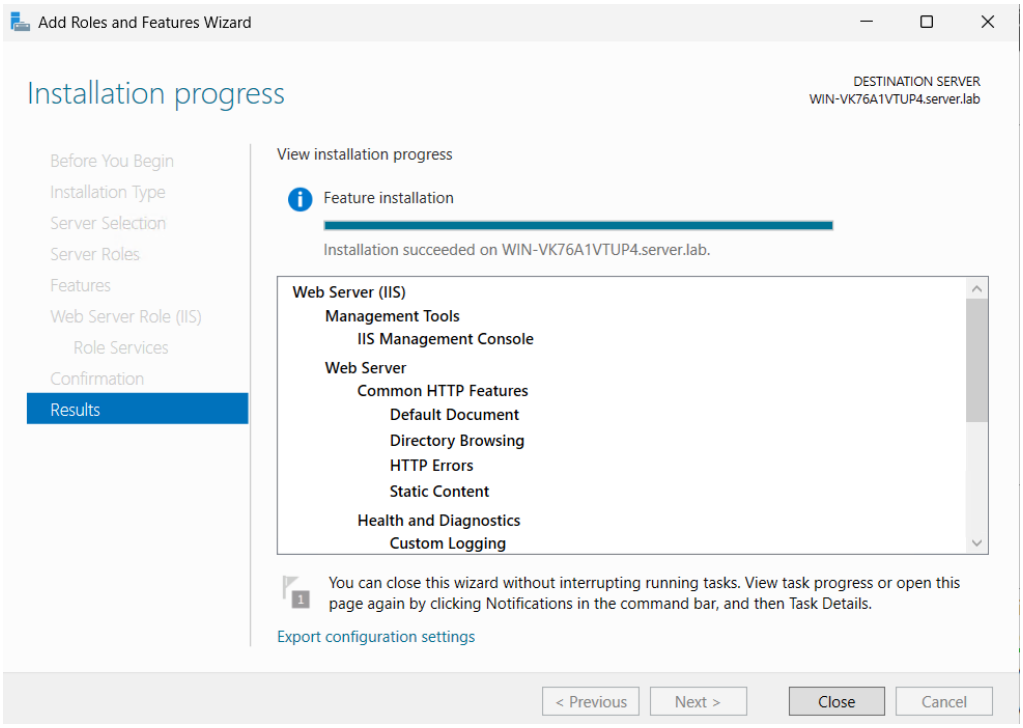

Рисунок 9.3 – Успішне завершення встановлення ролі «Веб-сервер (IIS)»

Після завершення інсталяції відкриваємо «Інструменти» – «Диспетчер служб IIS». У лівій панелі бачимо наш сервер (рис. 9.4).

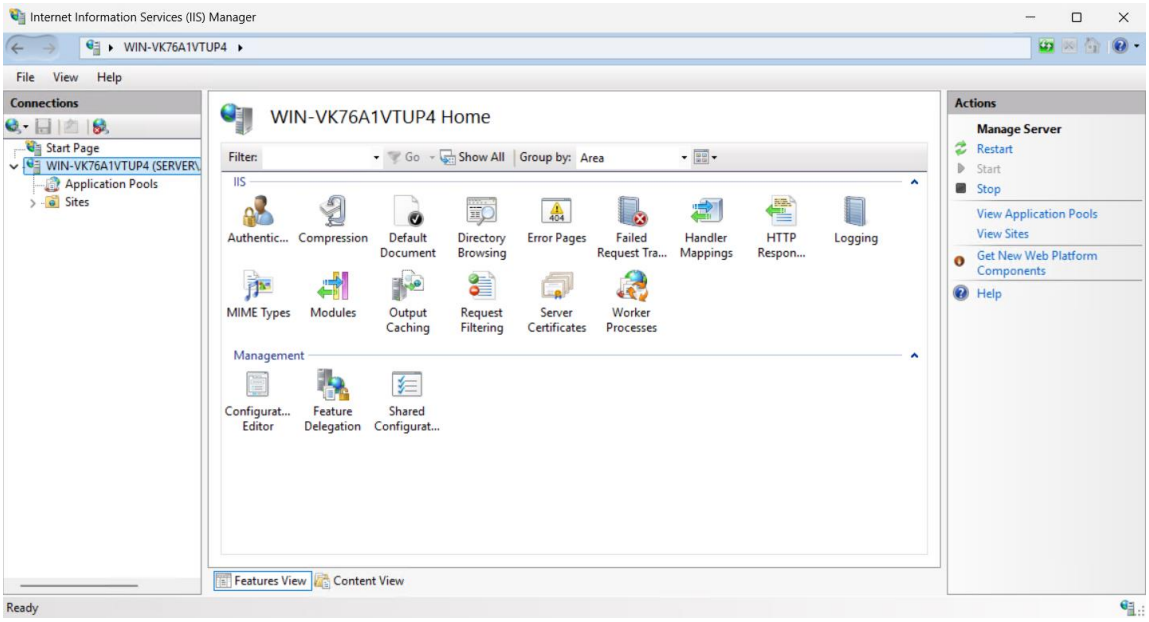

Рисунок 9.4 – Відкритий «Диспетчер служб IIS»

За замовчуванням IIS відразу з встановленням створює сайт Default Web Site. Щоб його відвідати відкриваємо веб-браузер у віртуальній машині й уводимо «http://localhost». В результаті має відкритися стандартна стартова сторінка IIS («Welcome to IIS») (рис. 9.5).

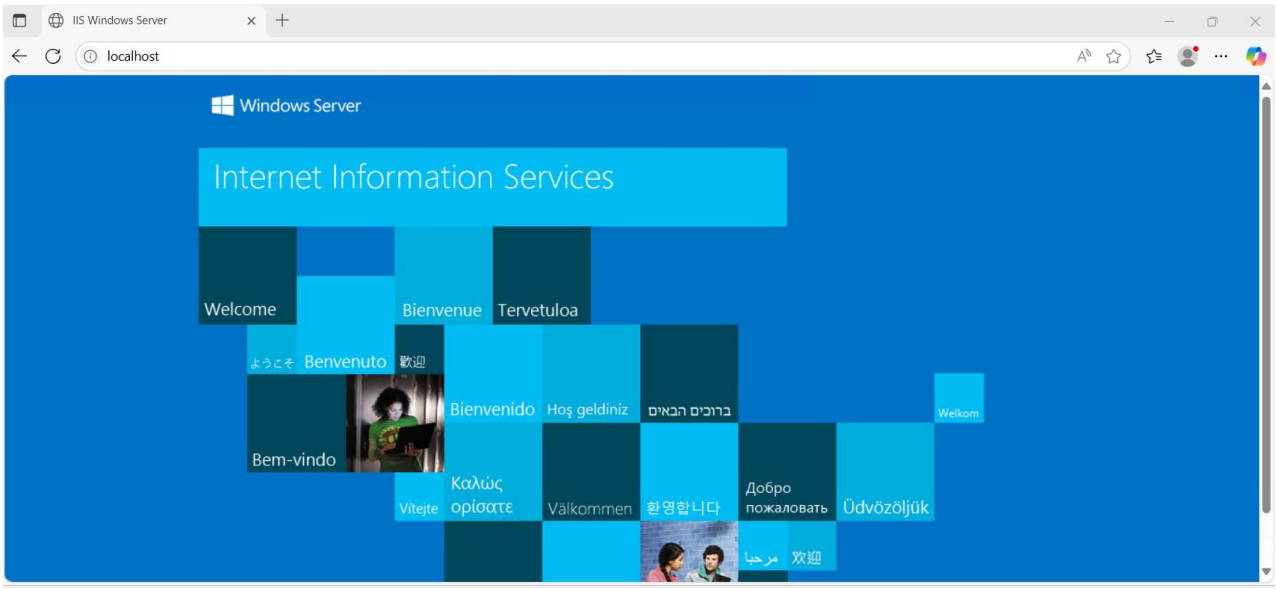

Рисунок 9.5 – Відкрита стартова сторінка IIS в браузері

Щодо базових налаштувань сайту, то у «Диспетчері IIS» можна: переглянути список сайтів (вкладка «Сайти»); зупинити або перезапустити сайт (команди «Запустити» / «Зупинити» / «Перезапустити» у правій панелі). Налаштувати папку, з якої беруться файли сайту («Основні налаштування») (рис. 9.6).

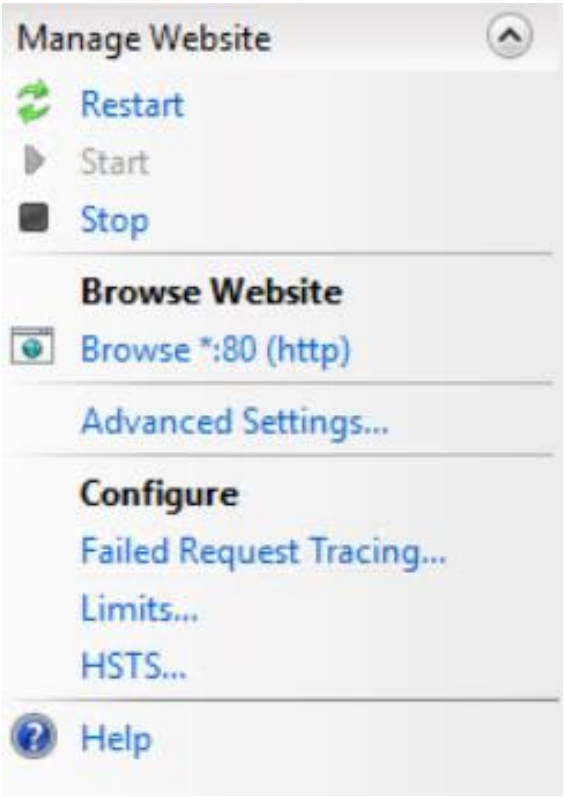

Рисунок 9.6 – Дії, що можна застосувати до веб-сайту в «Диспетчері IIS»

До основних налаштувань IIS належить створення і налаштування пулів застосунків. Для цього натискаємо «Пули застосунків» – ПКМ – «Додати пул застосунків…» (рис. 9.7).

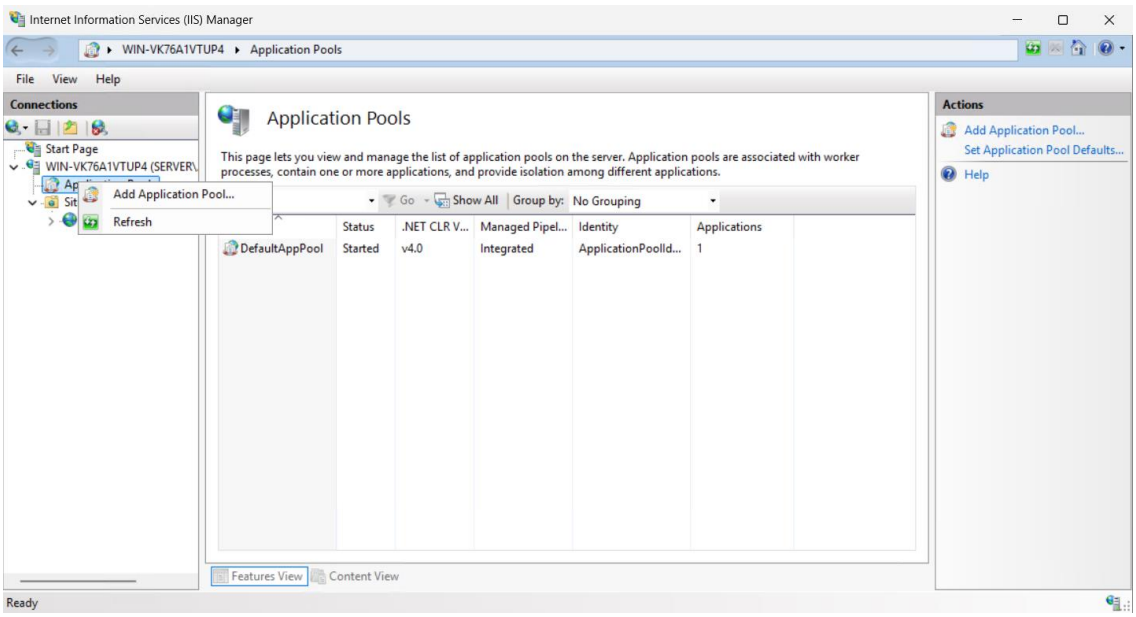

Рисунок 9.7 – Вибір «Додати пул застосунків…»

У вікні, що відкрилося заповнюємо поля: назва – «StudentPool», версія середовища .NET CLR – залишаємо без змін; режим керованого конвеєра – «Вбудований» (рис. 9.8).

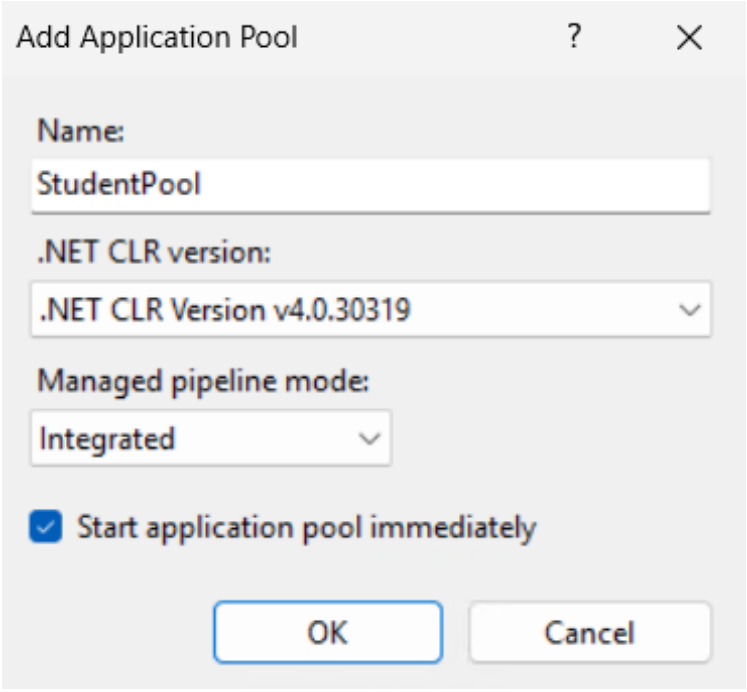

Рисунок 9.8 – Додавання пула застосунків

В результаті створюється новий пул застосунків, змінити його налаштування можна натиснувши ПКМ по назві пула та вибравши «Основні налаштування».

До базових налаштувань також відноситься налаштування базових параметрів сайту. Для цього тиснемо «Сайти» – обираємо Default Web Site або інший сайт за потреби та вибираємо у меню «Дії» тиснемо «Основні параметри…». Внаслідок цього відкривається вікно змін налаштувань веб-сайту (рис. 9.9).

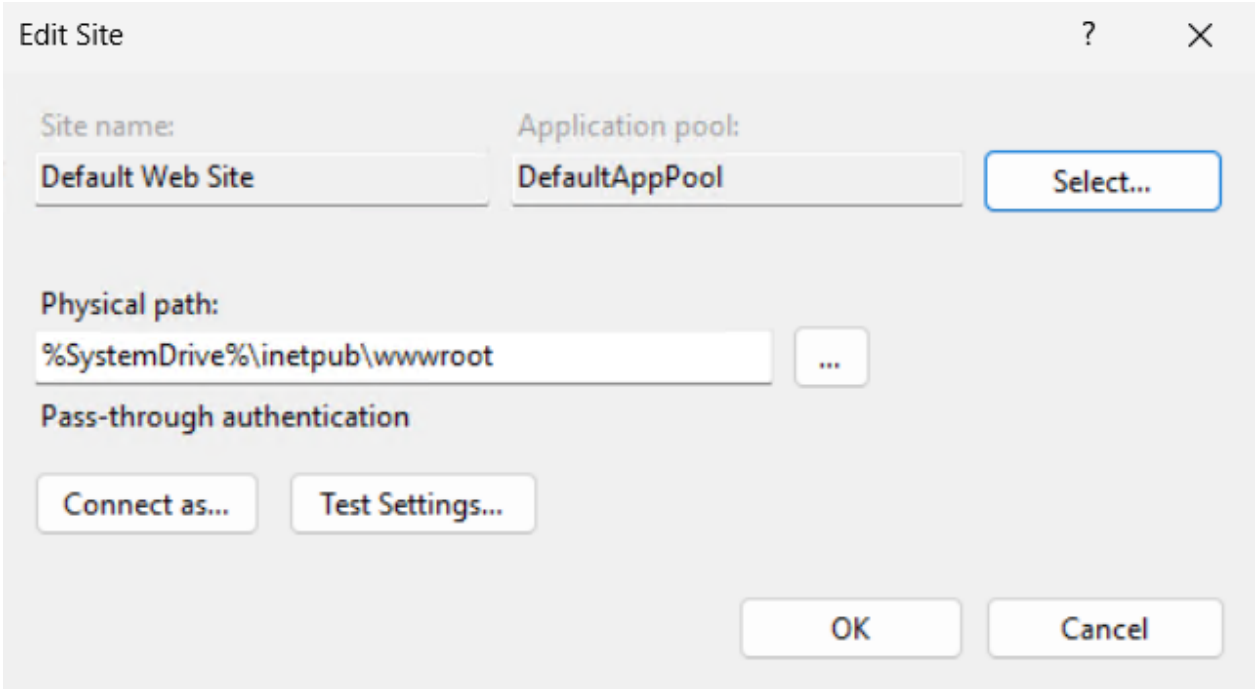

Рисунок 9.9 – Вікно «Змінення веб-сайту»

Проводимо зміни: пул застосунків обираємо «StudentPool», фізичний шлях укажемо «C:\sites\student» та тиснемо «ОК» (рис. 9.10).

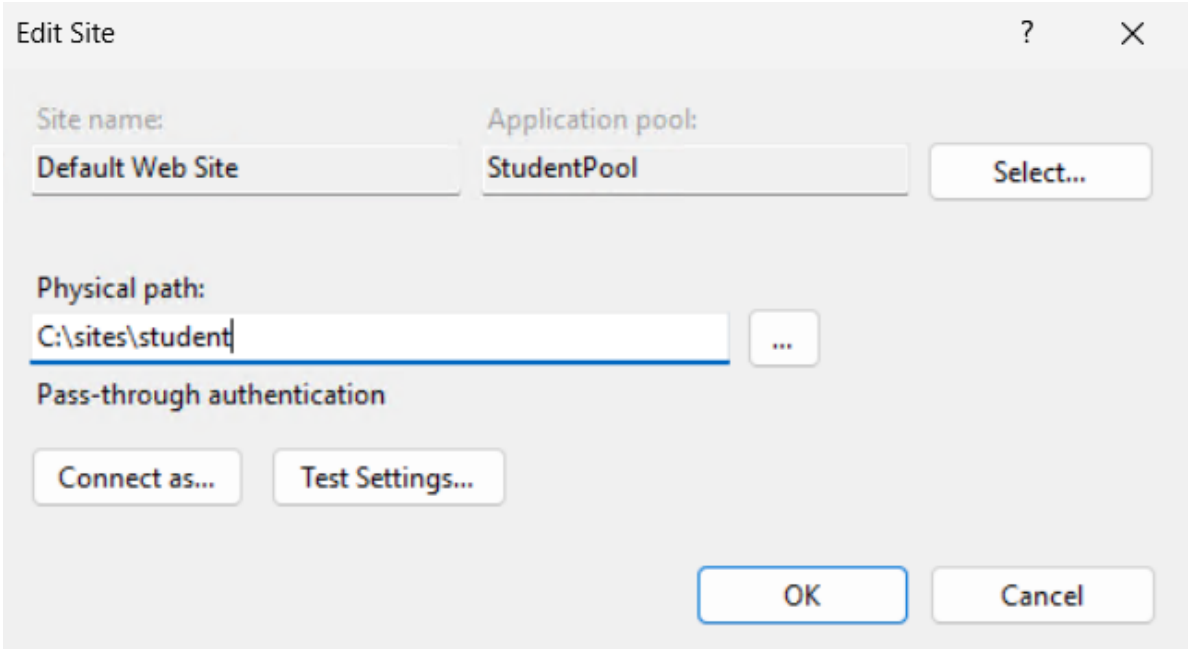

Рисунок 9.10 – Проведені зміни налаштувань сайту

Також основними налаштуваннями є налаштування прив’язки сайту: порт, IP, хост-заголовок. Для зміни цих параметрів натискаємо на сайт, до якого слід застосувати зміни, в меню «Дії» обираємо «Прив’язки…», у новому вікні, що відкрилося тиснемо «Додати» (рис. 9.11).

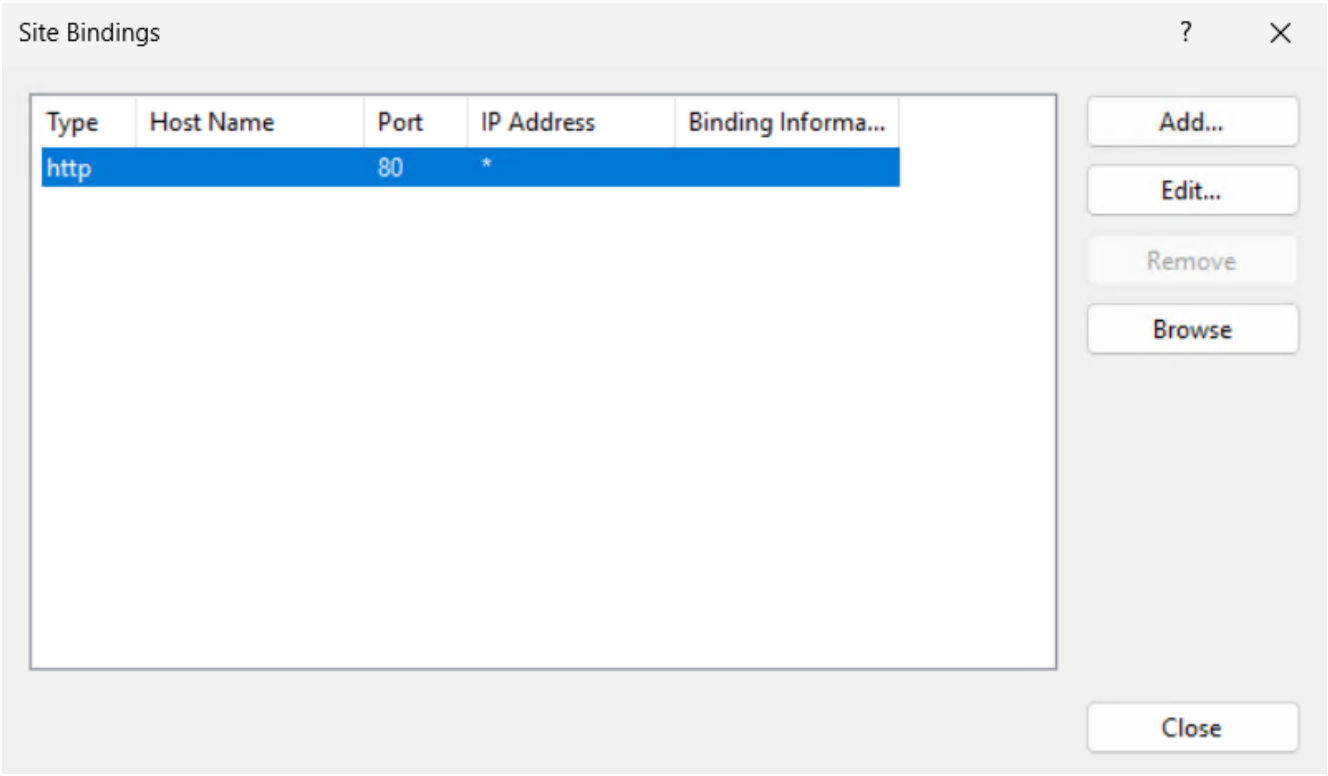

Рисунок 9.11 – Вікно «Прив’язки сайту»

Відкривається вікно налаштувань прив’язок сайту. Вибираємо протокол «http», IP-адреса: «172.30.243.252», порт: 8080, ім’я вузла, наприклад, «student1.local». Після зміни потрібних налаштувань тиснемо «ОК» (рис. 9.12).

