Міністерство освіти і науки України

ІНФОРМАЦІЙНІ МЕРЕЖІ ТА АДМІНІСТРУВАННЯ

Методичні вказівки до лабораторних робіт
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми
«Інформаційні системи та технології охорони і безпеки»
галузь знані 12 (F) Інформаційні технології
спеціальності 126 (F6) Інформаційні системи та технології
денної та заочної форм навчання

Луцьк 2025

УДК 004.65(07)
Б17

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

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

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

І-74 Інформаційні мережі та адміністрування: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2025. 73 с.

Методичне видання до лабораторних робіт з дисципліни «Інформаційні мережі та адміністрування» складено відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 126 (F6) Інформаційні системи та технології освітньої програми «Інформаційні системи та технології охорони і безпеки».

ЗМІСТ

ВСТУП

Сучасні інформаційні системи потребують надійної мережевої інфраструктури та кваліфікованого адміністрування, що забезпечує стабільність функціонування, безпеку даних та швидке реагування на зміни в середовищі. У професійній діяльності фахівця з інформаційних технологій особливе місце посідають уміння моделювати мережі, налаштовувати протоколами передачі даних, виявляти та усувати помилки, а також забезпечувати взаємодію різних програмно-технічних компонентів.

Методичні вказівки до лабораторних робіт з дисципліни «Інформаційні мережі та адміністрування» спрямовані на формування практичних компетентностей щодо роботи з мережевими протоколами, серверними платформами та інструментами адміністрування. Запропоновані лабораторні роботи охоплюють актуальні напрями сучасних мережевих технологій, такі як: адресація IPv4/IPv6, маршрутизація між VLAN, аналіз мережного трафіку за допомогою Wireshark, моніторинг DNS-перетворень, розгортання серверних платформ Windows Server 2025 та Linux у віртуальному середовищі

Кожна робота містить покрокові інструкції, практичні завдання та запитання для самоконтролю, що сприяє розвитку навичок критичного мислення та професійного аналізу отриманих результатів. Виконання лабораторних робіт передбачає використання програмних засобів Cisco Packet Tracer [1], Wireshark, Hyper-V та інструментів конфігурації мережевого обладнання, що наближає процес навчання до реальних виробничих умов.

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 імплементований в робочу програму дисципліни «Інформаційні мережі та адміністрування». В основному цей курс виноситься на самостійне опрацювання студентів, але окремі практичні завдання винесені на практичні заняття та лабораторні роботи (відповідно вказано запозичення даного матеріалу з цих ресурсів згідно вимог до оформлення посилання на літературні джерела), що зазначено в робочій програмі дисципліни. Також вивчаються окремі розділи курсів «Основи комутації, маршрутизації та бездротових мереж» та «Побудова, безпека і автоматизація корпоративних мереж».

Методичні вказівки призначені для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 126 «Інформаційні системи та технології», денної та заочної форм навчання. Виконання запропонованих лабораторних робіт забезпечує формування практичних навичок проєктування мережних рішень, конфігурування мережевого обладнання та адміністрування серверних систем, що є необхідною складовою професійної підготовки майбутнього фахівця в галузі інформаційних технологій.

Лабораторна робота 1
Обчислення підмереж IPv4

Мета роботи: закріплення знань щодо визначення IP-адреси мережі на основі заданої IP-адреси та маски підмережі [2].

Заповніть наведені нижче таблиці відповідями про задану IPv4-адресу вузла, вихідну та нову маски підмережі [2].

Завдання 1.

Дано:	
IP-адреса вузла:	192.168.200.139
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:	10.101.99.228
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:	172.22.32.12
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:	192.168.1.245
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:	128.107.0.55
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:	192.135.250.180
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 [2]?

Лабораторна робота 2
Перевірка адресації IPv4 і IPv6

Мета роботи: дослідити реалізацію подвійного стека IPv4 і IPv6, включаючи документування, перевірку з'єднання та трасування [2].

Завдання: доповнити документування таблиці адресації (табл. 2.1), перевірити з'єднання за допомогою команди ping, виявити шляхи трасуванням маршруту (рис. 2.1) [2].

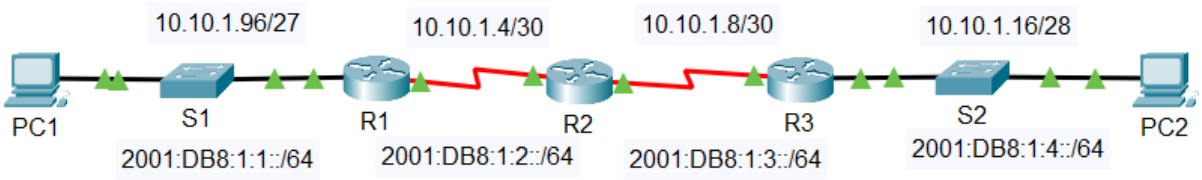

Рисунок 2.1– Топологія мережі

Таблиця 2.1 – Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс		Шлюз за замовчуванням
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:db8:1:1::1/64		
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:db8:1:2::2/64		
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:db8:1:2::1/64		
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:db8:1:3::1/64		
		fe80::2		
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:db8:1:4::1/64		
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:db8:1:3::2/64		
		fe80::3		
PC1	NIC			
PC2	NIC			

Хід роботи

Доповнення документування таблиці адресації (табл. 2.1).