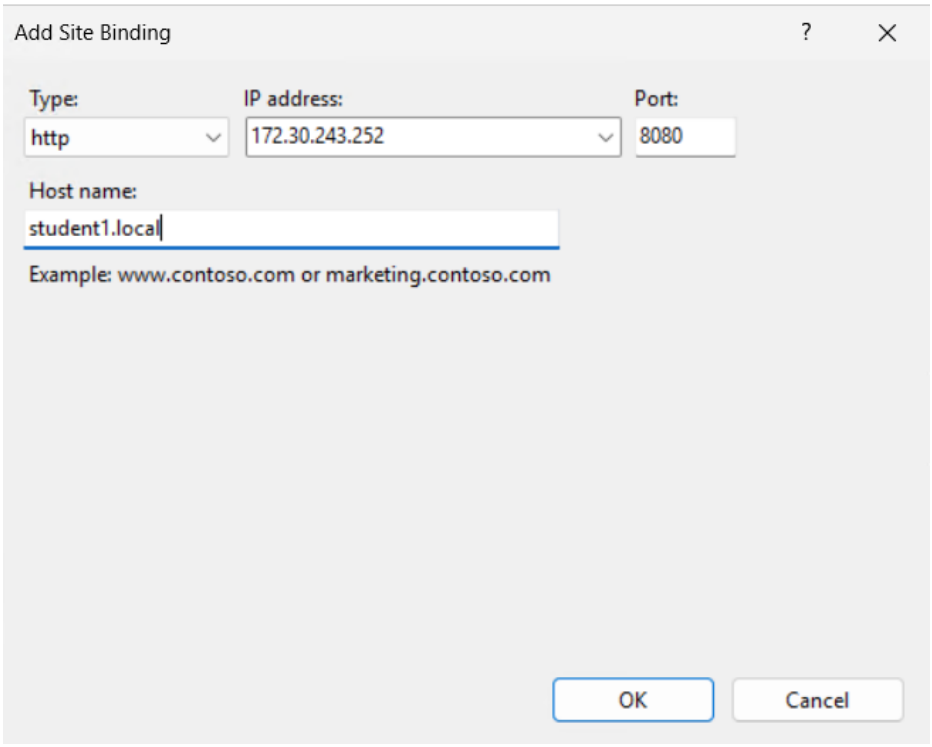

Рисунок 9.12 – Зміна прив’язки сайту

Основними налаштуваннями є і робота з документами за замовчуванням. Для їх налаштування натискаємо на назву потрібного сайту, та двічі тиснемо по піктограмі «Документи за замовчуванням», відкривається нове вікно, де відображені назви документів. Порядок документів зверху вниз – означає пріоритет (рис. 9.13).

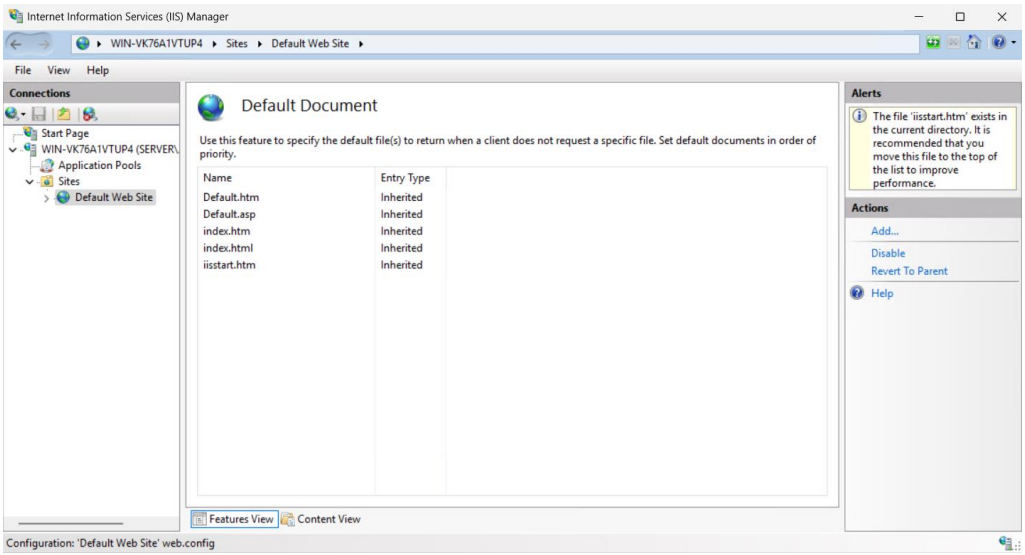

Рисунок 9.13 – Вікно «Документи за замовчуванням»

Для зміни порядку потрібно підняти потрібний документ вище, над іншими. Приклад: додаємо main.html («Дія» – «Додати…»), піднімаємо цей

документ вище за Default.htm/Default.aspx та інші. Якщо у корені сайту є main.html та default.aspx, відкриється main.html, бо він вище в списку (рис. 9.14).

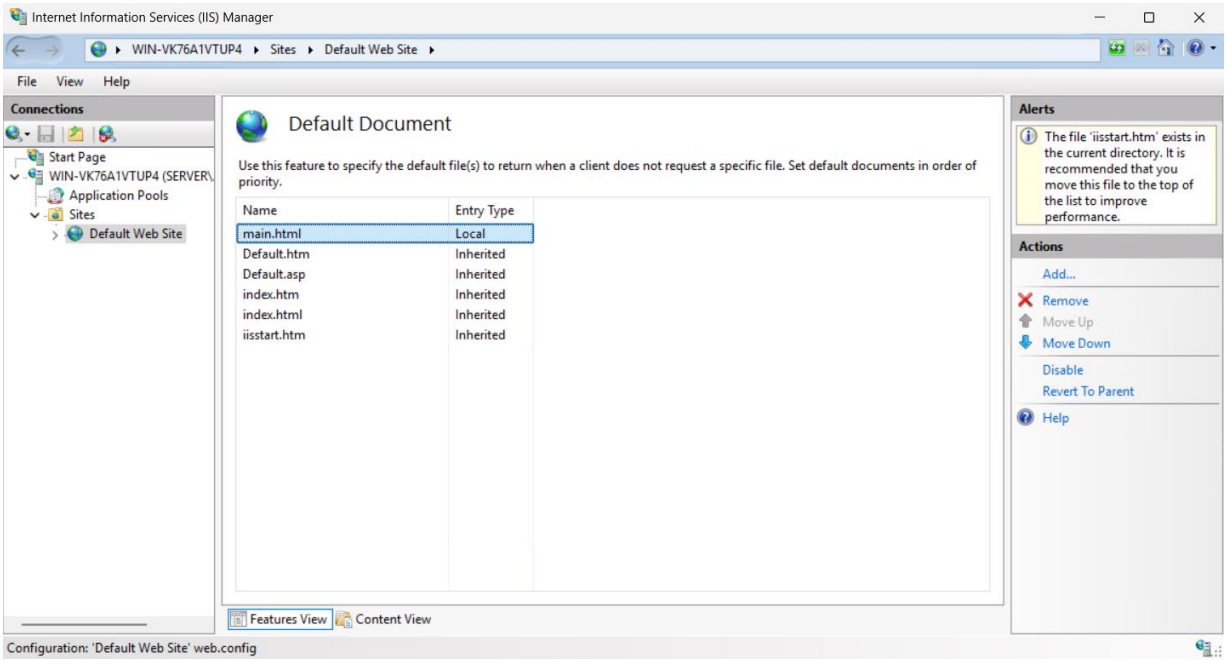

Рисунок 9.14 – Редагування порядку документів за замовчуванням

Отож, ми детально налаштували ключові параметри IIS: пули застосунків, прив'язки, документи за замовчуванням. З такими базовими налаштуваннями сервер готовий до подальшого більш детального та специфічного налаштування та розміщення веб-додатків.

Завдання 2. Додавання сайтів та віртуальних директорій

Для додавання нового сайту або ж створення нового сайту перебуваючи в «Диспетчері служб IIS», у лівій панелі («Підключення») розгортаємо вузол нашого сервера. Клацаємо правою кнопкою миші на папці «Сайти» – «Додати веб-сайт» (рис. 9.15).

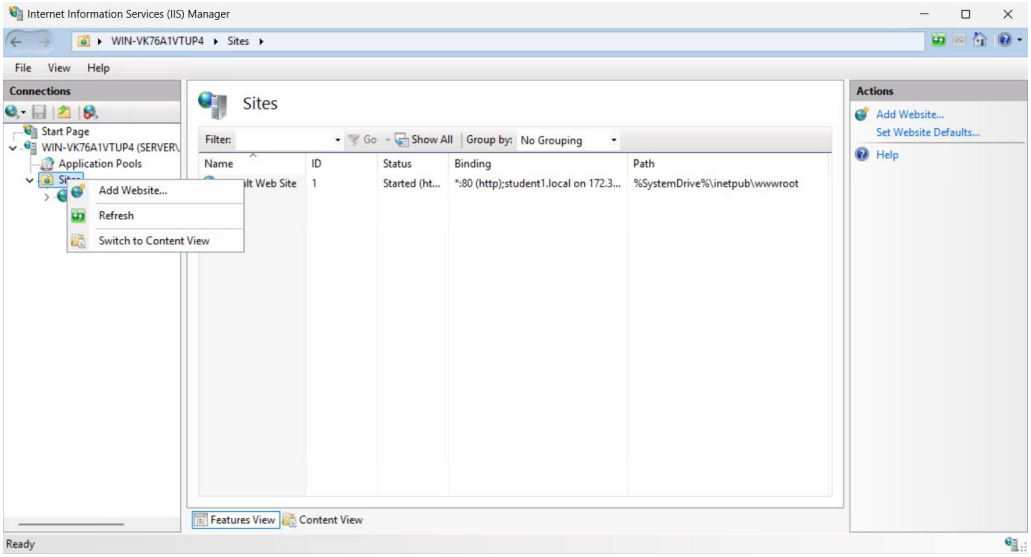

Рисунок 9.15 – Початок додавання веб-сайту

У вікні, що відкрилося вказуємо назву сайту, наприклад, «StudentSite», фізичний шлях – обираємо папку, де зберігаються файли сайту, наприклад – C:\sites\student, прив’язка – залишаємо http, IP-адреса – за замовчуванням, порт – 80. Після заповнення цих полів натискаємо «ОК» (рис. 9.16).

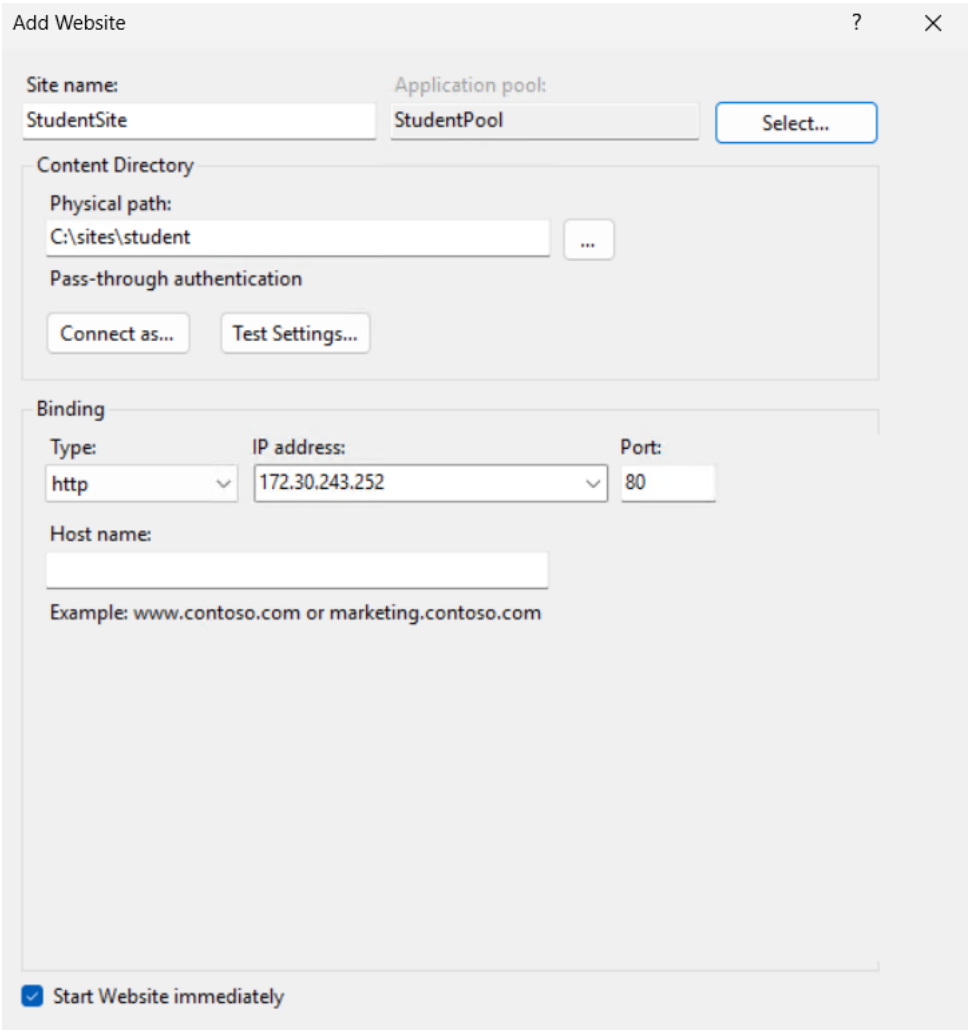

Рисунок 9.16 – Вікно додавання веб-сайту

Після цього у списку сайтів з’явився новий, створений нами сайт (рис. 9.17).

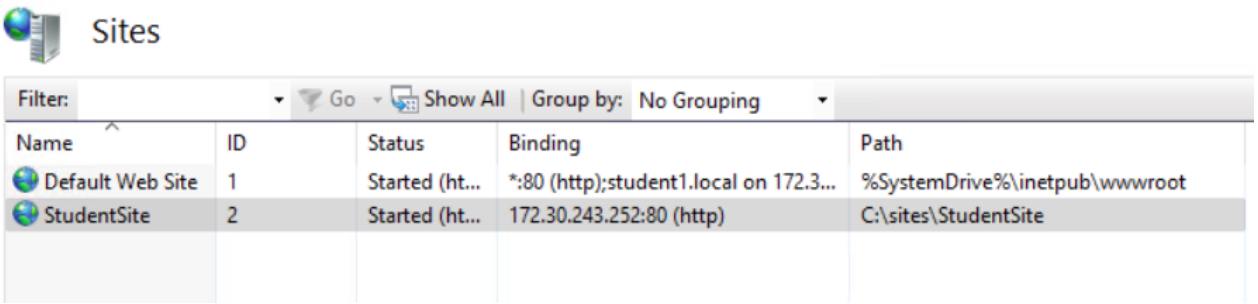

Рисунок 9.17 – Список сайтів

Для додавання контенту на доданий сайт переходимо у папку, яку вказали для сайту (C:\sites\student). Створюємо файл index.html з простим вмістом (рис. 9.18).

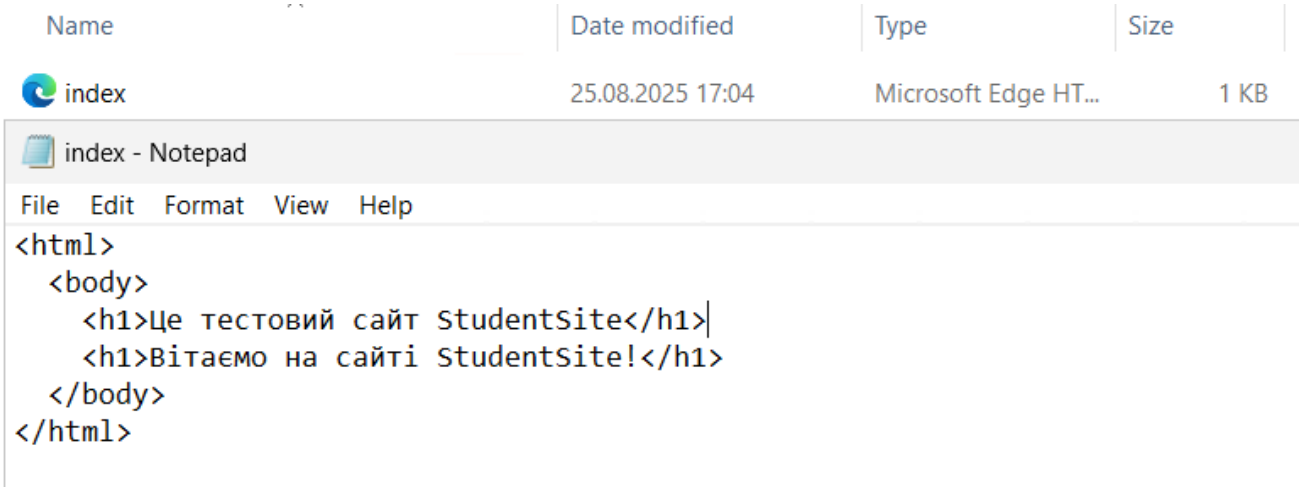

Рисунок 9.18 – Приклад створення та вмісту файлу index.html

Після створення та збереження файлу, у браузері вводимо «http://localhost», щоб перевірити роботу та вміст нового сайту (рис. 9.19).

Рисунок 9.19 – Відображення доданого сайту в браузері

Для додавання віртуальної директорії у «Диспетчері служб IIS» розгортаємо «Сайти» – «StudentSite». Правою кнопкою миші натискаємо на назві сайту та обираємо «Додати віртуальний каталог» (рис. 9.20).

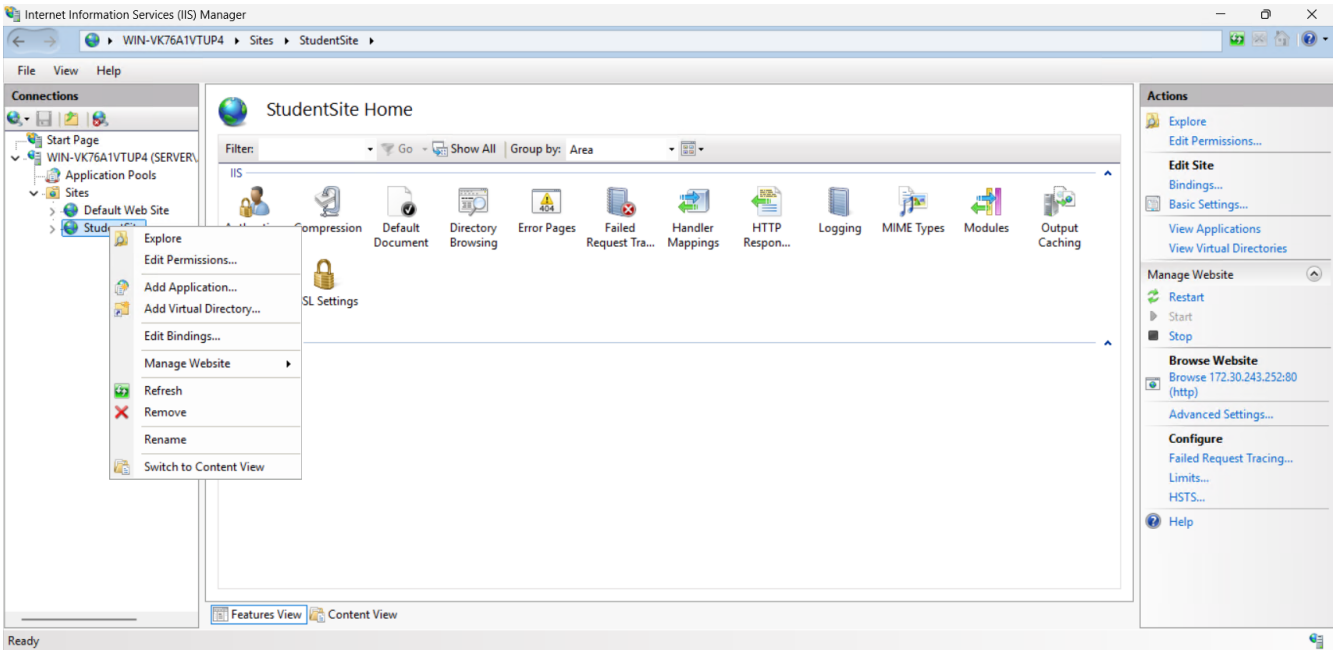

Рисунок 9.20 – Вибір «Додати віртуальний каталог»

Відкривається нове вікно. В полі «Псевдонім» пишемо, наприклад: images. У полі «Фізичний шлях» вказуємо папку, наприклад:

C:\sites\student\images. Після заповнення необхідних полів натискаємо «ОК» (рис. 9.21).

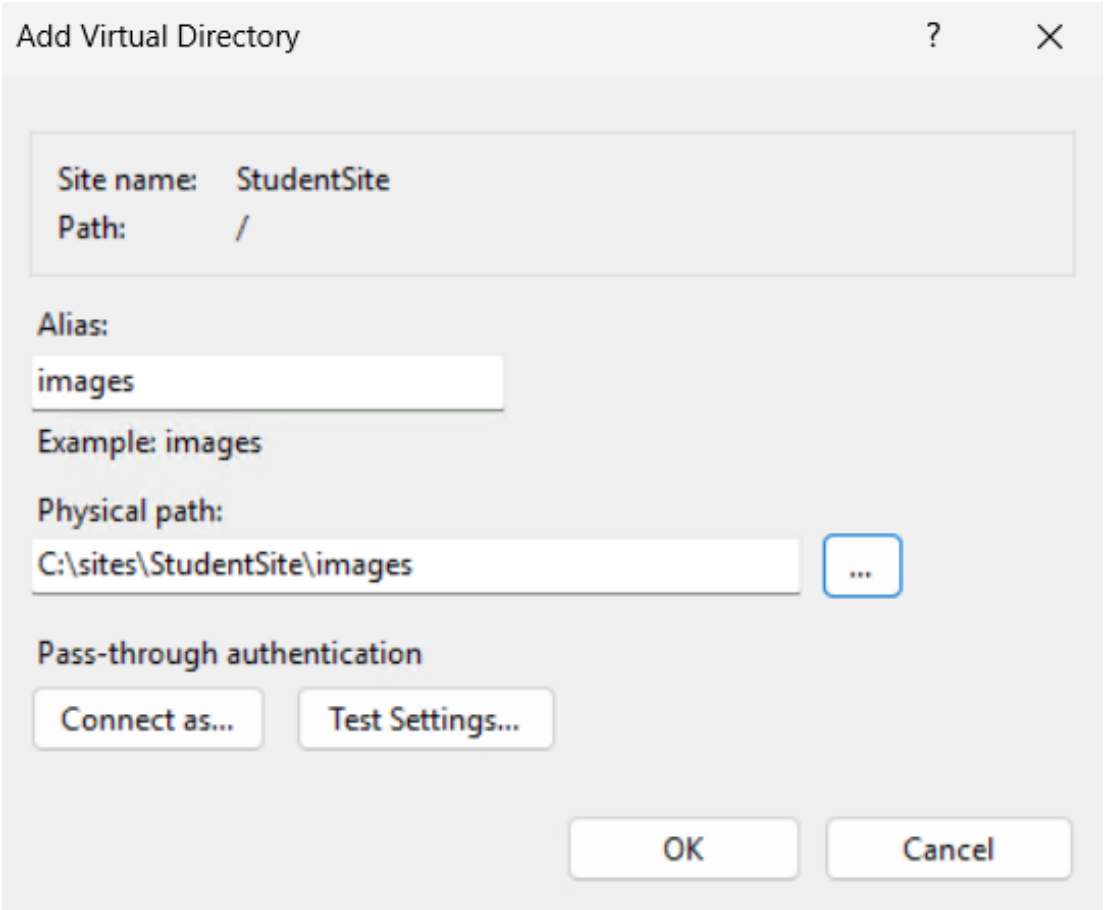

Рисунок 9.21 – Додавання віртуального каталога (директорії)

Для здійснення перевірки роботи віртуального каталогу у папку C:\sites\student\images додаємо будь-який файл (наприклад, картинку test.jpg). У браузері вводимо «file:///C:/sites/StudentSite/images/test.jpg», в результаті коректної роботи файл має відкритися напряму через IIS (рис. 9.22).

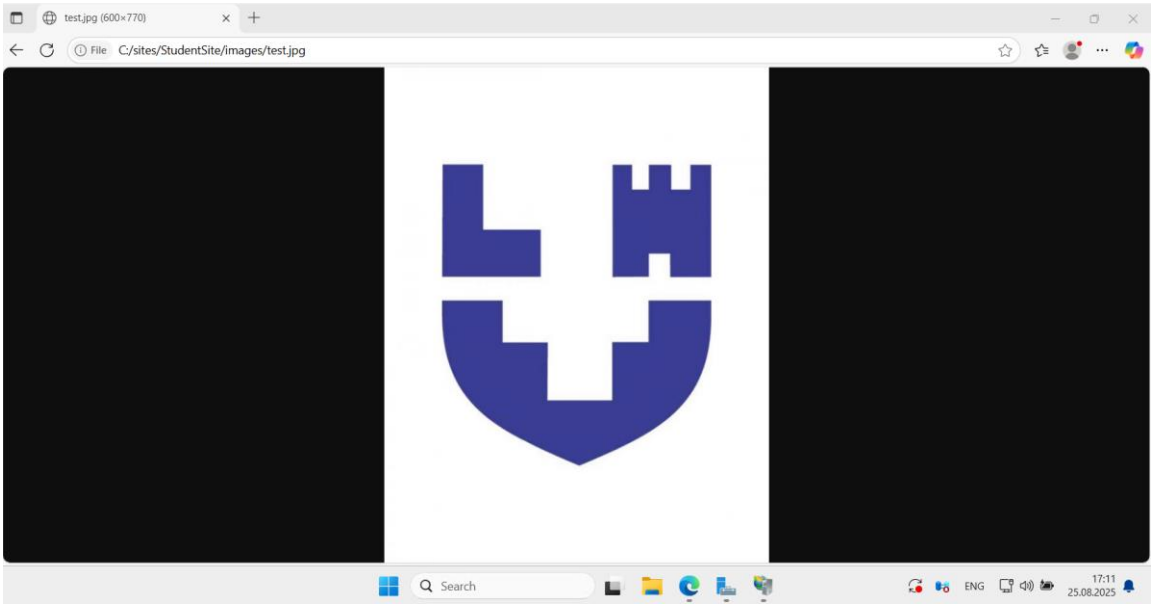

Рисунок 9.22 – Перевірка доданої віртуальної директорії

Завдання 3.Аналіз журналів IIS

Для роботи з журналами IIS відкриваємо «Диспетчер служб IIS», у лівій панелі вибираємо наш сервер, у центральному вікні переходимо до розділу «Ведення журналу» (рис. 9.23).

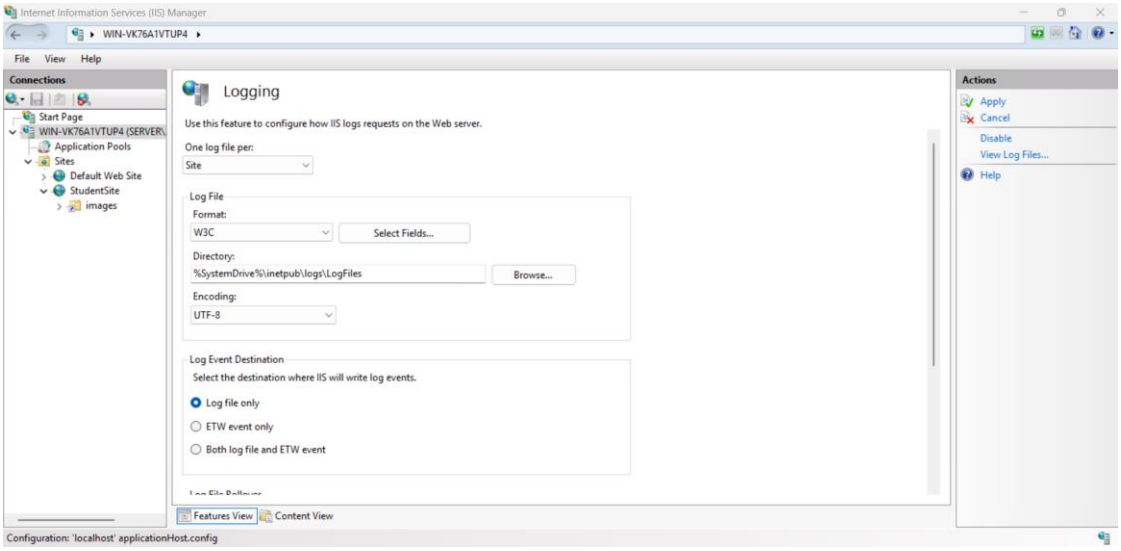

Рисунок 9.23 – Вікно «Ведення журналу»

У вікні «Ведення журналу» бачимо формат файлів журналу (W3C, IIS, NCSA), можливість вибору полів для записів у журналі, шлях до папки з файлами, тип кодування.

Для відкриття журналів IIS, переходимо до папки з журналами у «Провіднику». Усередині є підпапки виду W3SVC1, W3SVC2 (кожна відповідає окремому сайту). Відкриваємо файл у «Блокноті» або Excel для зручності (рис. 9.24).

Рисунок 9.24 – Відкритий файл журналу IIS

Щодо структури журналу, то у файлі бачимо колонки: date – дата запиту; time – час; c-ip – IP-адреса клієнта; cs-method – метод (GET, POST); cs-uri-stem – шлях до ресурсу (наприклад, /index.html); sc-status – код відповіді сервера (200 – успіх, 404 – не знайдено, 500 – помилка сервера); sc-bytes – розмір відповіді.

Аналізуючи журнал веб-сервера IIS, можемо зробити наступні висновки. Якщо бачимо багато рядків із кодом 404, значить клієнти намагаються відкрити неіснуючі сторінки. Якщо з’являються коди 500 або 503 – є проблеми з самим IIS чи веб-додатком. Якщо дуже багато запитів з однієї IP-адреси – можлива спроба DoS-атаки.

У «Диспетчері служб IIS» журнали можна змінити: формат журналу, які поля записуються, період створення нового файлу (щодня, щотижня). Для зручності аналізу можна імпортувати журнали у Excel і будувати фільтри (наприклад, показати лише рядки з кодом 404).

Лабораторна робота №7
Налаштування Linux у віртуальному середовищі

Мета роботи: опанувати процес встановлення та базового налаштування серверної операційної системи Linux у віртуальному середовищі, сформувати практичні навички роботи з користувачами, групами та їх правами доступу, а також засвоїти принципи автоматизації адміністративних завдань за допомогою Bash-скриптів. Виконання роботи спрямоване на розвиток компетентностей у розгортанні та адмініструванні Linux-систем, що є основою для подальшого вивчення серверних технологій та мережевої інфраструктури [15-18].

Хід роботи

Завдання1. Встановлення та базове налаштування Linux

В цій роботі досліджуватимемо серверну операційну систему Linux Server. Встановимо дану ОС на віртуальну машину Oracle VM VirtualBox. Для цього попередньо слід завантажити ISO-образ Linux Server на комп'ютер. Коли все готово, відкрити середовище Oracle VM VirtualBox та натиснути «Створити» і починається створення нової віртуальної машини. Надати назву ВМ, вказати папку зберігання файлів цієї ВМ, а також ISO-образ Linux Server (рис. 10.1).

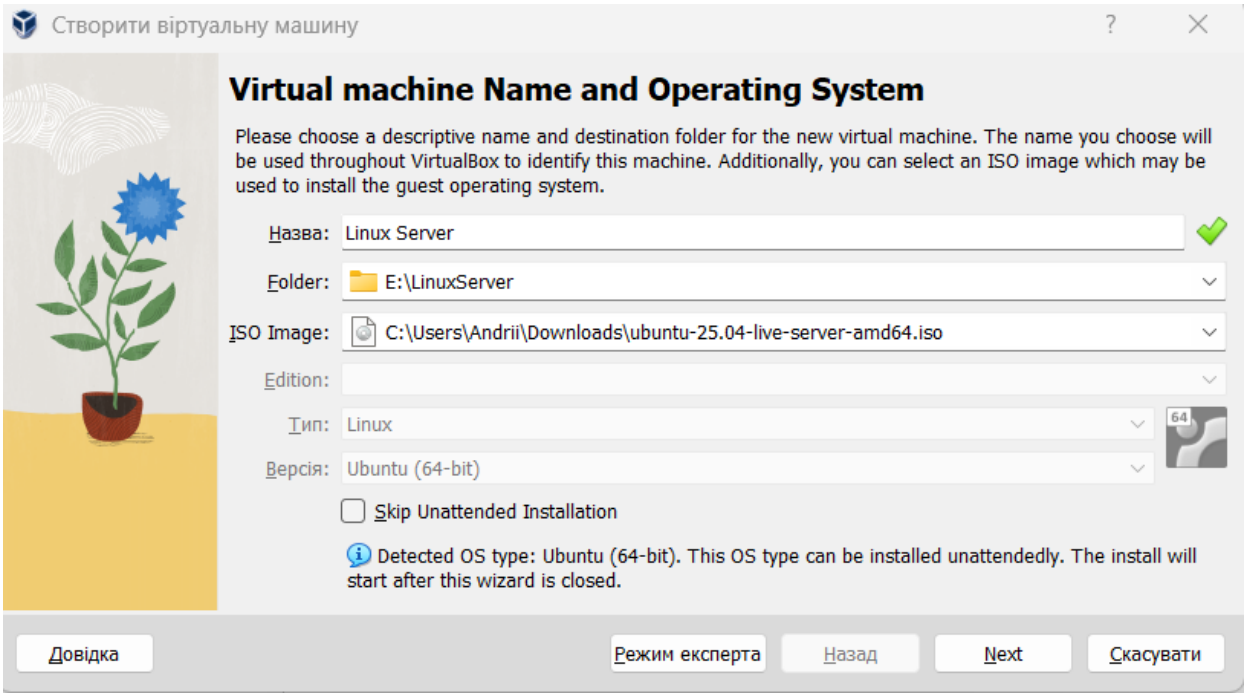

Рисунок 10.1 – Створення нової ВМ Linux Server

Після цього на наступній вкладці провести налаштування адміністраторського облікового запису користувача. Далі виділити оперативну пам'ять для ВМ (мінімальний обсяг 4096 МБ) та кількість ядер процесора (мінімальний обсяг 2 ядра) (рис. 10.2).

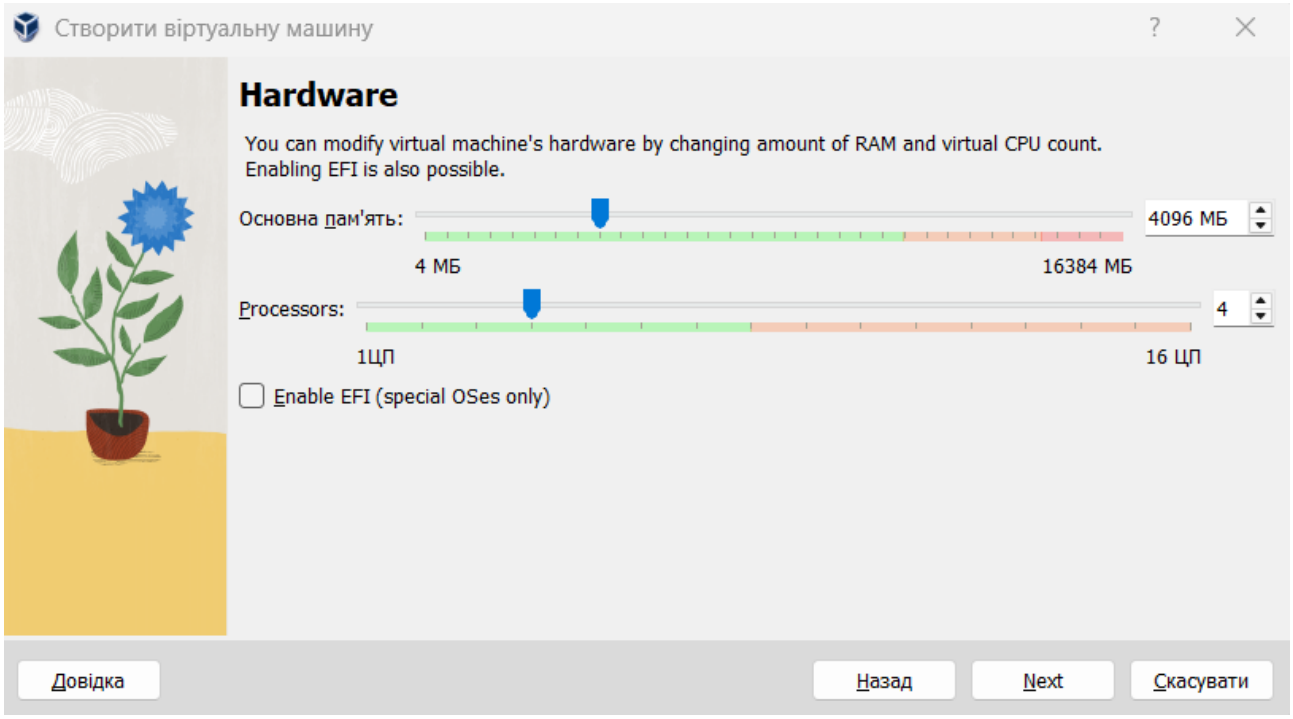

Рисунок 10.2 – Виділення ОП та ядер процесора для ВМ

Далі створити віртуальний жорсткий диск та вказати його розмір (мінімальний розмір 30 ГБ) (рис. 10.3).

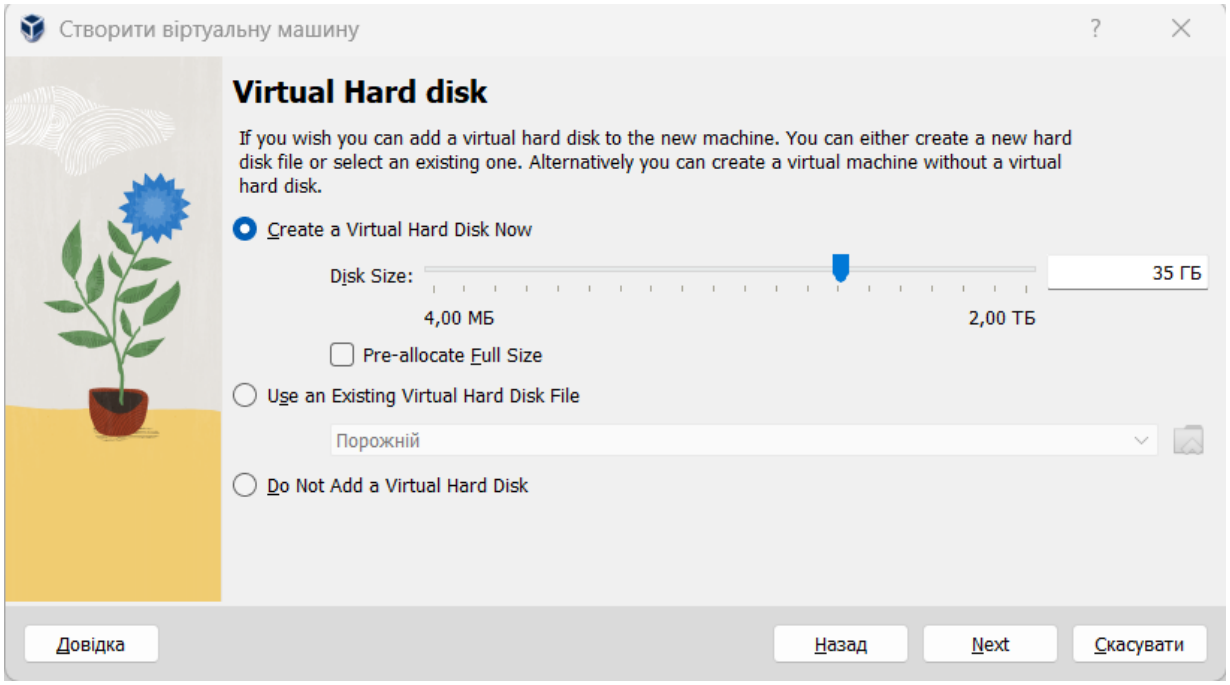

Рисунок 10.3 – Створення віртуального жорсткого диска

На наступній вкладці натиснути «Закінчити». Після цього автоматично запускається створена ВМ (рис. 10.4).

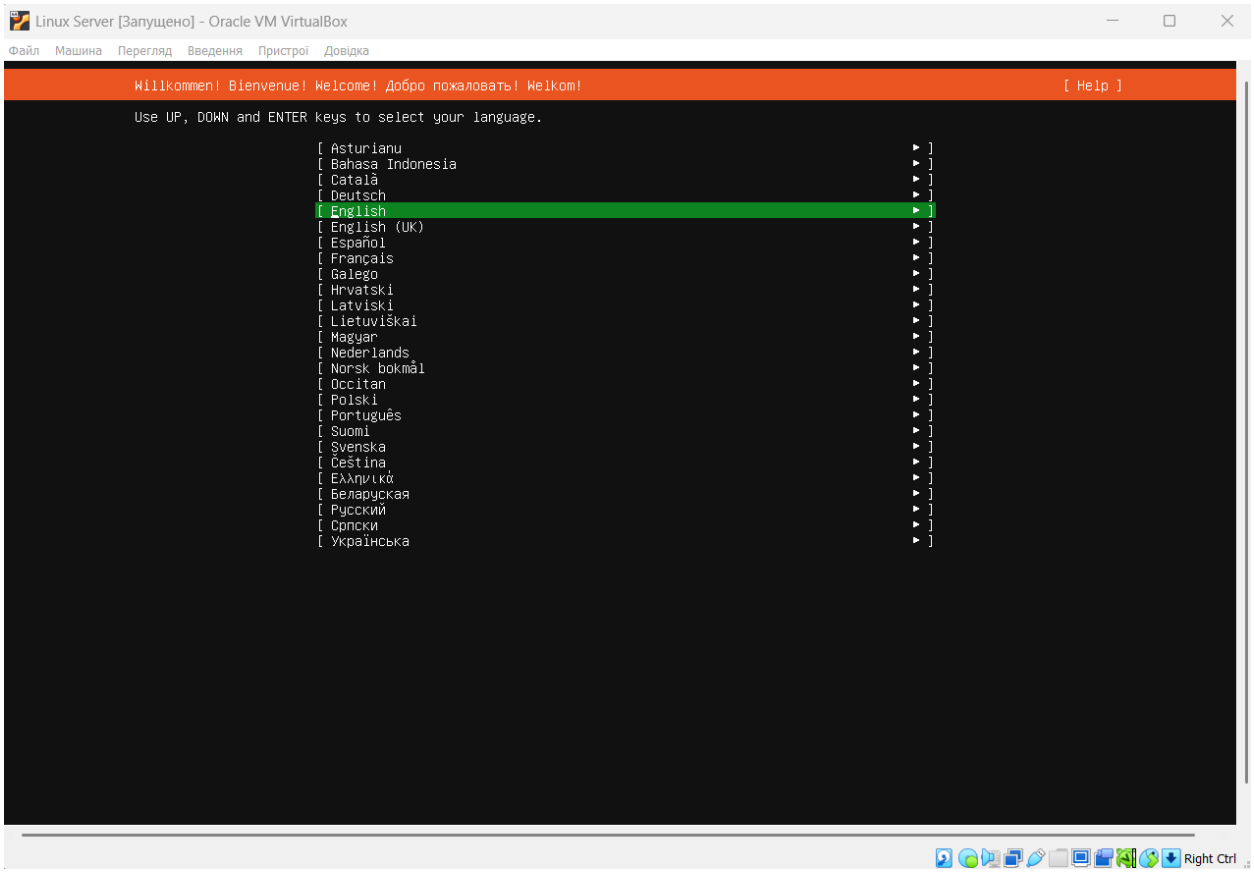

Рисунок 10.4 – Перший запуск ВМ для встановлення ОС

Запускається стандартне встановлення ОС Linux Server. На першому етапі вибирається мова – «Українська» та натиснути «Enter». В наступній вкладці «Налаштування клавіатури» налаштування підтягнуться автоматично, відповідно до встановленої попередньо мови. Натиснути «Виконано» (рис. 10.5).

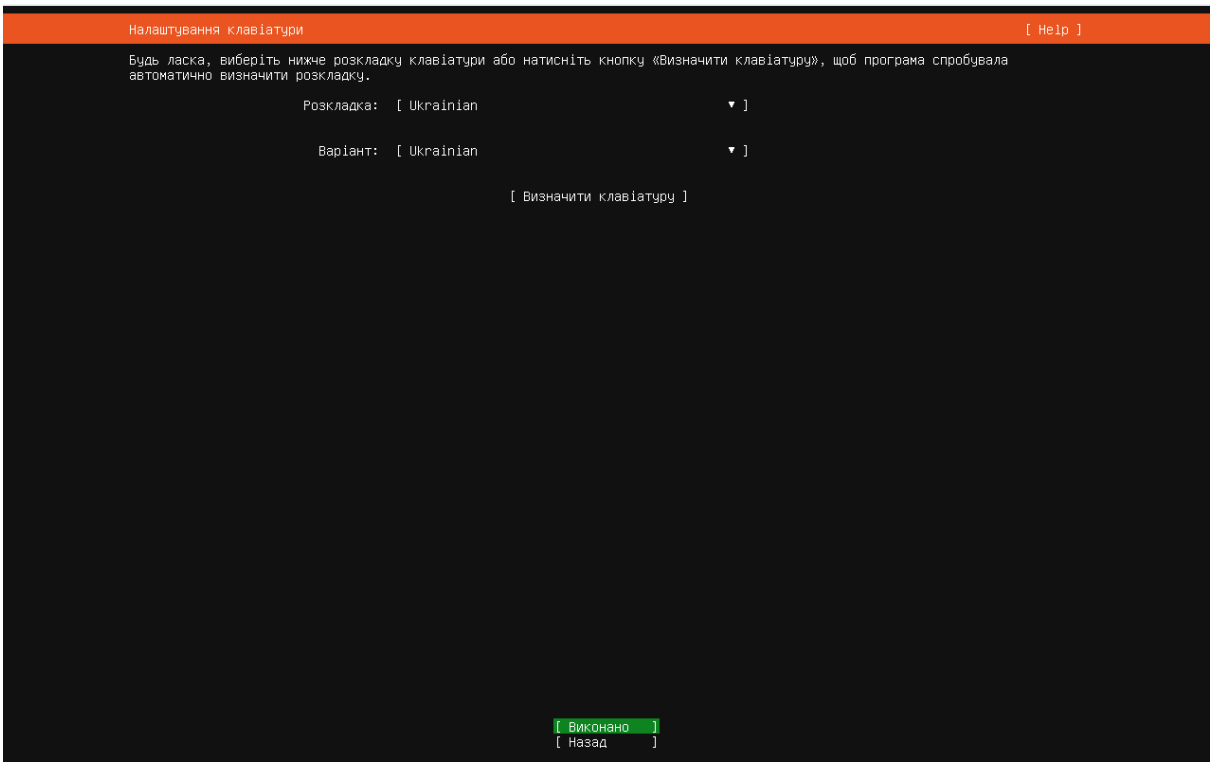

Рисунок 10.5 – Налаштування мови та клавіатури для Linux Server

В наступній вкладці вибирати тип інсталяції – «Ubuntu Server» і знову натиснути «Enter», щоб підтвердити вибір та перейти далі (рис. 10.6).