1. Використати команду ipconfig для перевірки адресації IPv4 [2]:

– натисніть на PC1 та відкрийте Command Prompt;

– введіть команду ipconfig /all для збору даних про IPv4. Внесіть дані в таблицю адресації вказавши IPv4-адресу, маску підмережі та шлюз за замовчуванням;

– натисніть на PC2 та відкрийте Command Prompt;

– введіть команду ipconfig /all для збору даних про IPv4. Внесіть дані в таблицю адресації вказавши IPv4-адресу, маску підмережі та шлюз за замовчуванням.

2. Використати команду ipv6config для перевірки адресації IPv6:

– на PC1, введіть команду ipv6config /all для збору даних про IPv6. Внесіть дані в таблицю адресації вказавши IPv6-адресу, префікс підмережі та шлюз за замовчуванням;

– на PC2, введіть команду ipv6config /all для збору даних про IPv6. Внесіть дані в таблицю адресації вказавши IPv6-адресу, префікс підмережі та шлюз за замовчуванням.

3. Перевірка з'єднання. Використати команду ping для перевірки IPv4-з'єднання:

– з PC1 пропінгуйте IPv4-адресу PC2 (додати скрін виконання команди та пояснити результат?);

– з PC2 пропінгуйте IPv4-адресу PC1 (додати скрін виконання команди та пояснити результат?).

4. Використати команду ping для перевірки IPv6-з'єднання.

– з PC1 пропінгуйте IPv6-адресу PC2 (додати скрін виконання команди та пояснити результат?);

– з PC2 пропінгуйте IPv6-адресу PC1 (додати скрін виконання команди та пояснити результат?).

5. Виявлення шляху трасуванням маршруту. Використати команду tracert для виявлення шляху IPv4.

– з PC1 виконайте трасування маршруту до PC2:

PC> tracert 10.10.1.20

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди.

– з PC2 виконайте трасування маршруту до PC1.

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди;

6. Використати команду tracert для виявлення шляху IPv6:

– з PC1 виконайте трасування маршруту до IPv6-адреси PC2:

PC> tracert 2001:db8:1:4::a

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди;

– З PC2 виконайте трасування маршруту до IPv6-адреси PC1.

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси [2]? Додати в звіт скріни виконання команди.

Лабораторна робота 3
Використання Wireshark для перегляду мережного трафіку

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

Завдання: перехопити та проаналізувати локальні та віддалені ICMP-дані за допомогою Wireshark (рис. 3.1) [2].

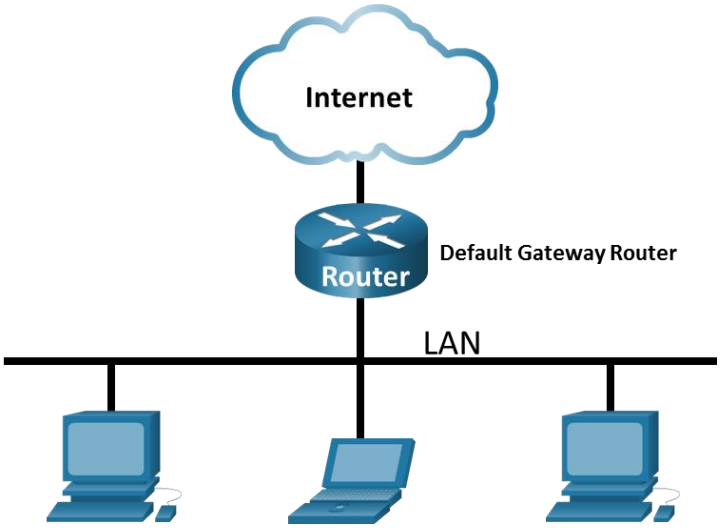

Рисунок 3.1 – Топологія мережі

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 [2].