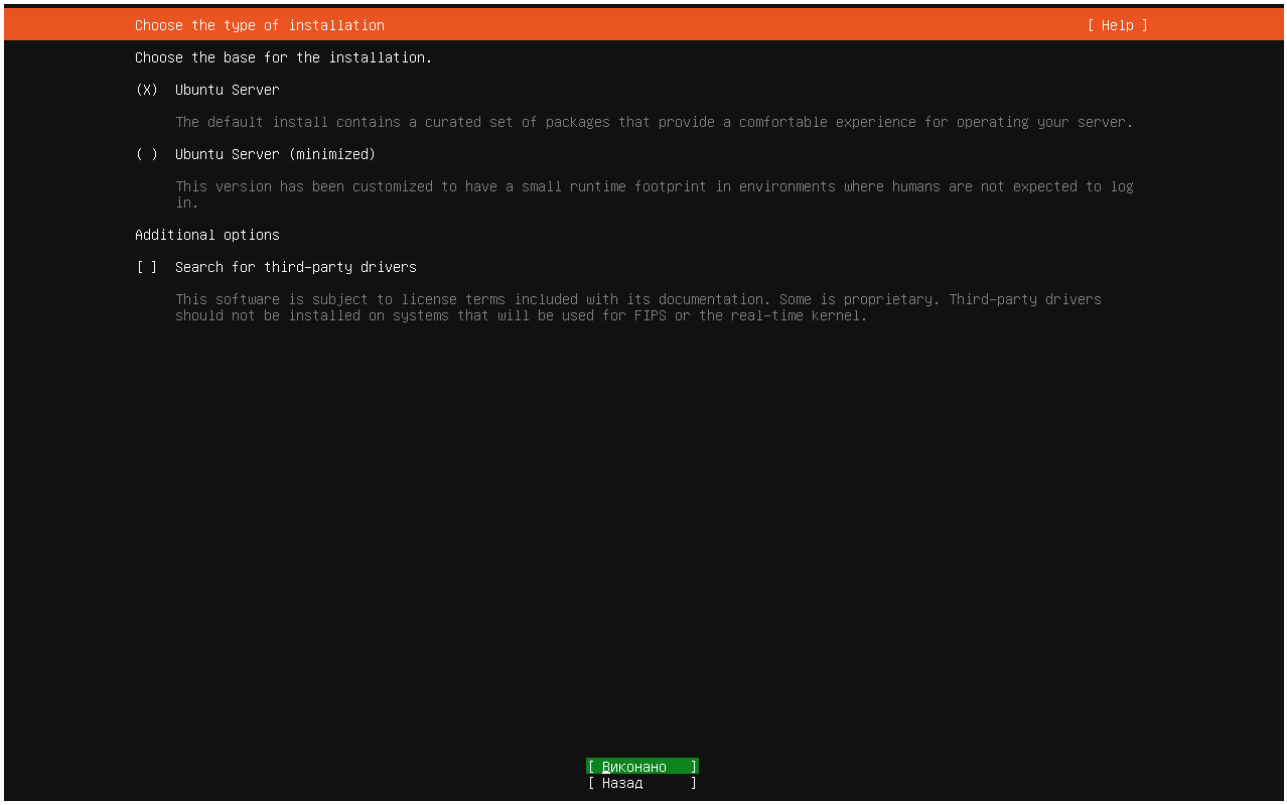

Рисунок 10.6 – Налаштування типу інсталяції для Linux Server

Потім провести початкові налаштування мережевої конфігурації, на цьому етапі все залишаємо без змін та натиснути «Enter» (рис. 10.7).

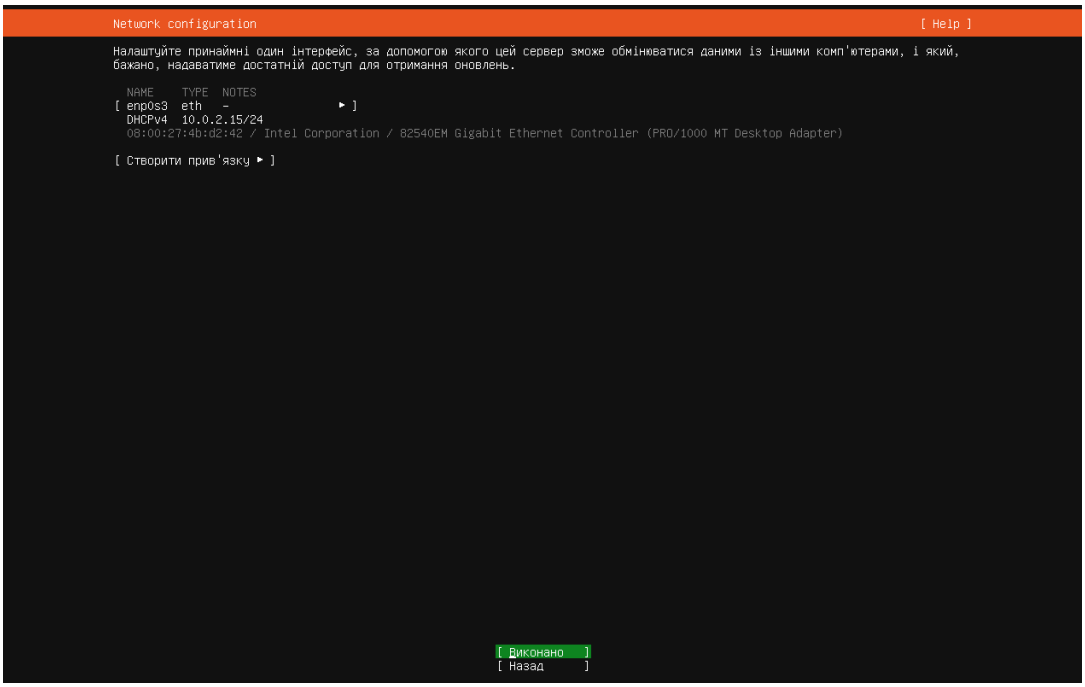

Рисунок 10.7 – Налаштування мережевої конфігурації для Linux Server

В наступній вкладці адресу проксі сервера залишити без змін та просто натиснути «Виконано». Далі «Адреса дзеркала» залишити за замовчуванням і перейти далі (рис. 10.8).

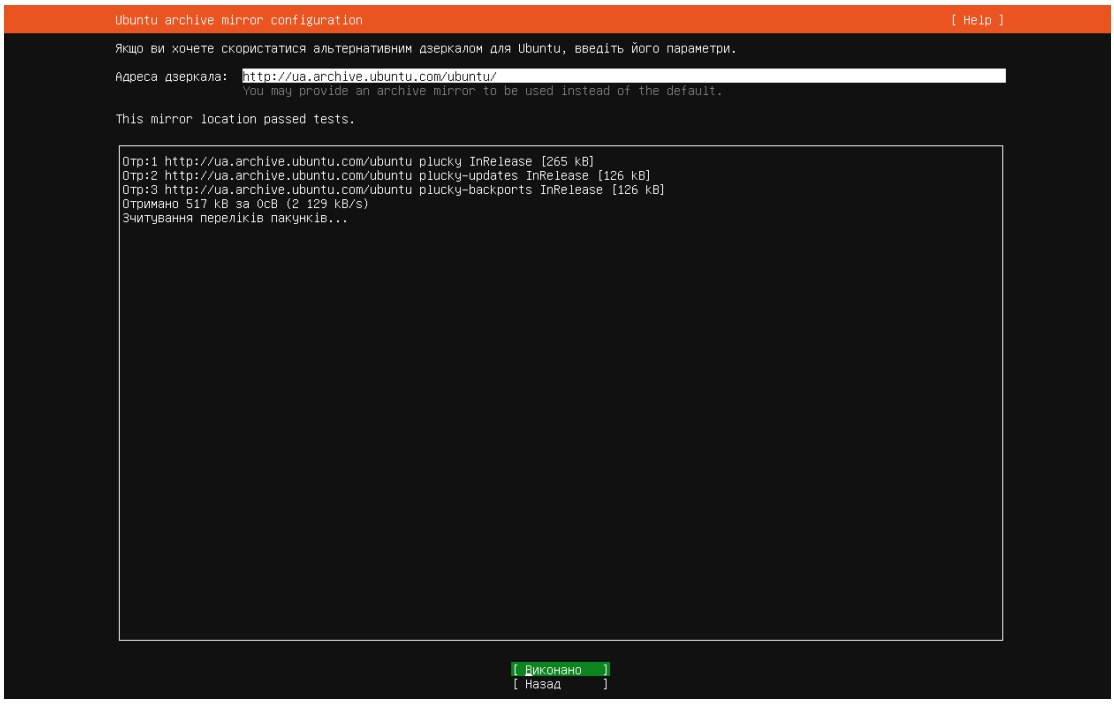

Рисунок 10.8 – Налаштування «Адреса дзеркала» для Linux Server

Згодом, в налаштуваннях сховища даних обирати «Використати увесь диск» та перейти до опції «Виконано» (рис. 10.9).

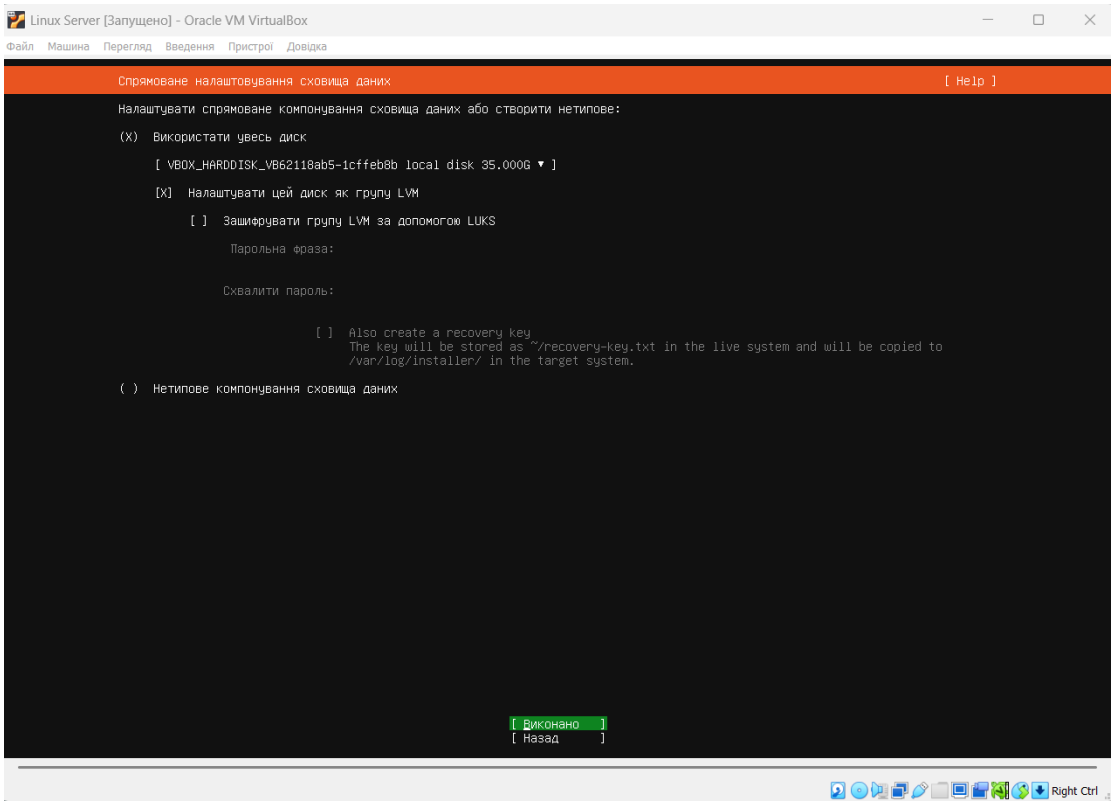

Рисунок 10.9 – Налаштування сховища даних для Linux Server

Після цього, на вкладці «Резюме файлової системи» все залишити без змін і натиснути «Виконано» (рис. 10.10).

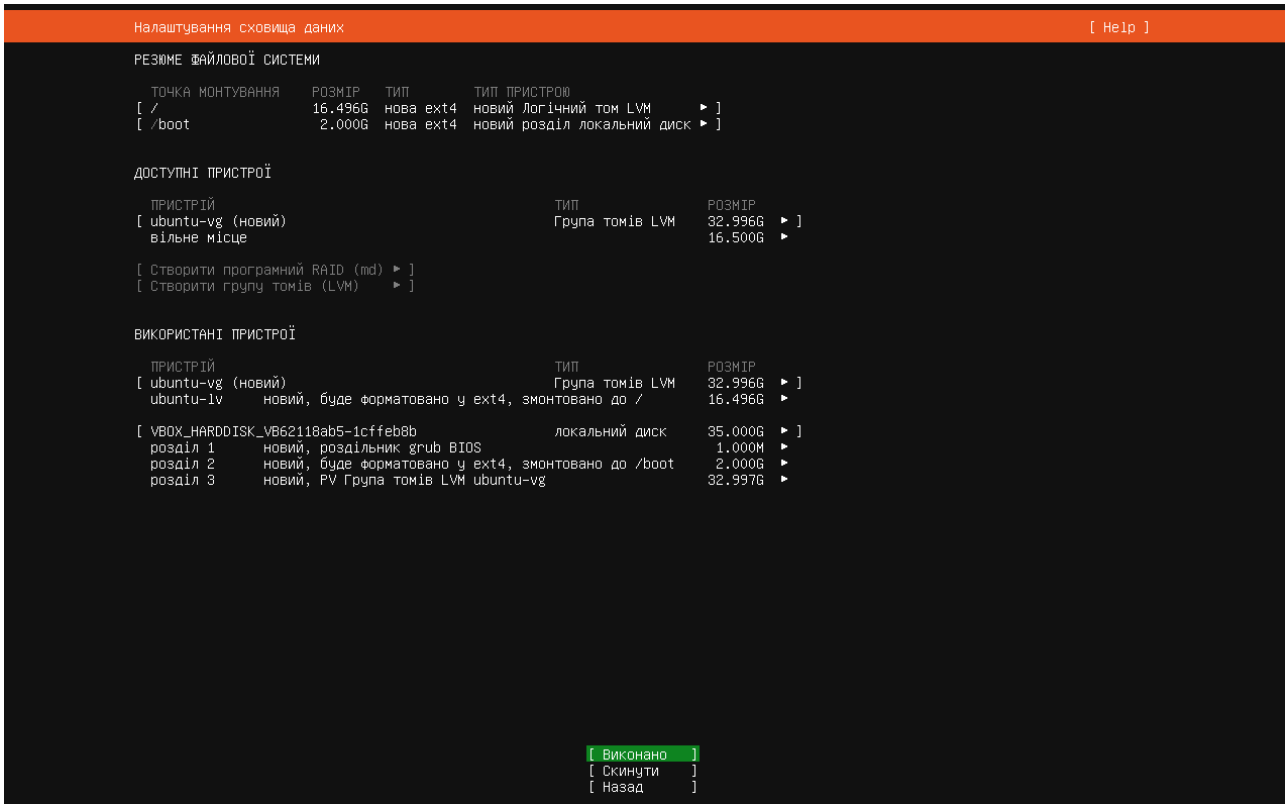

Рисунок 10.10 – Налаштування файлової системи для Linux Server

Далі підтвердити проведені налаштування та перейти до наступної вкладки – «Налаштування профіля». Тут вказати логін та пароль – слід бути особливо уважним, адже з цими даними потім здійснюватиметься вхід у систему
(рис. 10.11).

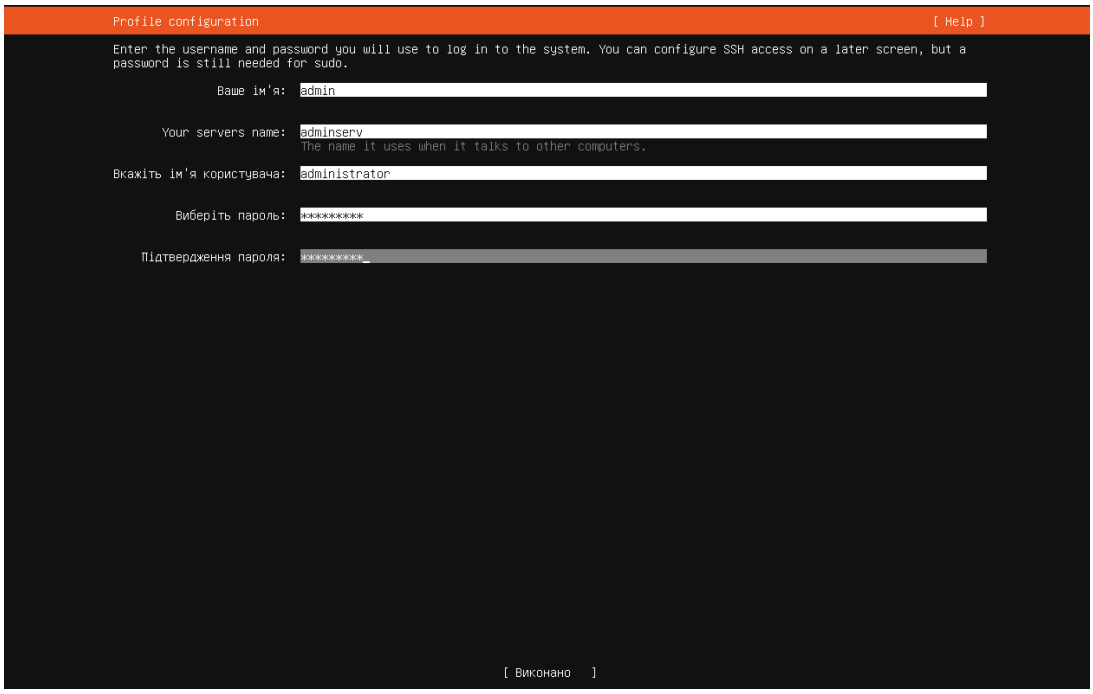

Рисунок 10.11 – Налаштування профіля для Linux Server

В наступному вікні обирати чи встановлювати оболонку SSH для віддаленого доступу на цьому етапі, залишаємо «Не встановлювати» (рис. 10.12).

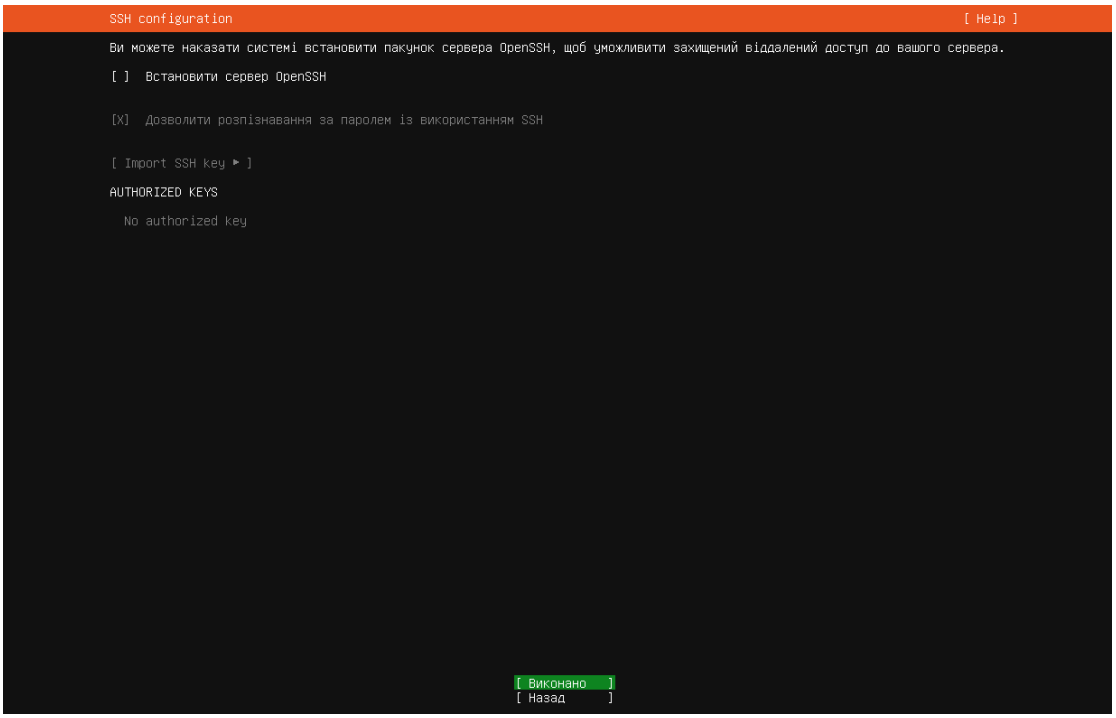

Рисунок 10.12 – Налаштування SSH для Linux Server

На наступному етапі починається встановлення серверної операційної системи Linux Server (рис. 10.13).

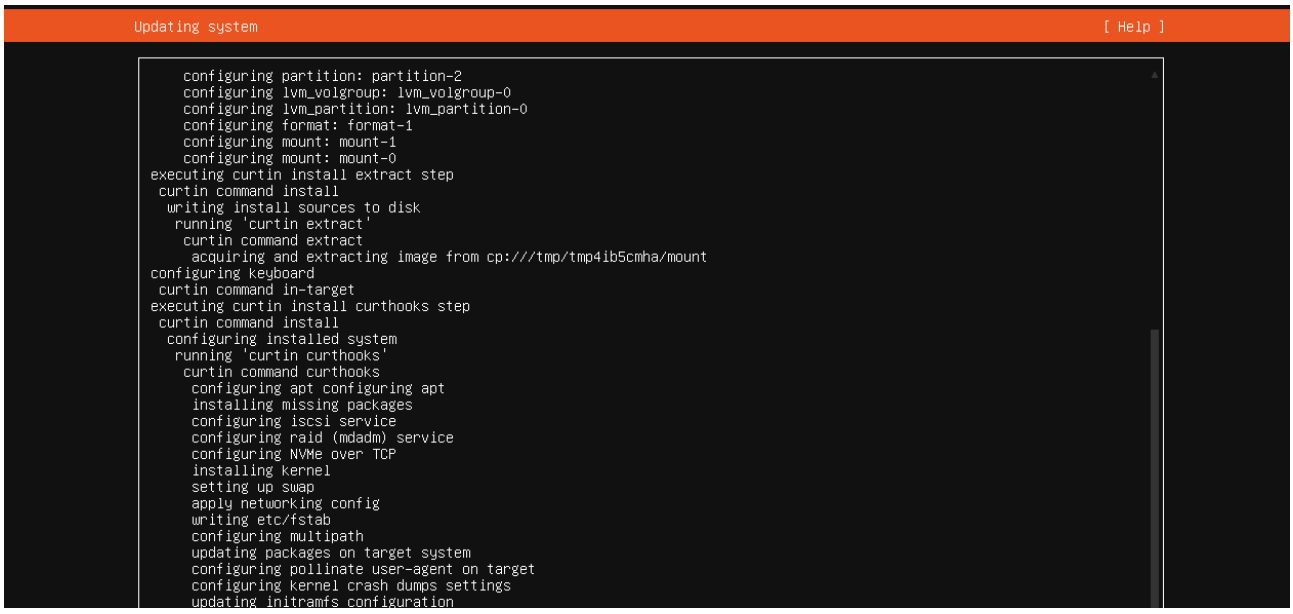

Рисунок 10.13 – Процес встановлення Linux Server

Коли встановлення завершено (вгорі пише «Installation Complete») натиснути «Перезавантажити» (рис. 10.14).

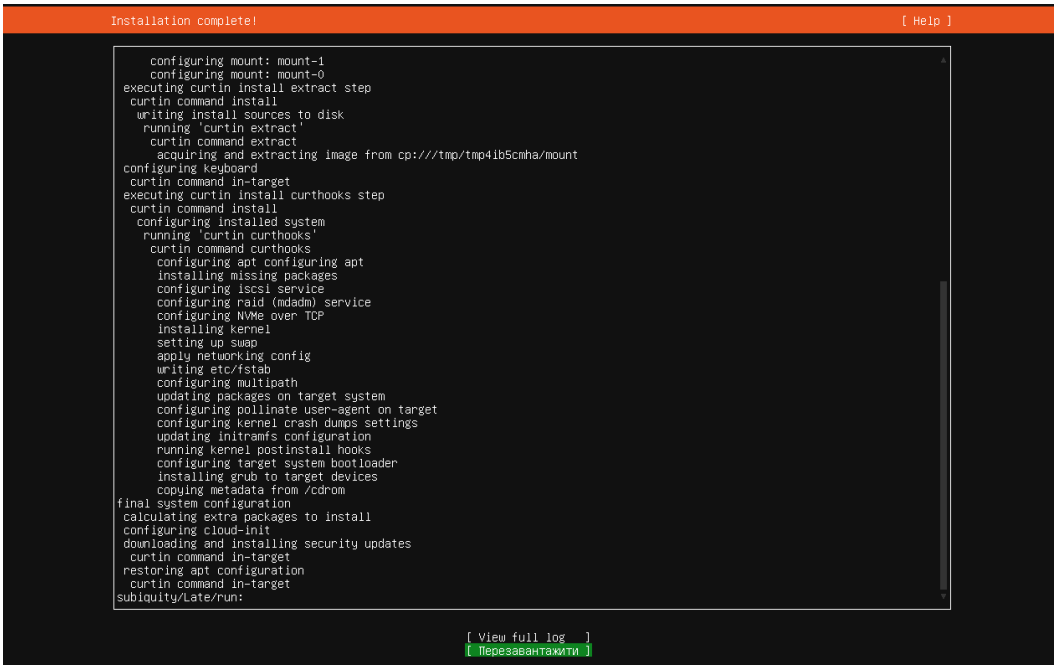

Рисунок 10.14 – Завершення встановлення Linux Server

Відбудеться перезавантаження ВМ, коли цей процес здійснено, то з’явиться рядок входу в операційну систему. Linux Server за замовчуванням є консольною операційною системою, тому всі дії відбуваються в командному рядку. Щоб це змінити, потім встановимо додаткову графічну оболонку GNOME, щоб застосувати десктопну версію цієї ОС.

Перебуваючи на цьому етапі здійснюємо вхід в систему за тим логіном і паролем, що вказували при встановленні системи в налаштуваннях профілю (рис. 10.15).

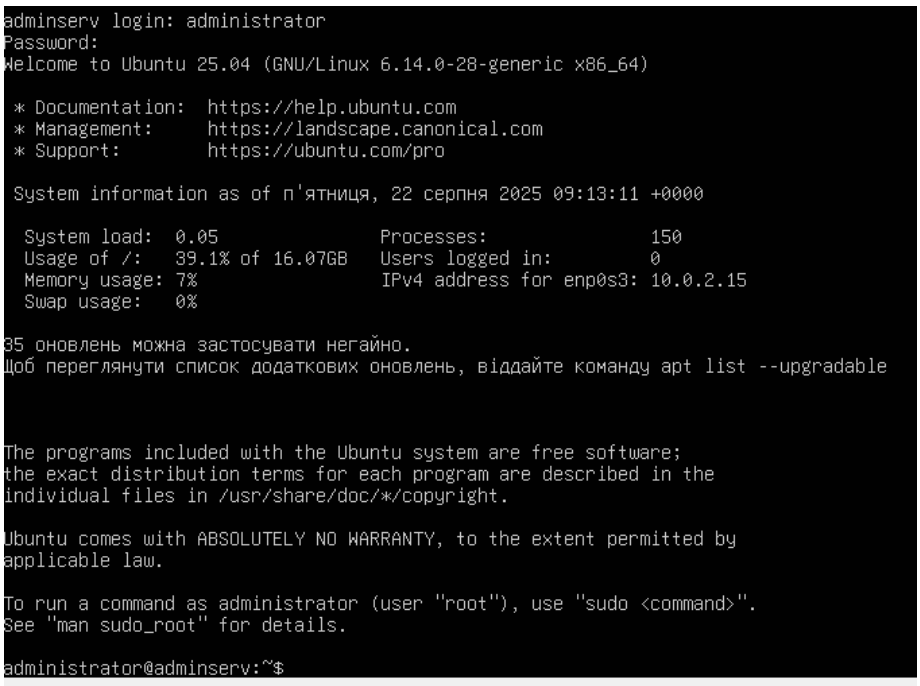

Рисунок 10.15 – Вхід в ОС Linux Server

Після входу провести базові налаштування. Для початку це буде оновлення системи, щоб це виконати, ввести команду «sudo apt update && sudo apt full-upgrade –y» та після неї «sudo reboot» (рис. 10.16).

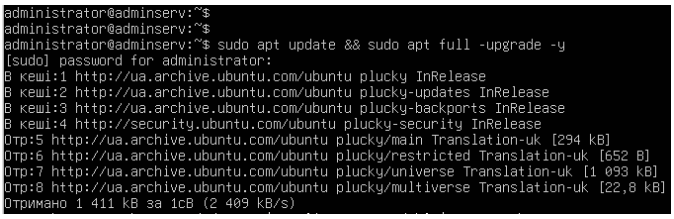

Рисунок 10.16 – Оновлення Linux Server

Далі налаштувати дату та час для сервера. Для цього ввести команду «sudo timedatectl set-timezone Europe/Kyiv» та перевірити потім командою «timedatectl» (рис. 10.17).

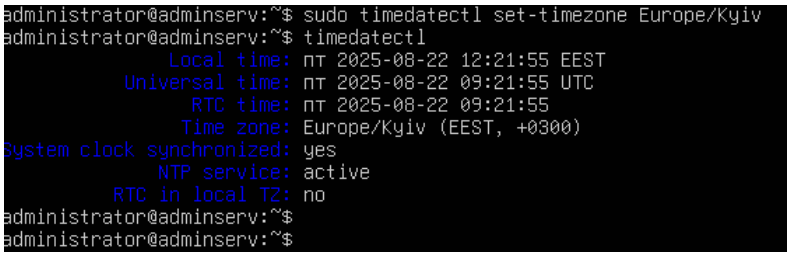

Рисунок 10.17 – Налаштування дати та часу в Linux Server

Після цього встановити графічний інтерфейс для Linux Server. Для встановлення графічного інтерфейсу (GNOME) ввести команду «sudo apt install -y ubuntu-desktop». Після цієї команди розпочинається процес встановлення графічного інтерфейсу на ВМ (рис. 10.18).

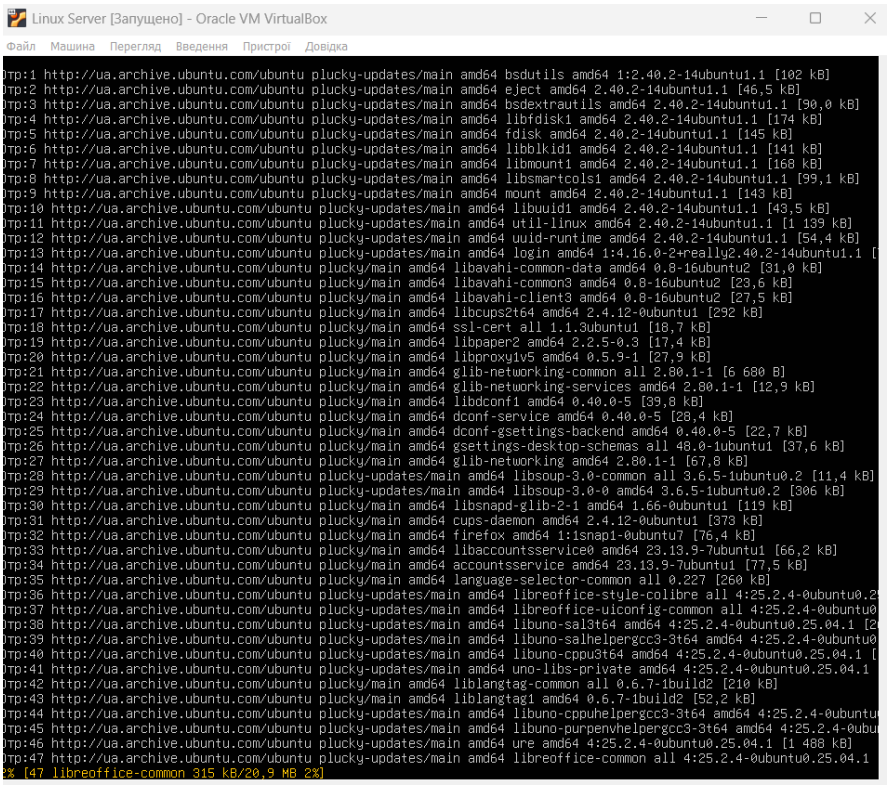

Рисунок 10.18 – Процес встановлення графічного інтерфейсу для Linux Server

Коли встановлення графічного інтерфейсу для Linux Server завершено, ввести команду «sudo systemctl set-default graphical.target» для того, щоб система відразу при запуску машини відкривалася в графічному режимі та провести перезапуск сервера командою «sudo reboot» (рис. 10.19).

```
administrator@adminserv:~$ sudo systemctl set-default graphical.target
[sudo] password for administrator:
Created symlink '/etc/systemd/system/default.target' → '/usr/lib/systemd/system/graphical.target'.
administrator@adminserv:~$
administrator@adminserv:~$ sudo reboot
```

Рисунок 10.19 – Команда для автоматичного відкриття графічного інтерфейсу

Після перезавантаження система запускається в графічному режимі, отже налаштування здійснені успішно (рис. 10.20).

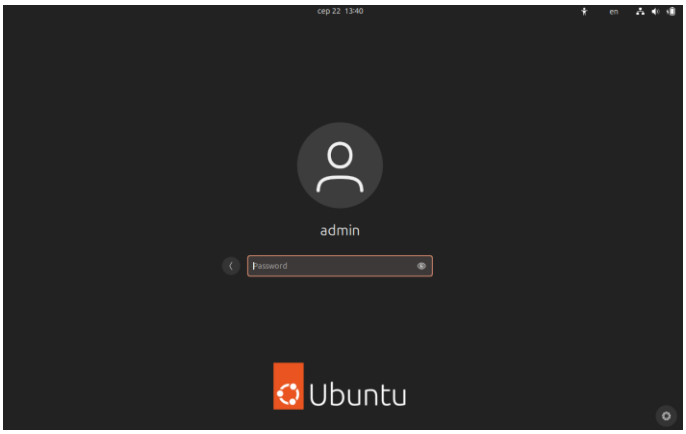

Рисунок 10.20 – Запуск системи Linux Server у графічному режимі роботи

Завдання 2. Керування користувачами та правами доступу

Для роботи з користувачами, групами та їх правами застосовується «Термінал» (аналог командного рядка Windows). Для початку здійснюється перевірка поточного користувача командою «whoami». Це покаже, під яким користувачем ми зараз працюємо. Для більшості команд налаштування потрібні права суперкористувача (root).

Для створення нового користувача ввести команду «sudo adduser <ім’я користувача>». Система попросить ввести пароль для нового користувача та деякі додаткові дані (можна пропустити, натиснувши Enter) (рис. 10.21).

```
administrator@adminserv:~$
administrator@adminserv:~$ sudo adduser student
info: Adding user `student' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `student' (1001) ...
info: Adding new user `student' (1001) with group `student (1001)' ...
info: Creating home directory `/home/student' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: пароль вдало змінено
Зміна інформації про користувача student
Введіть нове значення або натисніть ENTER для типового значення
        Ім'я повністю []:
        Номер кімнати []:
        Робочий телефон []:
        Домашній телефон []:
        Інше []:
Is the information correct? [Y/n] Y
info: Adding new user `student' to supplemental / extra groups `users' ...
info: Adding user `student' to group `users' ...
administrator@adminserv:~$
```

Рисунок 10.21 – Створення нового користувача

Після цього перевірити створеного користувача можна командою «id username». Ця команда покаже UID, GID і групи, до яких належить користувач.

Створення нової групи відбувається подібно до створення користувача та здійснюється командою «sudo groupadd <назва групи>». Для додавання користувача до групи використовується команда «sudo usermod -aG <назва групи> <ім'я користувача>». «-aG» означає додати користувача до додаткової групи, не видаляючи з інших груп.

Для перевірки членства в групі пишемо команду «groups <ім'я користувача>» (рис. 10.22).

```
administrator@adminserv:~$ sudo groupadd Students_KI
administrator@adminserv:~$
administrator@adminserv:~$ sudo usermod -aG Students_KI student
administrator@adminserv:~$
administrator@adminserv:~$ groups student
student : student users Students_KI
administrator@adminserv:~$
```

Рисунок 10.22 – Робота з групами в Linux Server

Для зміни пароля користувача застосуємо «sudo passwd <ім'я користувача>». Ввести новий пароль двічі.

Щоб переглянути історію входу користувача використати команду «last <ім'я користувача>».

Перевірка прав доступу до файлу – «ls -l filename». Вивід показує права у форматі rwx для власника, групи та інших.

Зміна власника та групи файлу здійснюється командою «sudo chown <ім'я користувача>:<назва групи> filename» (рис. 10.23).

```
administrator@adminserv: ~
dministrator@adminserv:~$ touch my_file.txt
dministrator@adminserv:~$
dministrator@adminserv:~$ sudo chown student:Students_KI my_file.txt
sudo] password for administrator:
dministrator@adminserv:~$
```

Рисунок 10.23 – Зміна власника файлу в Linux Server

Зміна прав доступу здійснюється командою «chmod» числовим або символічним способом. Наприклад, «chmod u=rwx,g=rx,o=r filename» – символічний спосіб; «chmod 754 filename» – аналогічний попередньому числовий спосіб. Обидва виконують одну і ту ж функцію.

Перевірку змін здійснюємо командою «ls -l filename» (рис. 10.24).

```
administrator@adminserv:~$ touch test.txt
administrator@adminserv:~$
administrator@adminserv:~$ chmod 754 test.txt
administrator@adminserv:~$ chmod u=rwx,g=rwx,o=r test.txt
administrator@adminserv:~$
administrator@adminserv:~$ ls -l test.txt
-rwxrwxr-- 1 administrator administrator 0 сер 22 14:18 test.txt
administrator@adminserv:~$
```

Рисунок 10.24 – Зміна прав для користувачів щодо файлу в Linux Server

Для адміністрування сервера потрібно вміти переглянути список користувачів у системі – команда «cut -d: -f1 /etc/passwd», переглянути групи у системі «cut -d: -f1 /etc/group», заблокувати користувача – «sudo usermod -L username» та розблокувати користувача «sudo usermod -U username», видалити користувача «sudo deluser username» (рис. 10.25).

```
administrator@adminserv:~$
administrator@adminserv:~$ sudo usermod -L student
administrator@adminserv:~$
administrator@adminserv:~$ sudo usermod -U student
administrator@adminserv:~$
administrator@adminserv:~$ sudo deluser student
info: Removing crontab ...
info: Removing user `student' ...
administrator@adminserv:~$
```

Рисунок 10.25 – Налаштування користувача в Linux Server

Завдання 3. Автоматизація завдань у Linux за допомогою Bash-скриптів

У системах Linux часто виникає потреба у регулярному виконанні однотипних завдань: створення резервних копій, очищення логів, моніторинг стану системи тощо. Замість того, щоб виконувати їх вручну, адміністратори застосовують Bash-скрипти – текстові програми, які виконують послідовність команд.

Автоматизація за допомогою Bash має переваги: зменшення кількості однотипної повторюваної роботи; уникнення помилок, що виникають при ручному виконанні; можливість повторного використання скриптів та інтеграція зі службою планування «cron» для запуску за розкладом.

Наприклад, створимо Bash-скрипт «backup.sh», який архівує вказаний каталог у підпапку ~/backups/. Для цього створюємо підпапку командою «mkdir -p backups», далі створюємо сам скрипт – «nano backup.sh» (рис. 10.26).

```
#!/usr/bin/env bash
# backup.sh – простий скрипт резервного копіювання
# Використання: ./backup.sh /шлях/до/каталогу

src="$1"
dest="$HOME/backups"
ts=$(date +%Y-%m-%d_%H-%M-%S)
file="backup_$(basename "$src")_$ts.tar.gz"

if [[ -z "$src" || ! -d "$src" ]]; then
  echo "Помилка: потрібно вказати існуючий каталог."
  exit 1
fi

mkdir -p "$dest"
tar -czf "$dest/$file" -C "$src" . || { echo "Помилка при створенні архіву"; exit 2; }

echo "Бекап створено: $dest/$file"
```

Рисунок 10.26 – Код Bash-скрипту для створення резервної копії каталога

Після того, як скрипт створено застосовуємо команди «chmod +x backup_dir.sh», «./backup_dir.sh /etc» та «ls -lh backups».

Щоб краще автоматизувати роботу цього скрипта, потрібно запланувати щоденний бекап /etc о 07:00. Для цього застосується команда «crontab –e». Додати рядок «00 7 * * * /home/$USER/backup.sh /etc >> /home/$USER/backup_cron.lo». Перегляд налаштування здійснюється командою «crontab –l».

Лабораторна робота №11
Налаштування мережевих служб у Linux

Мета роботи: закріпити практичні навички налаштування мережевих служб у Linux, зокрема конфігурації статичних IP-адрес, встановлення та адміністрування SSH-сервера, а також опанувати інструменти моніторингу мережевої активності. Виконання роботи спрямоване на формування компетентностей із забезпечення стабільного мережевого підключення, віддаленого управління сервером та контролю використання мережевих ресурсів у серверному середовищі Linux [40-43].

Хід роботи

Завдання 1. Налаштування статичної IP

Запускаємо Linux Server розгорнутий в результаті виконання завдань попередньої лабораторної роботи. Входимо в систему під своїм користувачем. Відкриваємо «Параметри» (Settings), далі розділ «Мережа» (Network). У списку інтерфейсів «Wired» (провідне з'єднання) натискаємо на піктограму шестерні (рис. 11.1).

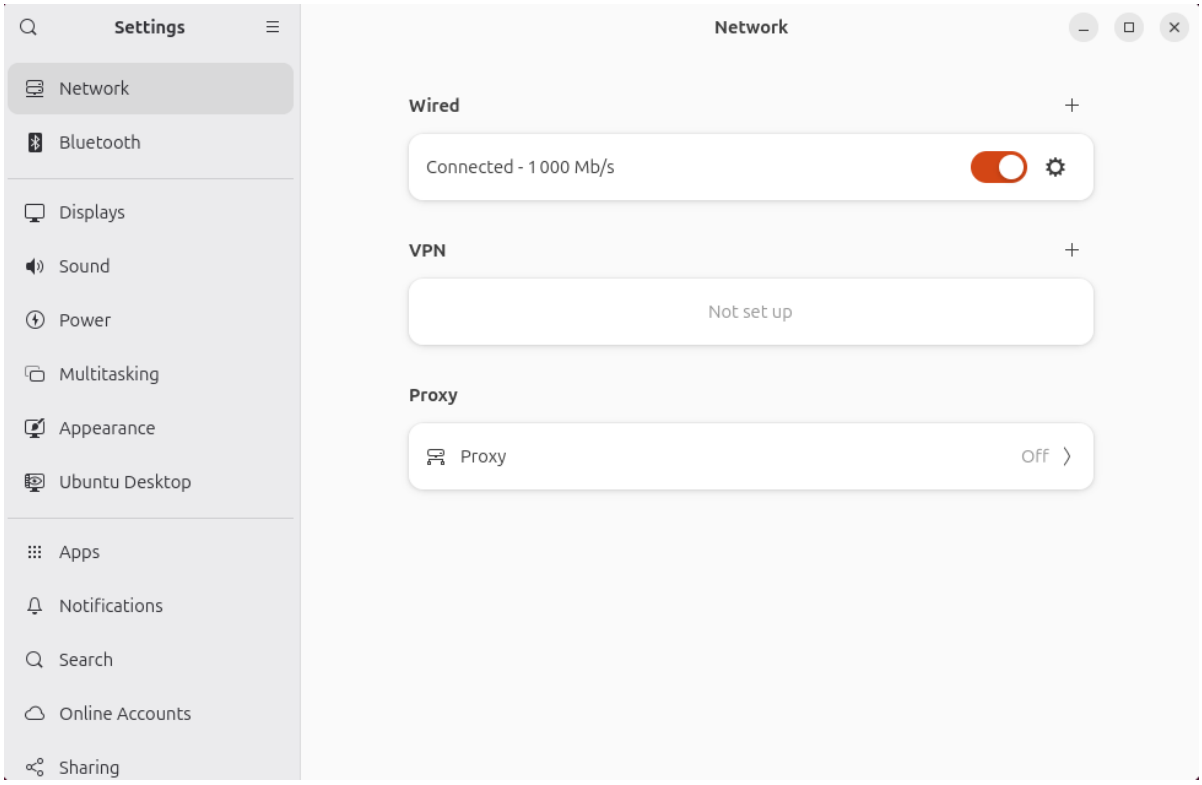

Рисунок 11.1 – Вікно «Налаштування мережі»

В результаті цього відкривається вікно налаштувань підключення. Переходимо у вкладку «IPv4», у вікні, що відкрилося (рис. 11.2).

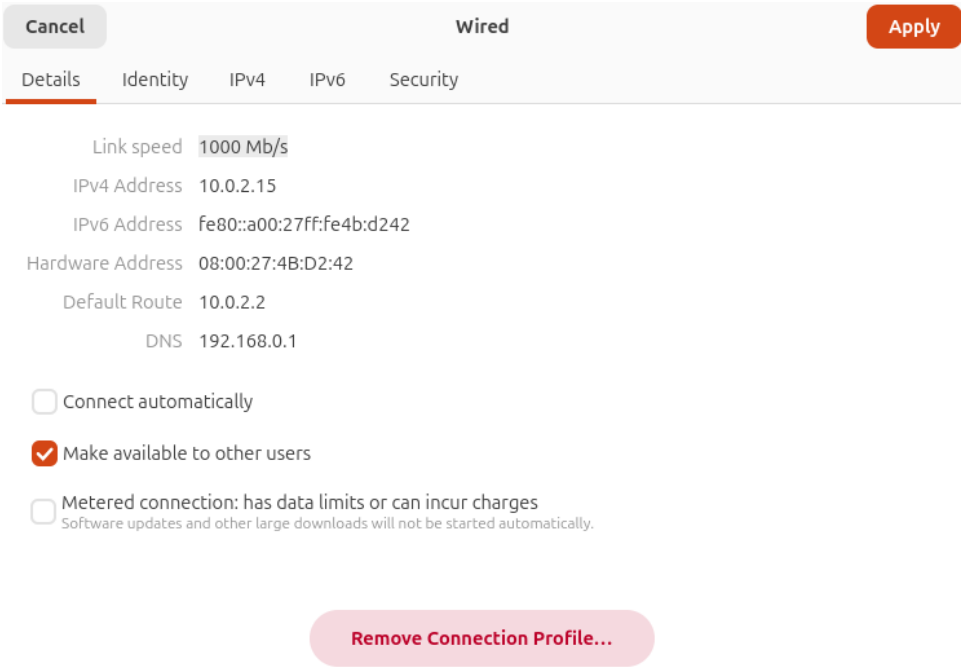

Рисунок 11.2 – Вікно «Налаштування провідного з’єднання мережі»

Відкривши вкладку «IPv4» у полі «Метод» обираємо «Manual» (Ручний). У полі «Addresses» додаємо: Address: 192.168.56.10; Netmask: 255.255.255.0; Gateway: 192.168.56.1. Зберігаємо налаштування натиснувши «Apply», вимикаємо/вмикаємо інтерфейс (або просто відключаємо і підключаємо мережу) (рис. 11.3).