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. 3.2).

```
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 3.2 – 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. 3.3).

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 3.3 – Пінг IP-адреси

Зверніть увагу на те, що дані знову з’являються у верхній частині вікна Wireshark (рис. 3.4).

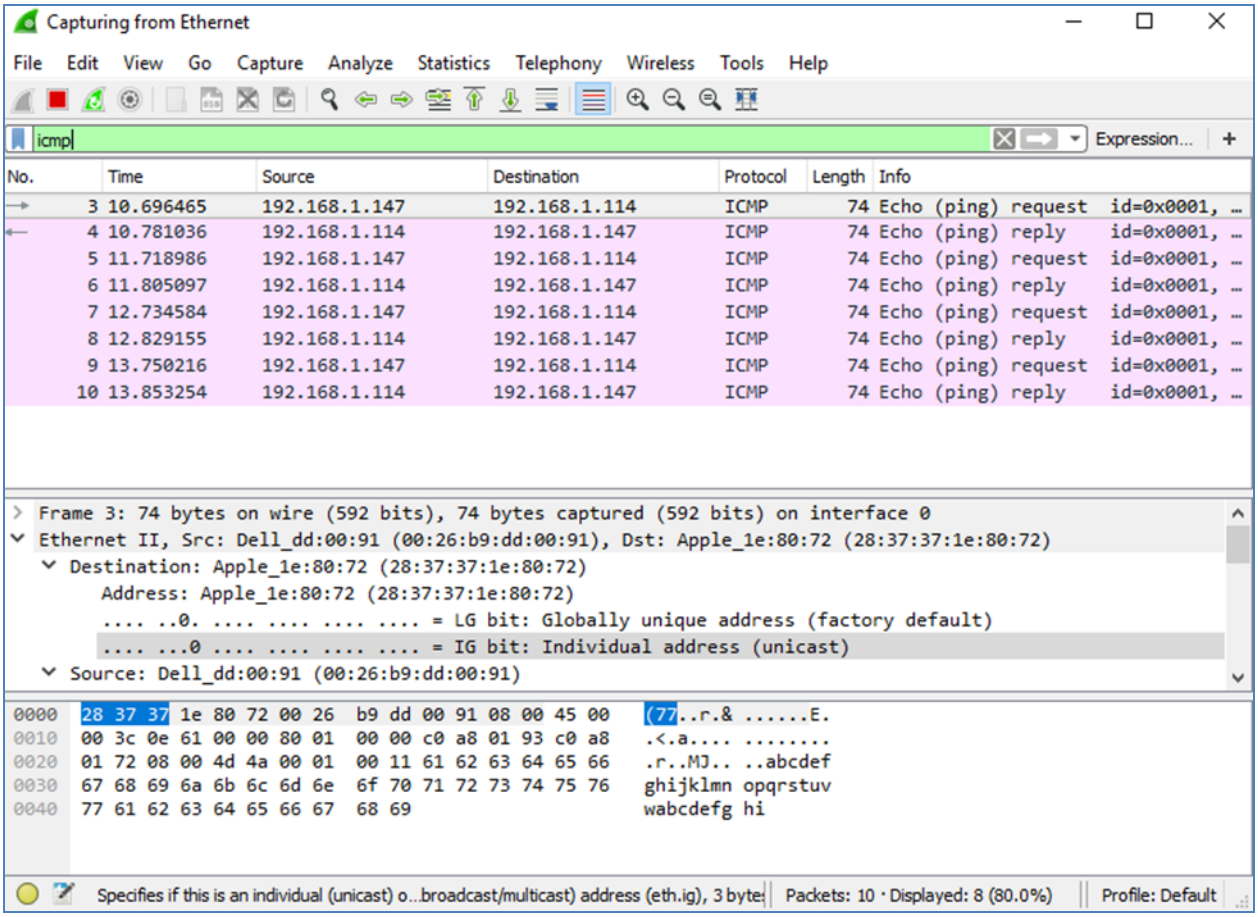

Рисунок 3.4 – Вікно Wireshark з даними

Примітка. Якщо ПК члена Вашої команди не відповідає на Ваші ping-запити, причиною може бути блокування цих запитів його міжмережним екраном. В 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 4
Впровадження маршрутизації між VLAN

Мета роботи: опанування принципи логічного поділу мережі за допомогою віртуальних локальних мереж (VLAN), набути практичні навички налаштування маршрутизації між VLAN для забезпечення взаємодії між різними сегментами мережі.

Завдання: налаштувати базові параметрів пристрою, створити мережі VLAN і призначити порти комутатора, налаштувати магістральний канал 802.1Q між комутаторами, налаштувати маршрутизацію між VLAN на маршрутизаторі, перевірити працездатність маршрутизації між VLAN (рис. 4.1) [2].

Хід роботи

Створити топологію як на рисунку 4.1, налаштувати адресацію згідно таблиці 4.1 та створити vlan згідно таблиці 4.2 [3-6].

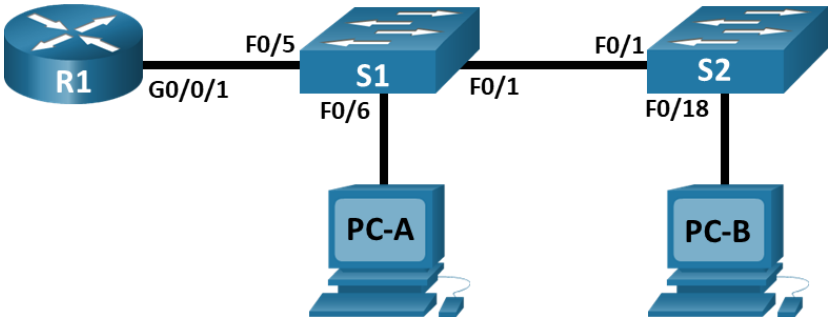

Рисунок 4.1 – Топологія мережі

Таблиця 4.1 − Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/0/1.20	192.168.20.1	255.255.255.0	
	G0/0/1.30	192.168.30.1	255.255.255.0	
	G0/0/1.1000	N/A	N/A	
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC-B	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Таблиця 4.2 − Таблиця VLAN

VLAN	Ім’я	Призначений інтерфейс
10	Management	S1: VLAN 10 S2: VLAN 10
20	Sales	S1: F0/6
30	Operations	S2: F0/18
999	Parking_Lot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2
1000	Native	N/A

Сучасні комутатори використовують віртуальні локальні мережі (VLAN) для поліпшення продуктивності мережі, розділяючи великі широкомовні домени рівня 2 на менші. VLAN також можна використовувати як засіб безпеки, відокремлюючи трафік конфіденційних даних від решти мережі. Загалом, VLAN спрощують проєктування мережі для досягнення цілей організації. Для зв’язку між VLAN потрібен пристрій, що працює на рівні 3 моделі OSI. Додавання маршрутизатора між VLAN дозволяє організації розмежувати і розділяти широкомовні домени, одночасно дозволяючи їм спілкуватися один з одним.