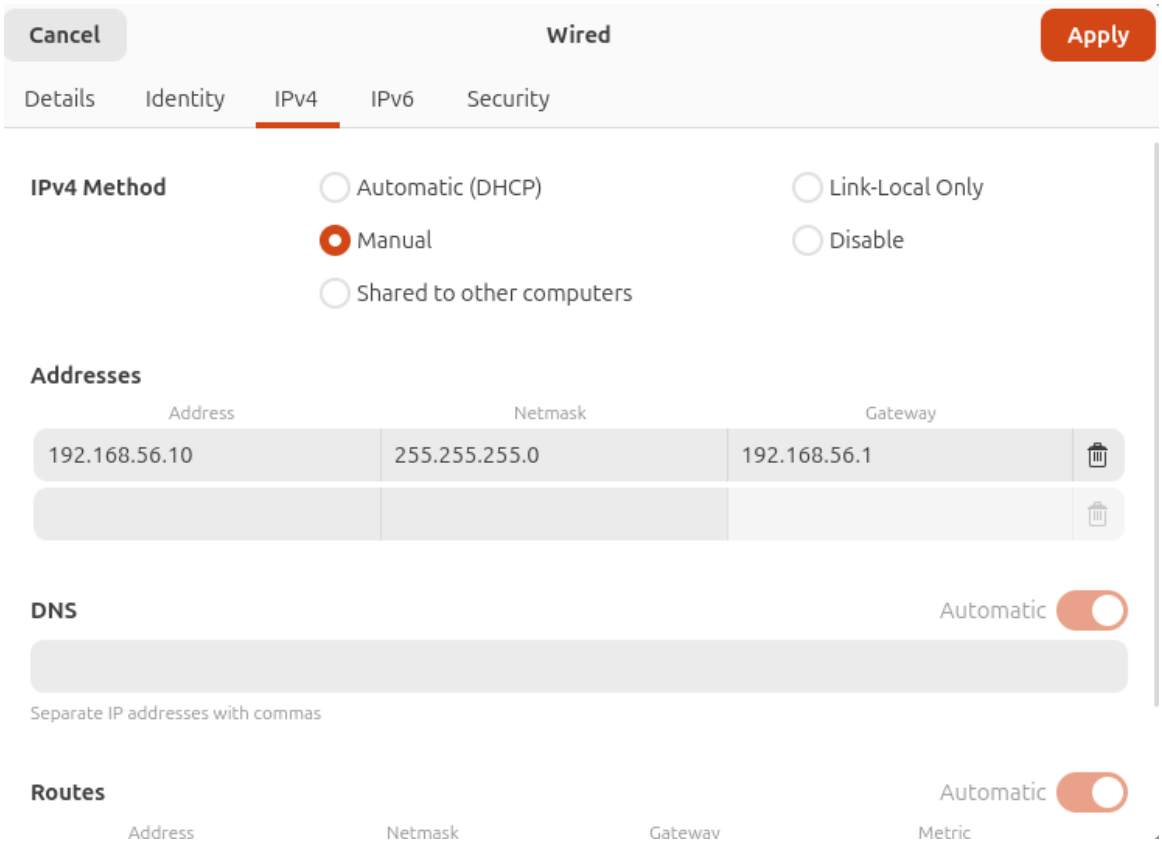

Рисунок 11.3 – Налаштування статичної IP-адресації для сервера

Після цього перевіряємо підключення та налаштування статичних IP-адрес. Для цього у терміналі виконуємо «ip addr show», «ping -c 4 192.168.56.1», «ping -c 4 8.8.8.8». Якщо команди виконалися коректно, відповідно налаштування статичної IP застосовано.

Завдання 2. Встановлення та налаштування SSH-сервера

Для встановлення SSH-сервера в терміналі застосовуємо команди «sudo apt update» та після неї команду «sudo apt install openssh-server –y» (рис. 11.4-11.5).

```
administrator@adminserv:~$ sudo apt install openssh-server -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  openssh-server
```

Рисунок 11.4 – Введення команд для встановлення SSH-сервера

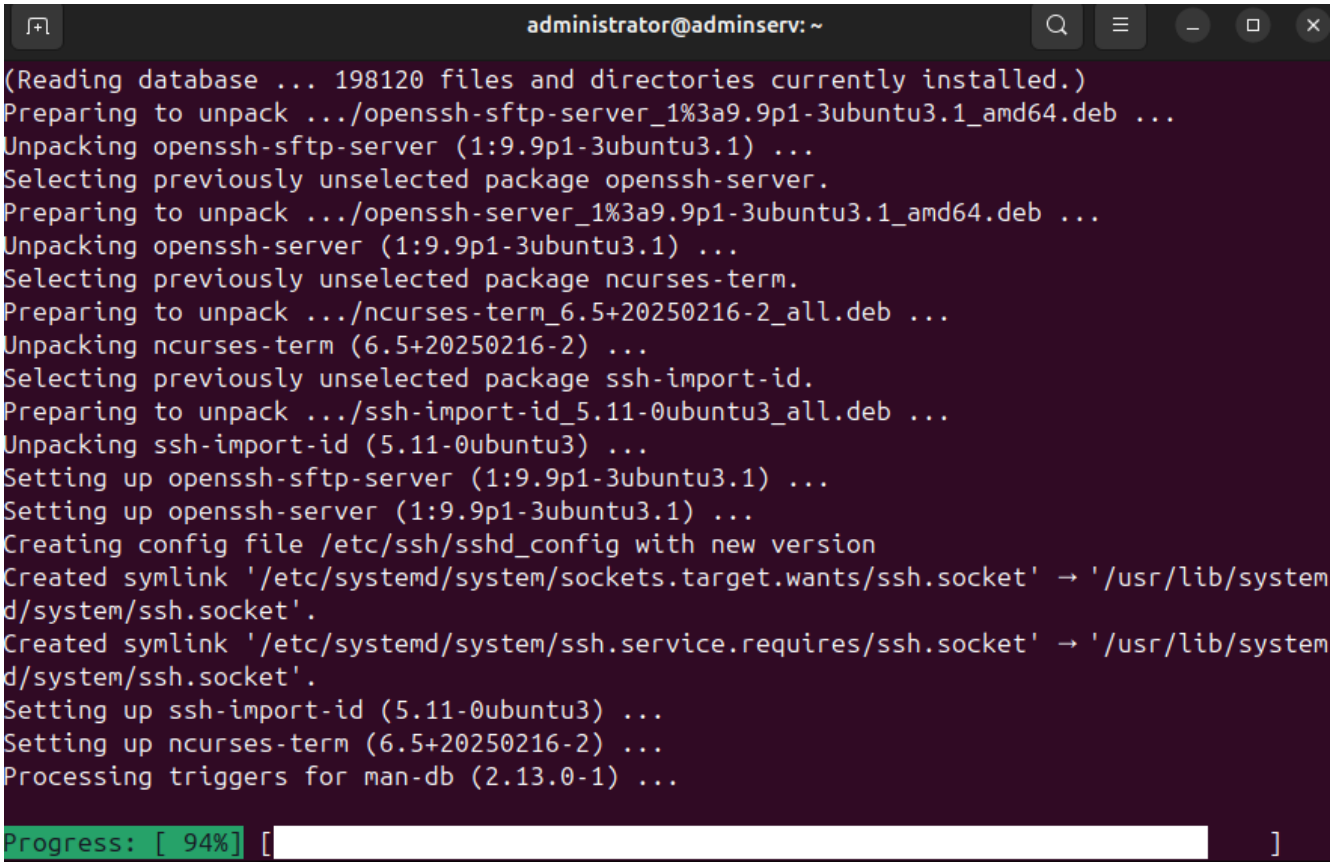

Рисунок 11.5 – Процес встановлення SSH-сервера

Після встановлення перевіряємо роботу служби SSH-сервера. Для цього використовуємо команду «sudo systemctl status ssh» в терміналі. Також після цього перевіряємо, чи «слухає» сервер порт 22 командою «ss -tlnp | grep 22» (рис. 11.6).

```
administrator@adminserv:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
administrator@adminserv:~$
administrator@adminserv:~$
administrator@adminserv:~$ ss -tlnp | grep 22
LISTEN 0      4096         0.0.0.0:22        0.0.0.0:*
LISTEN 0      4096            [::]:22           [::]:*
administrator@adminserv:~$
```

Рисунок 11.6 – Перевірка встановлення та роботи SSH-сервера

Для змінення налаштувань SSH слід відкрити конфігураційний файл, що міститься за адресою «/etc/ssh/ssh_config». Там знайшовши потрібне поле провести зміни. Після зміни виконуємо перезапуск SSH-сервера командою «sudo systemctl restart ssh» (рис. 11.7).

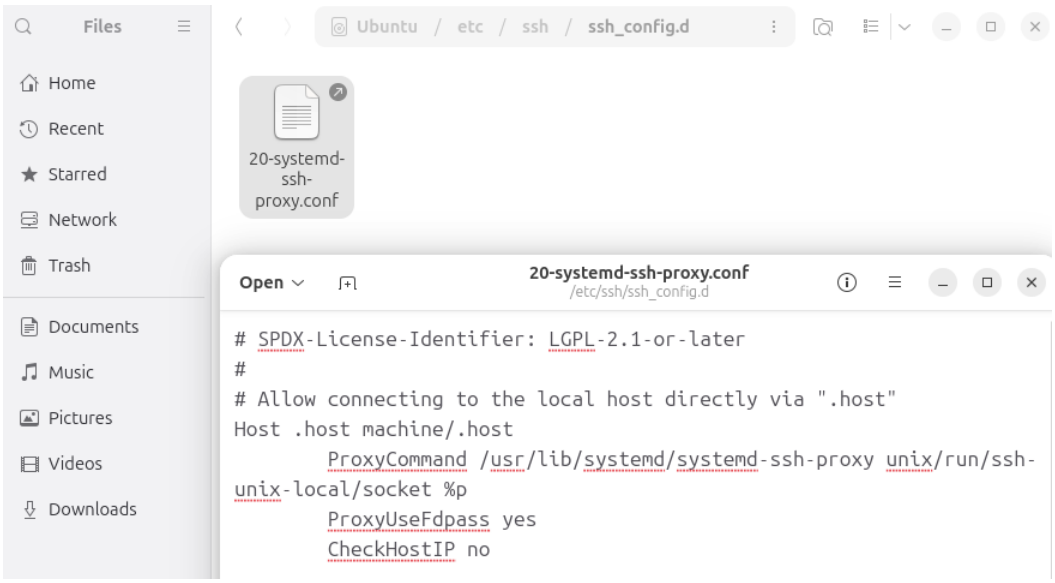

Рисунок 11.7 – Файл конфігурації SSH-сервера

Для подальшого правильного функціонування SSH-сервера проводимо налаштування відповідних параметрів брандмауера. Для цього в терміналі «вводимо команду «sudo ufw allow 22/tcp» та наступну команду «sudo ufw enable». Коли ці дії зроблено, то SSH-сервер має коректно працювати (рис. 11.8).

```
administrator@adminserv: ~
administrator@adminserv:~$ sudo ufw allow 22/tcp
[sudo] password for administrator:
Rules updated
Rules updated (v6)
administrator@adminserv:~$
administrator@adminserv:~$ sudo ufw enable
Firewall is active and enabled on system startup
administrator@adminserv:~$
```

Рисунок 11.8 – Налаштування брендмауера для роботи SSH-сервера

Завдання 3. Моніторинг мережевої активності у Linux

Для моніторингу мережевої активності у Linux відкриваємо «Додатки», там шукаємо групу додатків «Система», тиснемо на неї і там обираємо «System Monitor» (Системний монітор). У вікні «Системного монітора» переходимо у вкладку «Resources» (Ресурси). У розділі «Мережа» відображаються: швидкість прийому/передачі даних на сервері (RX/TX) та загальний обсяг переданих даних (рис. 11.9).

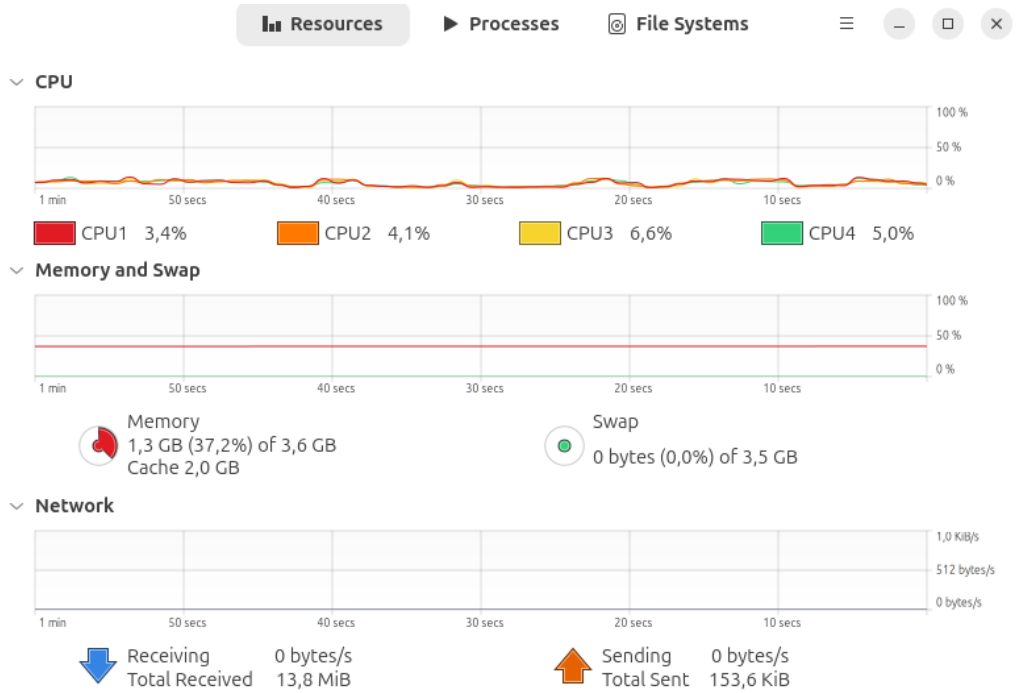

Рисунок 11.9 – Моніторинг мережевої активності у вікні «Системного монітора»

Також у вкладці «Processes» (Процеси) можна відсортувати процеси та подивитися, які програми активно використовують мережу.

Моніторинг мережевої активності можна також здійснювати у терміналі. Активні з’єднання переглядаємо командою «ss –tulpn». Дана команда показує активні сокети, протоколи, порти й процеси (рис. 11.10).

Рисунок 11.10 – Моніторинг активних сокетів, протоколів, портів й процесів

Для моніторингу трафіку інтерфейсу встановлюємо в терміналі інструмент «iftop». Це виконується командою «sudo apt install iftop –y». Після цього запускаємо даний інструмент – «sudo iftop -i enp0s3». Замість «enp0s3» використовується назву інтерфейсу (рис. 11.11-11.12)

```
administrator@adminserv:~$ sudo apt install iftop -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  iftop

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 18
  Download size: 33,5 kB
  Space needed: 87,0 kB / 5 297 MB available

Отр:1 http://ua.archive.ubuntu.com/ubuntu plucky/universe amd64 iftop amd64 1.0
pre4-9build2 [33,5 kB]
Отримано 33,5 kB за 0cB (205 kB/s)
```

Рисунок 11.11 – Встановлення інструменту моніторингу трафіку «iftop»

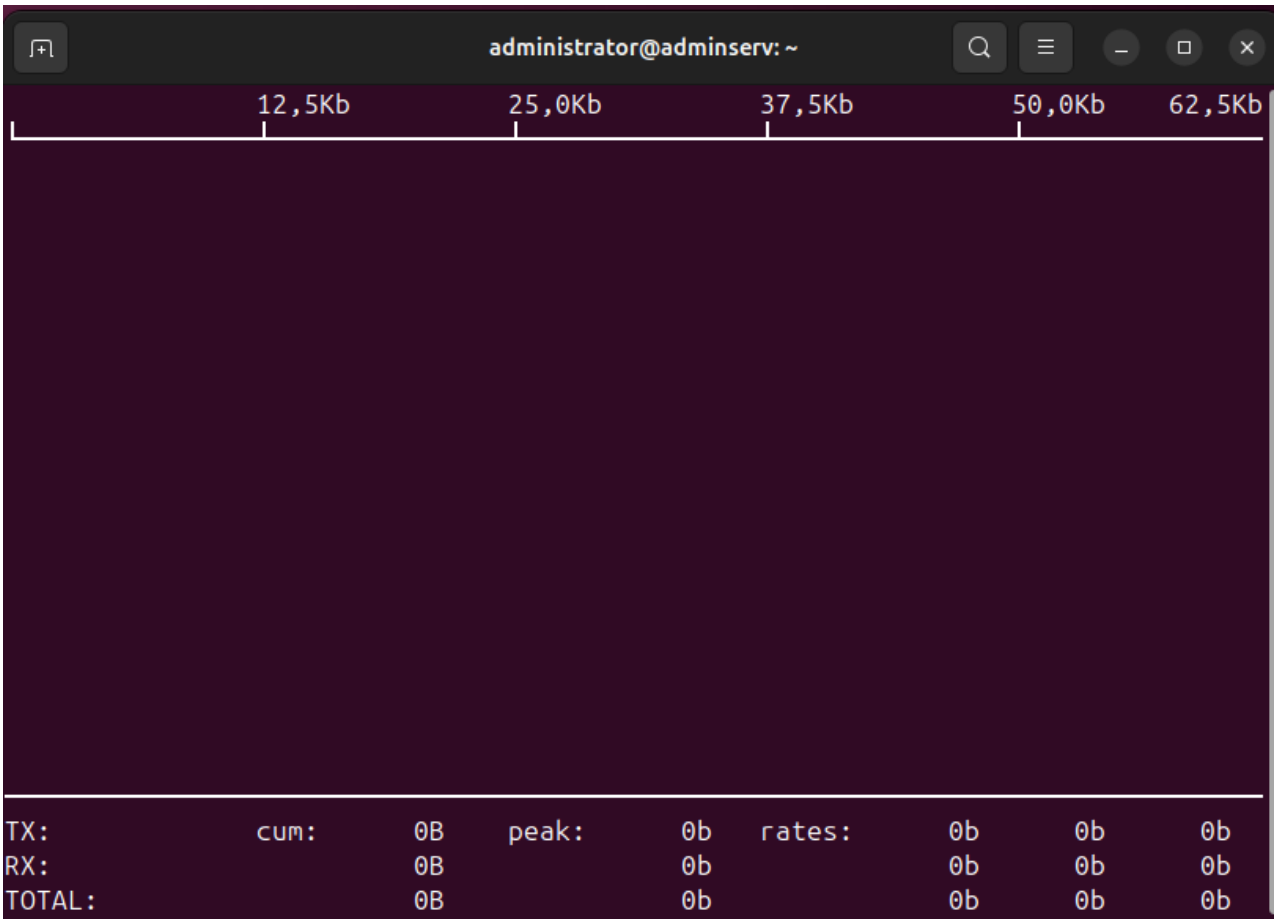

Рисунок 11.12 – Вікно роботи інструменту моніторингу трафіку «iftop»

Для моніторингу трафіку по процесах виконуємо встановлення «nethogs». Для цього вписуємо команду «sudo apt install nethogs –y» і встановлюємо даний інструмент. Після цього запускаємо – «sudo nethogs». Ця утиліта показує, які процеси створюють навантаження на мережу (рис. 11.13-11.14).

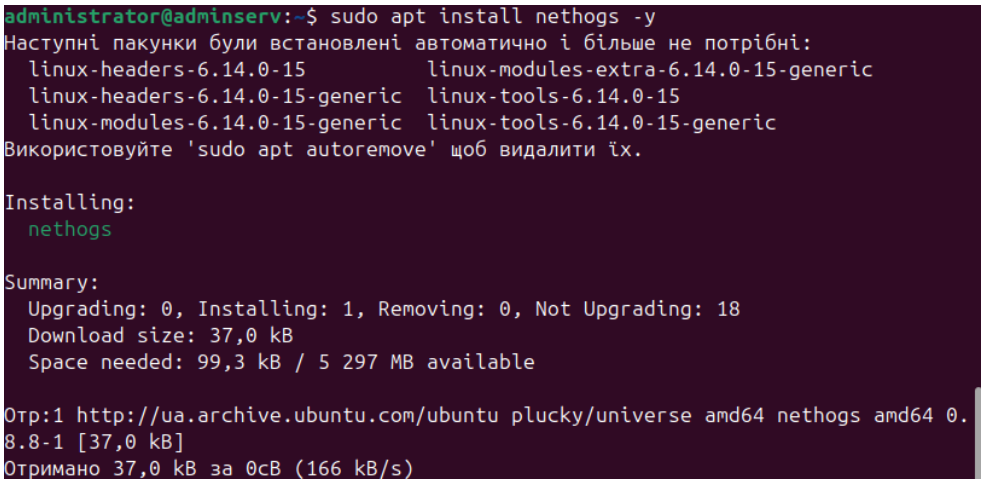

Рисунок 11.13 – Встановлення інструменту моніторингу трафіку по процесах «nethogs»

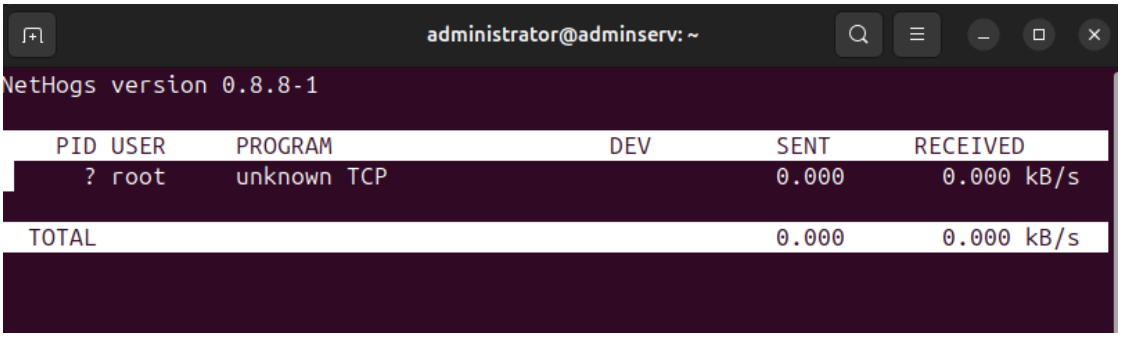

Рисунок 11.14 – Вікно роботи інструменту моніторингу трафіку по процесах «nethogs»

Для моніторингу статистики інтерфейсів та помилок в передачі мережевого трафіку застосовується команда «ip -s link». Дана команда виведе статистику по кожному мережевому інтерфейсу (пакети, помилки тощо) (рис. 11.15).

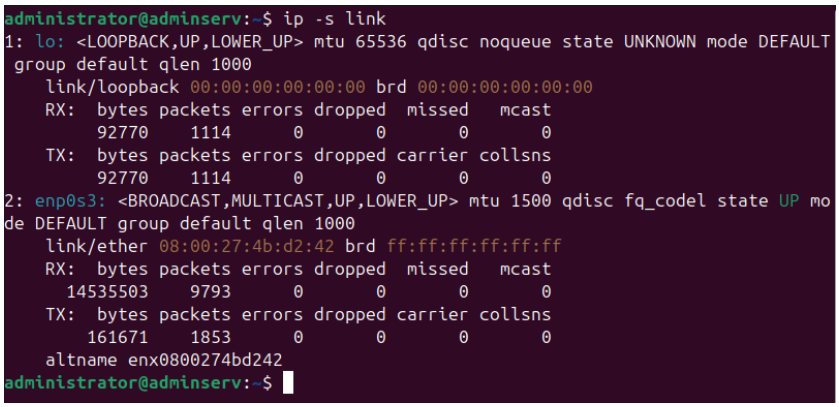

Рисунок 11.15 – Моніторинг статистики інтерфейсів, пакетів та помилок в терміналі Linux Server

Моніторинг мережевої активності у Linux дозволяє контролювати використання мережевих ресурсів, виявляти аномалії та потенційні загрози, а також оптимізувати продуктивність системи. Використовуючи інструменти як ss, iftop, nethogs та графічні утиліти в GNOME, адміністратор може отримувати детальну інформацію про з’єднання, трафік та активні процеси. Регулярний моніторинг підвищує безпеку та стабільність серверного середовища.

Лабораторна робота №12
Веб-сервер та служби в Linux

Мета роботи: набути практичних навичок встановлення та налаштування веб-серверів Apache і Nginx у середовищі Linux, організувати роботу FTP-сервера з урахуванням безпекових параметрів, а також засвоїти методи аудиту й захисту веб-серверів за допомогою інструментів Lynis, Fail2Ban та nmap. Виконання роботи спрямоване на формування компетентностей у сфері адміністрування серверних служб і забезпечення безпеки веб-ресурсів [40-43].

Хідроботи

Завдання 1.Встановлення Apache

Запускаємо Linux Server розгорнутий в результаті виконання завдань однієї з попередніх лабораторних робіт. Починаємо встановлення Apache. Для цього для початку оновлюємо пакети системи командою «sudo apt update». Після цього вводимо команду для безпосереднього встановлення веб-сервер Apache «sudo apt install apache2 –y» (рис. 12.1-12.2).

```
administrator@adminserv:~$ sudo apt update
[sudo] password for administrator:
В кеші:1 http://ua.archive.ubuntu.com/ubuntu plucky InRelease
В кеші:2 http://ua.archive.ubuntu.com/ubuntu plucky-updates InRelease
В кеші:3 http://ua.archive.ubuntu.com/ubuntu plucky-backports InRelease
В кеші:4 http://security.ubuntu.com/ubuntu plucky-security InRelease
18 packages can be upgraded. Run 'apt list --upgradable' to see them.
administrator@adminserv:~$ sudo apt install apache2 -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  apache2
```

Рисунок 12.1 – Встановлення Apache

```
Processing triggers for ufw (0.36.2-9) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for libc-bin (2.41-6ubuntu1.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
administrator@adminserv:~$
```

Рисунок 12.2 – Завершений процес інсталяції Apache

Після здійснення інсталяції перевіряємо статус сервісу командою «sudo systemctl status apache2» (рис. 12.3).

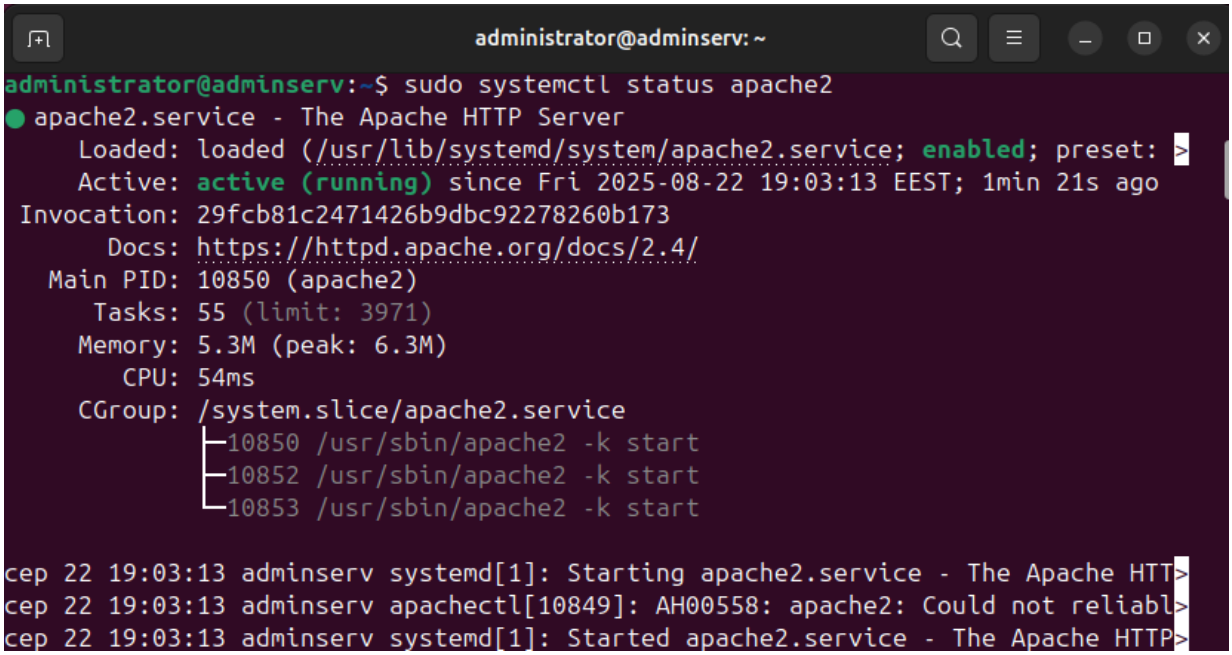

Рисунок 12.3 – Перевірка статусу сервісу Apache

Далі запускаємо Apache та додаємо у автозавантаження – «sudo systemctl start apache2» і потім «sudo systemctl enable apache2» (рис. 12.4).

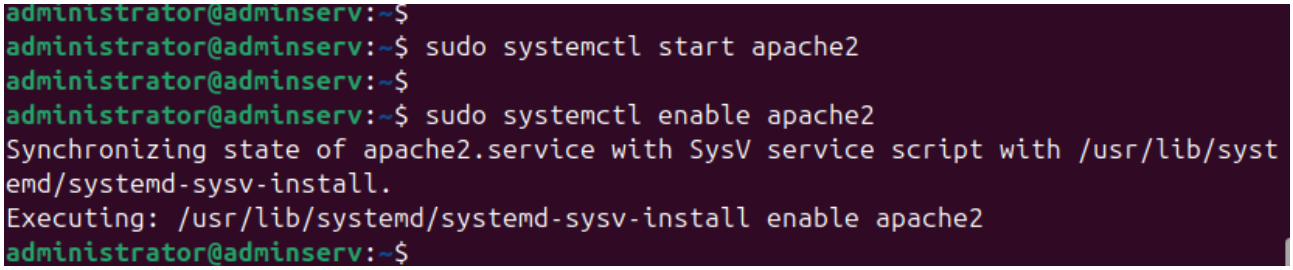

Рисунок 12.4 – Запуск та додавання в автозавантаження сервісу Apache

Щодо налаштування Apache, то його основний конфігураційний файл знаходиться за шляхом «/etc/apache2/apache2.conf» (рис. 12.5).

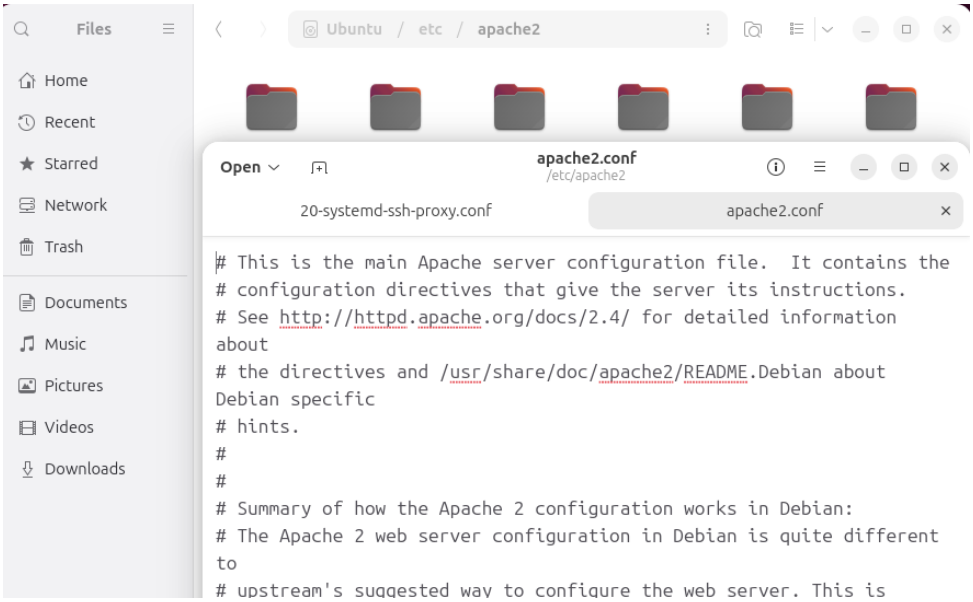

Рисунок 12.5 – Конфігураційний файл сервісу Apache

Для додавання нового сайту (VirtualHost) створюємо папку для сайту, використовуючи команди: «sudo mkdir -p /var/www/mywebsite» та «sudo chown -R $USER:$USER /var/www/mywebsite» (рис. 12.6).

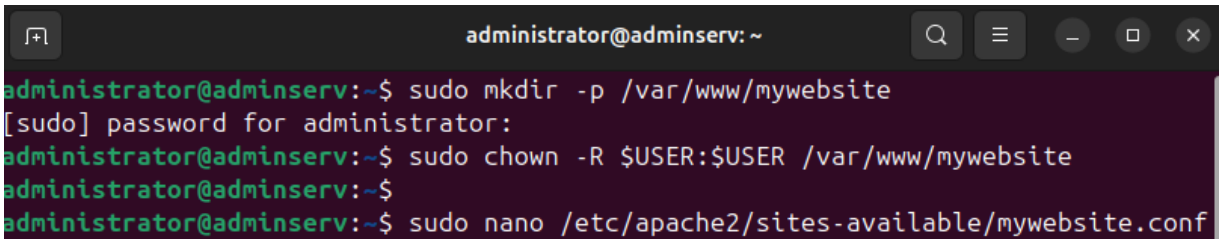

Рисунок 12.6 – Додавання нового сайту з використанням сервісу Apache

Після цього створюємо файл конфігурації для сайту – команда «sudo nano /etc/apache2/sites-available/mywebsite.conf». Записуємо конфігурацію у вікні, що відкрилося.

Далі активуємо сайт та перезавантажуємо сервер, використавши команди «sudo a2ensite mywebsite.conf», «sudo systemctl reload apache2» (рис. 12.7).

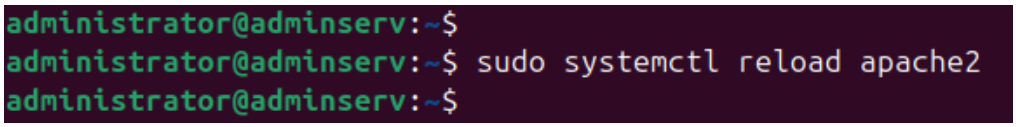

Рисунок 12.7 – Перезавантаження сервера Apache

Щодо Nginx, то алгоритм буде подібним до Apache. Для початку встановлюємо Nginx командою «sudo apt install nginx –y» (рис. 12.8).

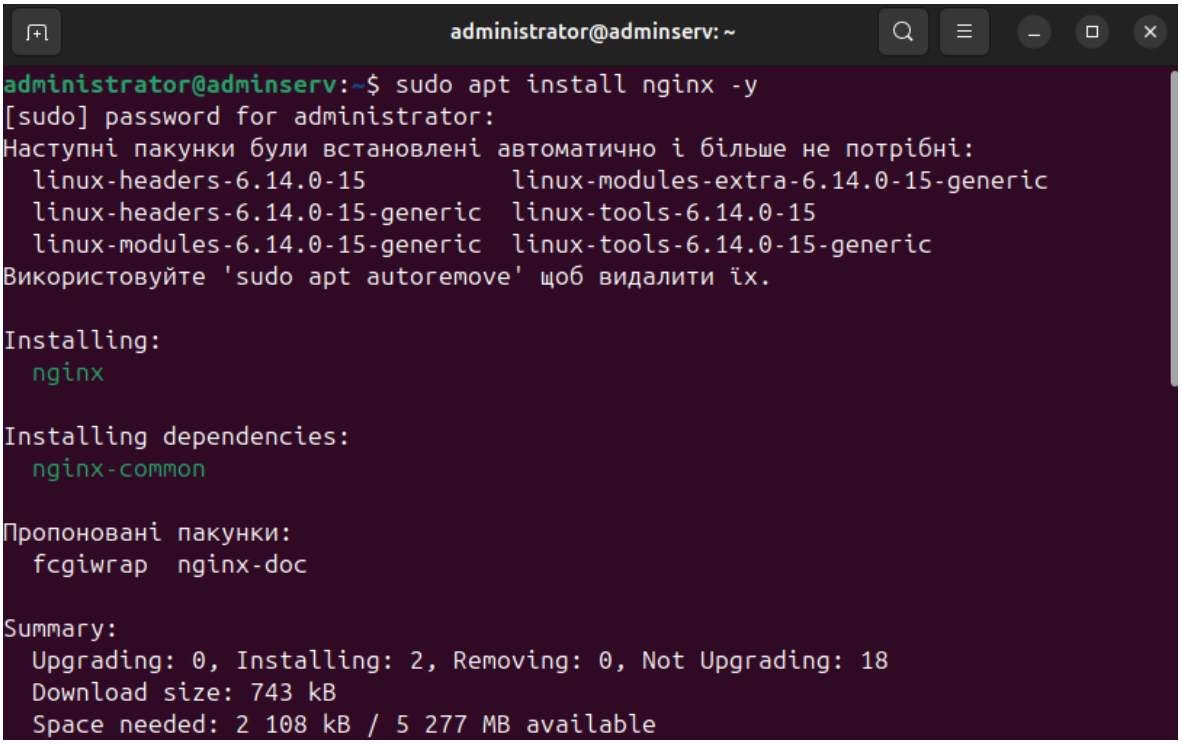

Рисунок 12.8 – Встановлення Nginx

Після встановлення перевіряємо статус – «sudo systemctl status nginx».

Далі запускаємо та додаємо у автозавантаження командами «sudo systemctl start nginx» та «sudo systemctl enable nginx» (рис. 12.9).

```
administrator@adminserv:~$ sudo systemctl start nginx
administrator@adminserv:~$
administrator@adminserv:~$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /usr/lib/syst
emd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nginx
administrator@adminserv:~$
```

Рисунок 12.9 – Запуск та додавання у автозавантаження Nginx

Щодо налаштувань, то основний конфігураційний файл знаходиться за маршрутом «/etc/nginx/nginx.conf» у файловій системі.

Для створення нового сайту в сервісі Nginx, застосовуємо набір команд: «sudo mkdir -p /var/www/nginxsite», «sudo chown -R $USER:$USER /var/www/nginxsite» та «sudo nano /etc/nginx/sites-available/nginxsite» і після цього у вікні, що відкрилося прописуємо конфігурацію сайту.

Коли це зроблено, активуємо сайт та перевіряємо конфігурацію командами «sudo ln -s /etc/nginx/sites-available/nginxsite /etc/nginx/sites-enabled/», «sudo nginx –t» та «sudo systemctl reload nginx» (рис. 12.10).

```
administrator@adminserv: ~
administrator@adminserv:~$ sudo ln -s /etc/nginx/sites-available/nginxsite /etc/
nginx/sites-enabled
[sudo] password for administrator:
administrator@adminserv:~$ sudo nginx -t
2025/08/22 20:10:32 [emerg] 15326#15326: open() "/etc/nginx/sites-enabled/nginxs
```

Рисунок 12.10 – Активація та перевірка сайту в Nginx

Завдання 2. Створення та налаштування FTP-сервера

На Linux Server найчастіше використовують vsftpd (Very Secure FTP Daemon) FTP-сервер. Тому встановлюємо vsftpd командою «sudo apt install vsftpd –y» (рис. 12.11).

```
administrator@adminserv:~$ sudo apt install vsftpd -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 18
  Download size: 131 kB
  Space needed: 333 kB / 5 276 MB available

Отр:1 http://ua.archive.ubuntu.com/ubuntu plucky/main amd64 vsftpd amd64 3.0.5-0
.1 [131 kB]
Отримано 131 kB за 0cB (507 kB/s)
Передналаштування пакунків...
```

Рисунок 12.11 – Встановлення FTP-сервера

Після цього, перевіряємо статус сервісу – «sudo systemctl status vsftpd». Коли це виконано, то запускаємо цей FTP-сервер та додаємо у автозавантаження. Для цього існують команди «sudo systemctl start vsftpd» та «sudo systemctl enable vsftpd» (рис. 12.12-12.13).

Рисунок 12.12 – Перевірка статусу встановлено FTP-сервера

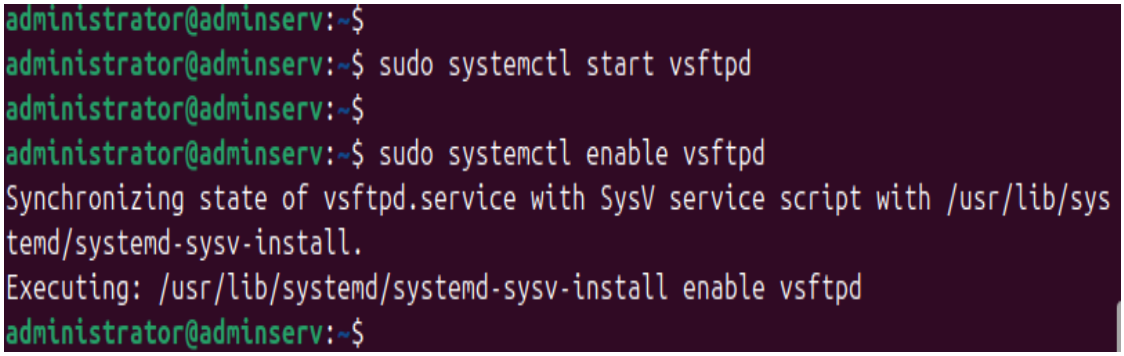

Рисунок 12.13 – Запуск FTP-сервера

Коли встановлення завершено переходимо до налаштування. Конфігураційний файл міститься за адресою «/etc/vsftpd.conf». Відкриваємо цей файл для редагування – команда «sudo nano /etc/vsftpd.conf». Відкривши, змінюємо основні параметри відповідно до потреб. Наприклад, для того, щоб дозволити локальним користувачам підключатися слід записати «local_enable=YES», щоб дозволити завантаження файлів – «write_enable=YES», щоб включити обмеження користувача у домашній директорії – «chroot_local_user=YES». Подібно змінюємо і інші параметри, за потреби. Після змін перезавантажуємо сервер командою «sudo systemctl restart vsftpd» (рис. 12.14).

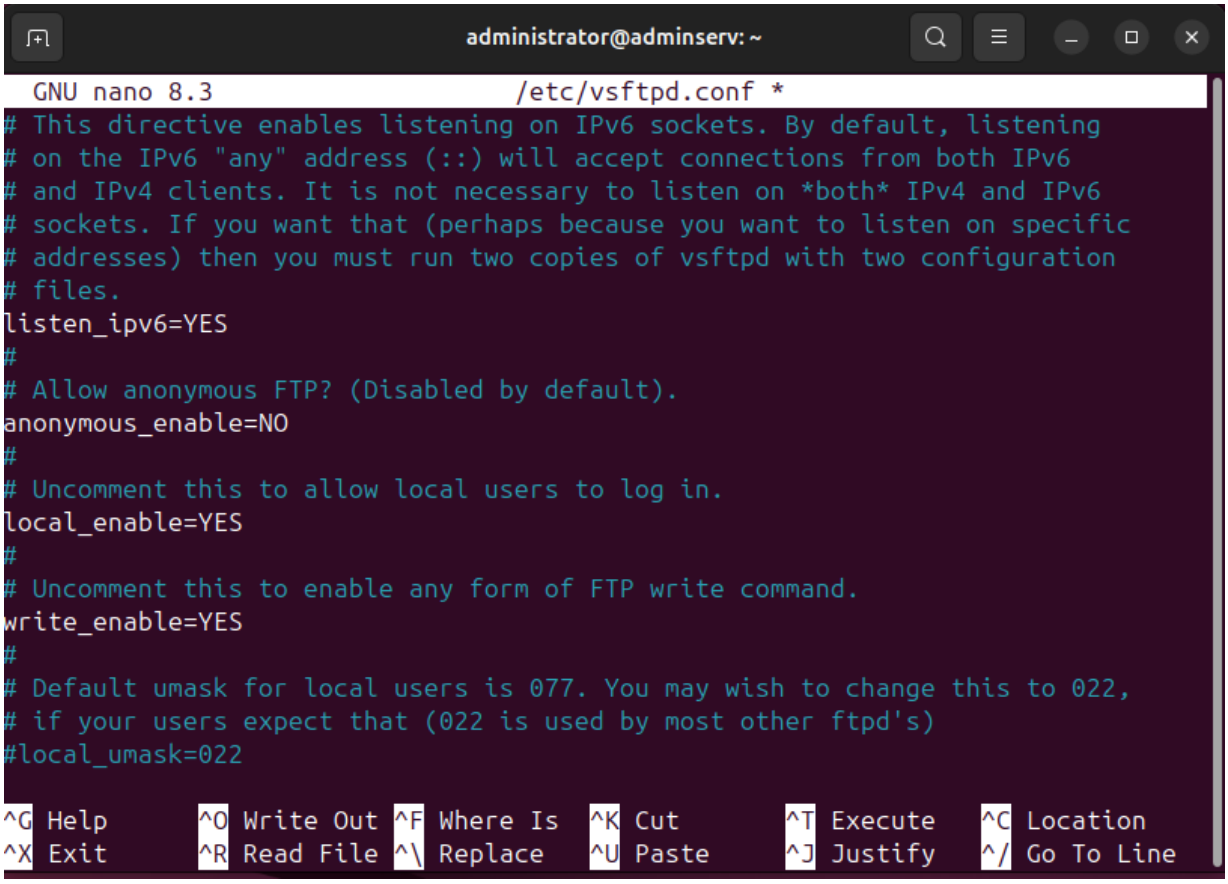

Рисунок 12.14 – Зміна конфігураційного файлу для налаштування FTP-сервера

Якщо потрібно виконати створення користувачів для FTP, то це виконується за наступним алгоритмом. Створюємо нового користувача командою «sudo adduser ftpuser». Присвоюємо пароль та створюємо домашню директорію «/home/ftpuser». На наступному етапі дозволяємо доступ до FTP – користувач буде автоматично використовувати свій домашній каталог (рис. 12.15).

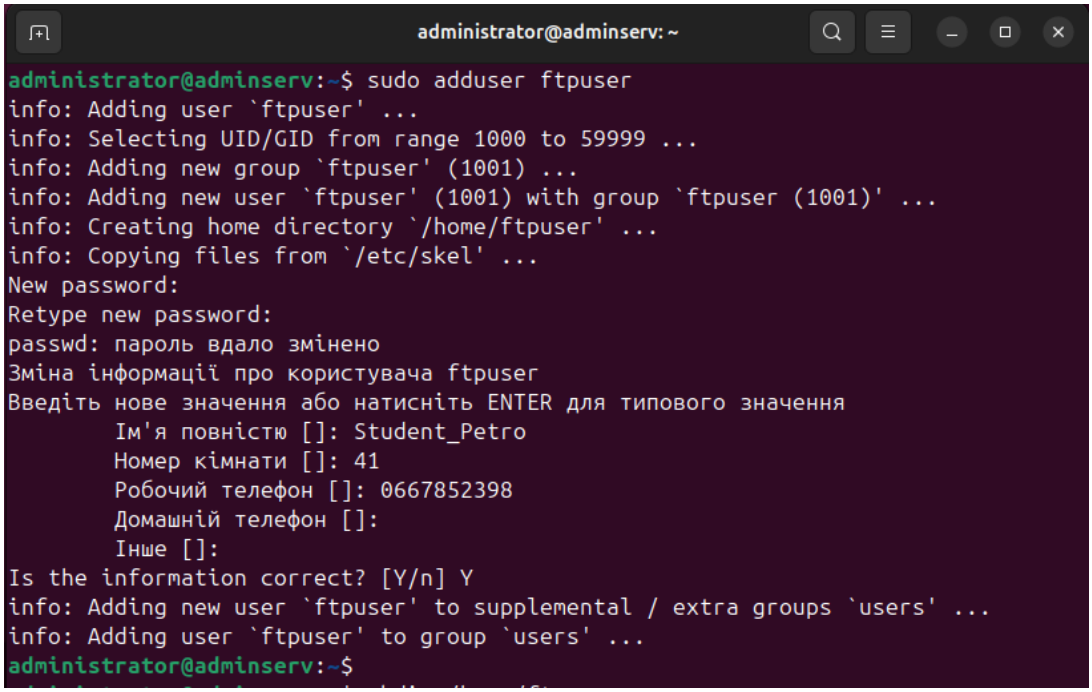

Рисунок 12.15 – Створення нового користувача для FTP-сервера

Для підключення до FTP-сервера через командний рядок Linux застосовуємо команду «ftp <IP-серверу>». Вказуємо логін та пароль.

Для підключення через графічні FTP-клієнти застосовують FileZilla та WinSCP. В цьому випадку під'єднання проводиться через IP-сервера, протокол FTP, порт – «21» та логін і пароль.

Для налаштувань безпеки використовуємо FTPS для шифрування з'єднання, для цього в конфігураційному файлі «/etc/vsftpd.conf» додати (рис. 12.16):

ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.key

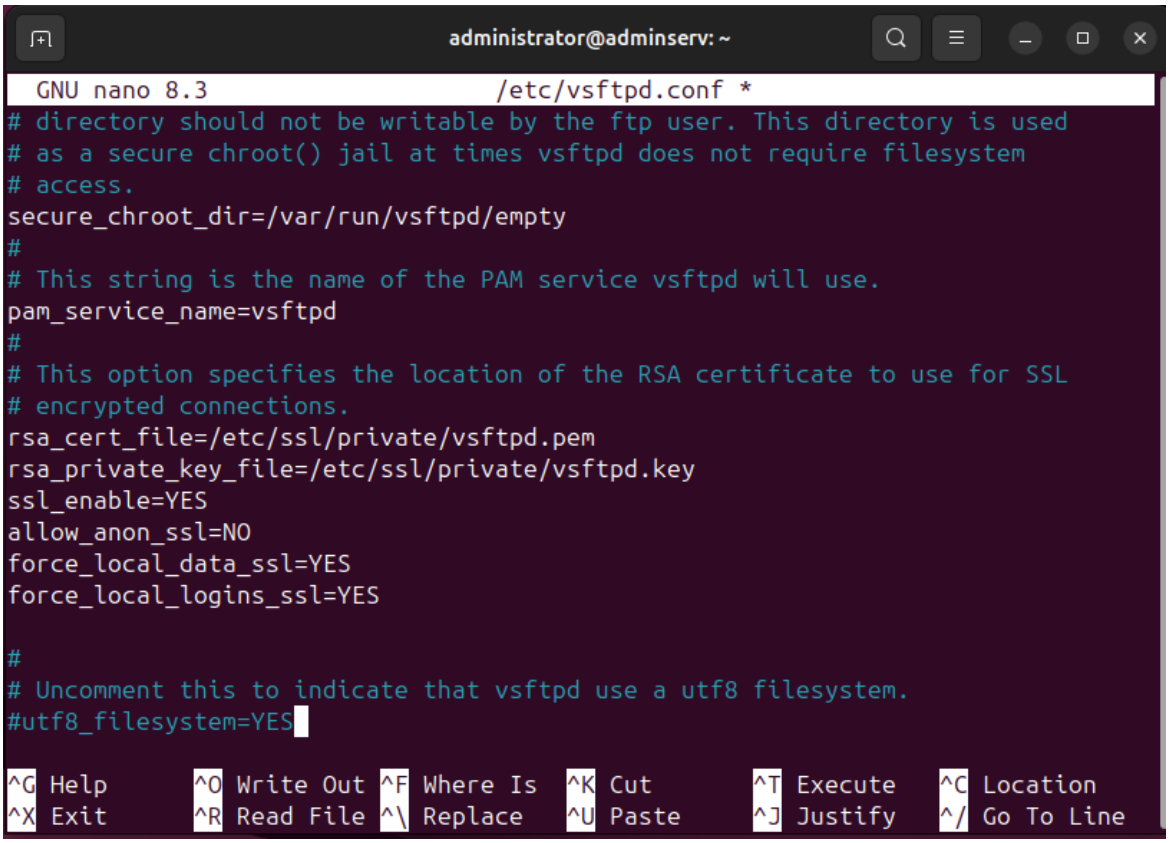

Рисунок 12.16 – Зміна конфігураційного файлу для налаштувань безпеки

Зберігаємо зміни та після цього створюємо сертифікат SSL командою «sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/private/vsftpd.pem». Далі перезавантажуємо FTP-сервер після змін командою «sudo systemctl restart vsftpd» (рис. 12.17-12.18).

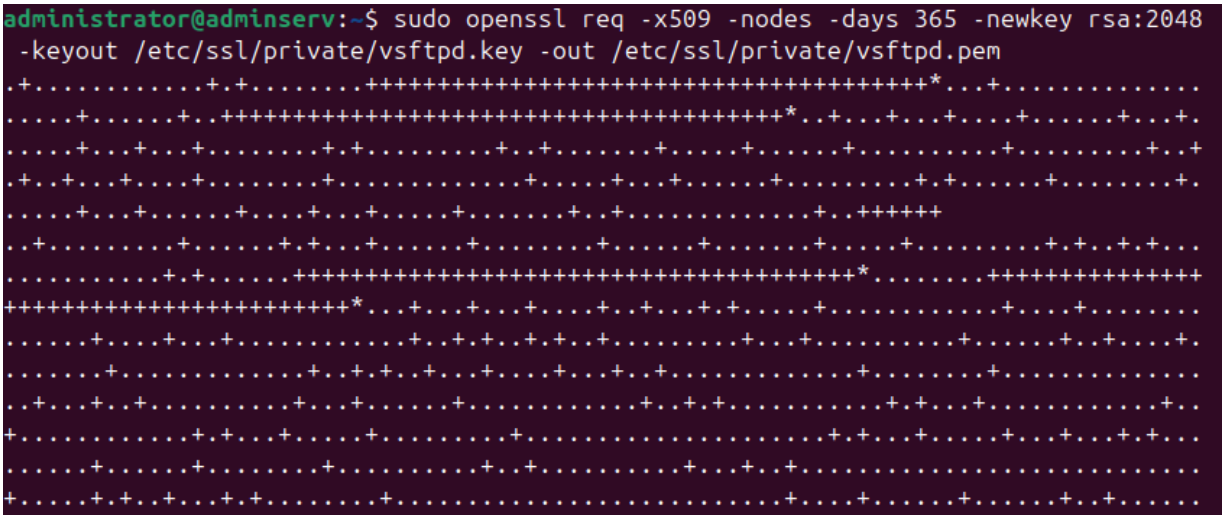

Рисунок 12.17 – Створення сертифікату SSL

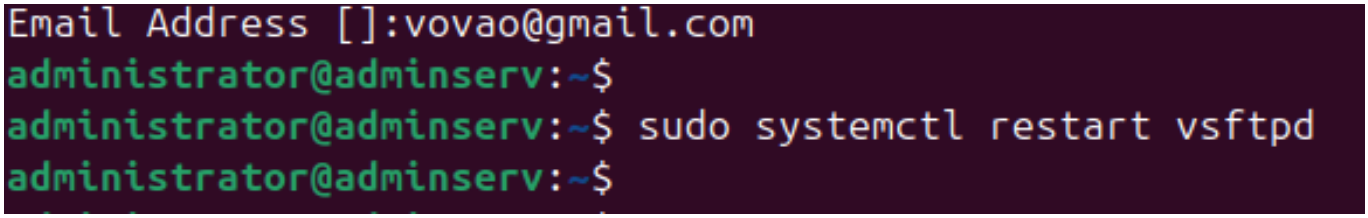

Рисунок 12.18 – Перезавантаження FTP-сервера після налаштування

Завдання 3. Аналіз безпеки веб-сервера у Linux

Для аудиту безпеки веб-сервера встановлюємо інструмент Lynis для перевірки системи командою «sudo apt install lynis –y» (рис. 12.19).

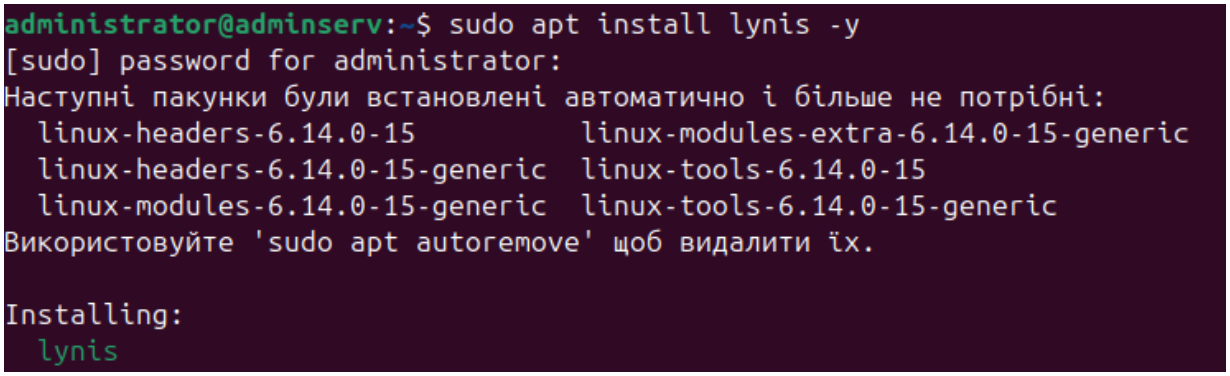

Рисунок 12.19 – Встановлення інструменту «Lynis»

Після встановлення запускаємо базовий аудит – «sudo lynis audit system». Перевіряються права файлів, налаштування сервера, відкриті порти та можливі вразливості. Далі вивчаємо і аналізуємо результати, шукаємо помилки з категорії «Warning» або «Suggestion» (рис. 12.20).

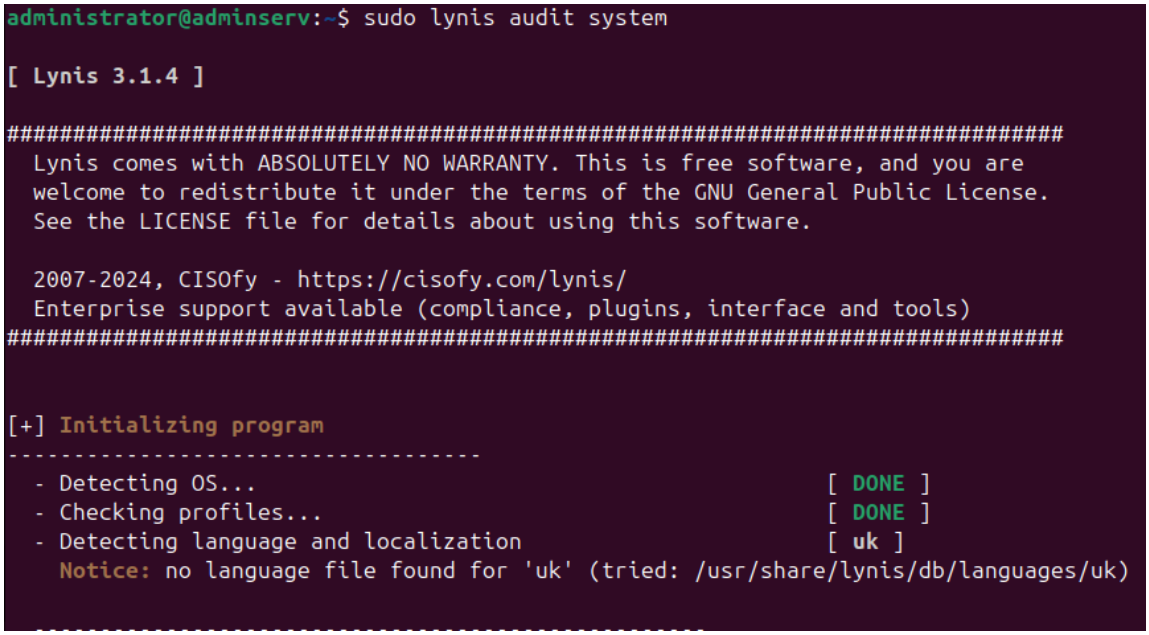

Рисунок 12.20 – Проведення аудиту інструментом «Lynis»

Для захисту від несанкціонованого доступу. Встановлюємо та налаштовуємо «Fail2Ban» для захисту від brute-force атак. Щоб це виконати застосовуємо команду «sudo apt install fail2ban –y», далі «sudo systemctl enable fail2ban» і «sudo systemctl start fail2ban» (рис. 12.21).

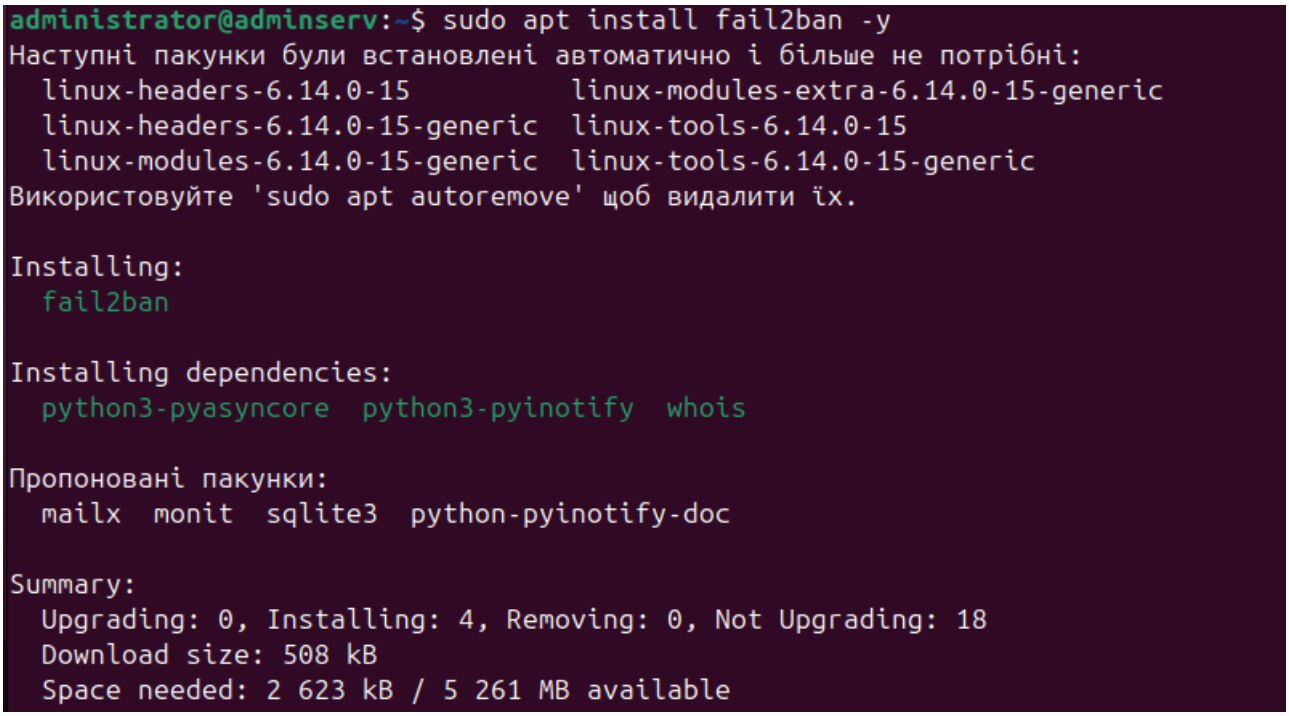

Рисунок 12.21 – Встановлення «Fail2Ban»

Потім створюємо локальні правила для захисту веб-сервера через термінал командою «sudo nano /etc/fail2ban/jail.local» (рис. 12.22-12.23).

```
administrator@adminserv:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/syste
md-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban

administrator@adminserv:~$ sudo systemctl start fail2ban
administrator@adminserv:~$
administrator@adminserv:~$ sudo nano /etc/fail2ban/jail.local
```

Рисунок 12.22 – Запуск «Fail2Ban» та створення локальних правил

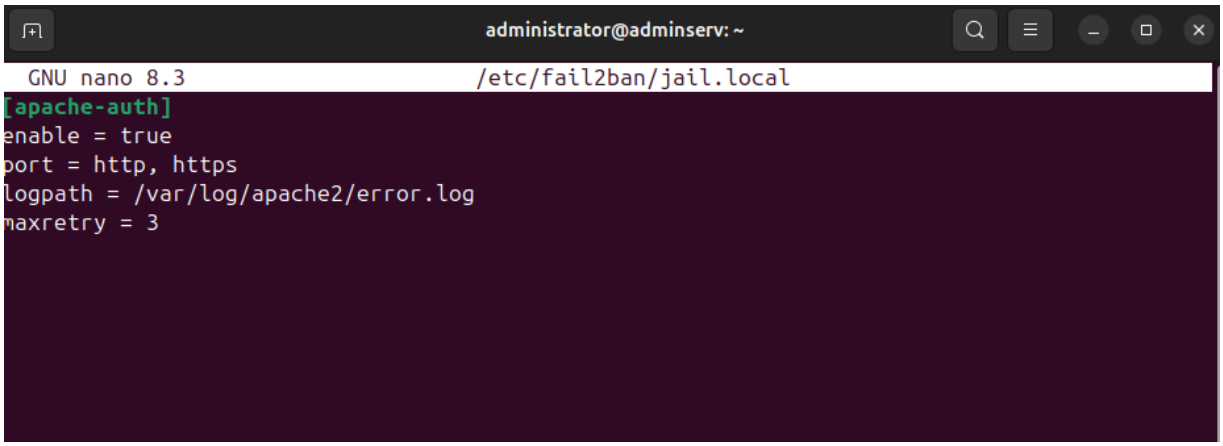

Рисунок 12.23 – Запис локальних правил

Для тестування вразливостей використовуємо «nmap» для виявлення відкритих портів та сервісів – застосовуємо команду «sudo nmap -sV -p 1-1000 <IP-серверу>». Перед цим «nmap» потрібно встановити командою «sudo apt install nmap –y» (рис. 12.24).

```
administrator@adminserv:~$
administrator@adminserv:~$ sudo nmap -sV -p 1-1000 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 21:30 EEST
Nmap scan report for 192.168.56.1
Host is up (0.0024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds
administrator@adminserv:~$
```

Рисунок 12.24 – Тестування вразливостей з використанням «nmap»

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курс Мережевої академії Cisco CCNA: Introduction to Networks URL: https://www.netacad.com/courses/networking/ccna-introduction-networks (дата звернення: 18.05.2025).

2. Комп'ютерні мережі. Книга 1: навчальний посібник / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Львів: «Магнолія 2006», 2023. 256 с.

3. Комп'ютерні мережі. Книга 2: навчальний посібник / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Львів: «Магнолія 2006», 2023. 312 с.

4. Dauti B. Windows Server 2025 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments: Fourth Edition. Birmingham : Packt Publishing, 2025. 634 p.

5. Subnetting: Brushing up on the fundamentals. Network World. URL: https://www.networkworld.com/article/969792/subnetting-brushing-up-on-the-fundamentals.html?utm_source=chatgpt.com (date of access: 20.05.2025).

6. IPv4 Subnet Cheat Sheet. StationX. URL: https://www.stationx.net/ipv4-subnet-cheat-sheet/?utm_source=chatgpt.com (date of access: 21.05.2025).

7. A complete beginner's guide to subnetting. network fun-times. URL: https://www.networkfuntimes.com/a-complete-beginners-guide-to-subnetting/?utm_source=chatgpt.com (date of access: 21.05.2025).

8. Windows Server 2019 Beginners Video Tutorials. URL: http://surl.li/mkrxs (дата звернення: 21.05.2025).

9. CodeUA. Курс Основи адміністрування Windows Server Огляд серверних операційних систем (ОС), 2023. YouTube. URL: https://www.youtube.com/watch?v=JA2Gjz9Sibg (дата звернення: 21.05.2025).

10. CodeUA. Курс Основи адміністрування Windows Server Базові інструменти адміністрування ОС, 2023. YouTube. URL: https://www.youtube.com/watch?v=rWLgcbixkF8 (дата звернення: 21.05.2025).

11. Огляд Microsoft Windows Server 2025. URL: https://softlist.com.ua/ua/news/oglyad-microsoft-windows-server (дата звернення: 21.05.2025).

12. Операційна система Windows Server. Microsoft. Чому варто вибрати Windows Server 2025? URL: https://www.microsoft.com/uk-ua/windows-server (дата звернення: 21.05.2025).

13. Discover what's new in Windows Server 2025. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/windows-server-2025-data-sheet.pdf (date of access: 29.05.2025).

14. Windows Server 2025 URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025 (date of access: 29.05.2025).

15. What is Windows Server?. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/uk-ua/windows-server/get-started/overview (date of access: 29.05.2025).

16. Install Hyper-V in Windows and Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-

us/windows-server/virtualization/hyper-v/get-started/install-hyper-v?utm_source=chatgpt.com&tabs=powershell&pivots=windows (date of access: 02.06.2025).

17. Create a virtual machine in Hyper-V. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v?utm_source=chatgpt.com&tabs=hyper-v-manager (date of access: 02.06.2025).

18. What's new in Windows Server 2025. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-windows-server-2025?utm_source=chatgpt.com (date of access: 04.06.2025).

19. Hyper-V virtualization in Windows Server and Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/overview?utm_source=chatgpt.com (date of access: 05.06.2025).

20. System Requirements for Hyper-V on Windows and Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/host-hardware-requirements?utm_source=chatgpt.com&pivots=windows (date of access: 07.06.2025).

21. Windows Server 2025 | Microsoft Evaluation Center. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025?utm_source=chatgpt.com (date of access: 07.06.2025).

22. Active Directory overview - Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/active-directory-overview?utm_source=chatgpt.com (date of access: 10.06.2025).

23. Install Active Directory Domain Services on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-?utm_source=chatgpt.com (date of access: 12.06.2025).

24. Install Active Directory Domain Services on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-?utm_source=chatgpt.com (date of access: 12.06.2025).

25. Active Directory Domain Services overview. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview?utm_source=chatgpt.com (date of access: 15.06.2025).

26. Group Policy overview for Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview (date of access:

15.06.2025).

27. Group Policy preferences in Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-preferences (date of access: 15.06.2025).

28. Group Policy Management Console in Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-management-console (date of access: 15.06.2025).

29. The Admin's Guide to Group Policy Best Practices | Netwrix. Data Security that Starts with Identity| Netwrix. URL: https://netwrix.com/en/resources/guides/group-policy-best-practices/ (date of access: 15.06.2025).

30. Group Policy Management Guide. Active Directory Pro. URL: https://activedirectorypro.com/group-policy-guide/ (date of access: 15.06.2025).

31. Group Policies and Group Policies Preferences (2025). Hybrid Infrastructure and Cloud Architecture. URL: https://hartiga.de/windows-server/group-policies-foundation/ (date of access: 15.06.2025).

32. Install and Configure DNS Server on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server?utm_source=chatgpt.com&tabs=powershell (date of access: 19.06.2025).

33. Manage DNS zones using DNS server in Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/manage-dns-zones?utm_source=chatgpt.com&tabs=powershell (date of access: 19.06.2025).

34. What is DHCP Server in Windows Server?. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top (date of access: 19.06.2025).

35. Install and configure DHCP Server on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server?tabs=powershell (date of access: 19.06.2025).

36. Guidance for troubleshooting DHCP - Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/troubleshoot-dhcp-guidance (date of access: 21.06.2025).

37. Migrate existing DHCP failover deployment on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/migrate-existing-dhcp-failover?tabs=powershell (date of access: 21.06.2025).

38. Windows Server Security documentation. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/security/security-and-assurance?utm_source=chatgpt.com (date of access: 21.06.2025).

39. Windows Server 2025: Install IIS Web Server - RDR-IT. RDR-IT. URL: https://rdr-it.com/en/windows-server-2025-install-iis-web-server/ (date of access: 21.06.2025).

40. Configuring IIS for Web Hosting on Windows: A Step-by-Step Guide. Kamatera. URL: https://www.kamatera.com/knowledgebase/configuring-iis-for-web-hosting-on-windows/ (date of access: 21.06.2025).

41. Ubuntu Server documentation. Ubuntu Server. URL: https://documentation.ubuntu.com/server/ (date of access: 27.06.2025).

42. Munna R. Linux DNS Server Configuration: Detailed Guide [2025]. MailServerGuru. URL: https://mailserverguru.com/linux-dns-server/?utm_source=chatgpt.com#Master-Update-the-System (date of access: 27.06.2025).

43. Imron M. Guide to Creating a Simple Web Server Using Nginx and Apache2. Medium. URL: https://medium.com/@muhammadimron1410/guide-to-creating-a-simple-web-server-using-nginx-and-apache2-ae7d27b421c6 (date of access: 27.06.2025).

Для нотаток

Для нотаток

А31 Адміністрування комп’ютерних мереж та систем: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузі знань 12 (F) Інформаційні технології спеціальності 123 (F7) Комп’ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, О. Л. Кайдик, К. Я. Бортник. Луцьк: ЛНТУ, 2025. 144 с.

Методичне видання до лабораторних робіт з дисципліни «Адміністрування комп’ютерних мереж та систем» складене відповідно до діючої програми курсу.

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

Комп’ютерний набір Н. В. Багнюк

Редактор Н. В. Багнюк

Підп. до друку «___» _____ 2025р.

Формат 60х84/16. Папір офс. Гарнітура Таймс.

Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій

Луцького національного технічного університету

43018, м. Луцьк, вул. Львівська, 75