Магістральні канали VLAN використовуються для поширення VLAN на декілька пристроїв. Магістральні канали дозволяють трафіку з декількох VLAN рухатися по одному каналу, зберігаючи ідентифікацію та сегментацію VLAN незмінними. Особливий вид маршрутизації між VLAN, названий «Router-On-A-Stick», використовує магістральний канал від маршрутизатора до комутатора, щоб всі VLAN могли проходити на маршрутизатор.

У цій лабораторній роботі ви створите VLAN на обох комутаторах в топології, призначите VLAN для портів доступу комутатора, переконаєтесь, що VLAN працюють належним чином, створите магістральні канали VLAN між двома комутаторами і між S1 і R1, а також налаштуєте маршрутизацію між VLAN на R1, щоб дозволити вузлам в різних VLAN спілкуватися, незалежно від того, в якій підмережі знаходиться вузол.

Примітка. Маршрутизатори, що використовуються в лабораторній роботі − Cisco 4321, комутатори − Cisco Catalyst 2960.

Виконати наступні пункти:

1) створіть мережу та налаштуйте базові параметрів пристрою:

– з’єднайте пристрої у мережу, відповідно до схеми топології;

– приєднайте пристрої необхідними кабелями, як показано на схемі топології;

2) налаштуйте основні параметри на маршрутизаторі:

– підключіть консольне з’єднання до маршрутизатора і увійдіть в привілейований режим EXEC;

Router> enable

– увійдіть до режиму конфігурації;

Router# config terminal

– призначте маршрутизатору ім’я;

Router(config)# hostname R1

– вимкніть пошук DNS, щоб упередити маршрутизатор від спроби неправильно перекласти введені команди: ніби вони є іменами хостів;

R1(config)# no ip domain lookup

– призначте class як зашифрований пароль привілейованого режиму EXEC;

R1(config)# enable secret class

– призначте cisco як пароль доступу до консолі і активуйте авторизацію;

R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login

– призначте cisco як пароль для віртуальних ліній і активуйте авторизацію;

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login

– зашифруйте всі відкриті текстові паролі;

R1(config)# service password-encryption

– створіть банер, який попереджатиме всіх, хто має доступ до пристрою, про те, що несанкціонований доступ заборонено;

R1(config)# banner motd $ Authorized Users Only! $

– збережіть поточну конфігурацію у файл стартової конфігурації;

R1(config)# exit
R1# copy running-config startup-config

– встановіть час на маршрутизаторі;

R1# clock set 14:30:00 27 Aug 2025

– закрийте вікно конфігурації.

2) налаштуйте базові параметри для кожного комутатора:

– призначте комутатору ім’я;

switch(config)# hostname S1
switch(config)# hostname S2

– вимкніть пошук DNS, щоб упередити комутатор від спроби неправильно перекласти введені команди: ніби вони є іменами хостів;

S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup

– призначте class як зашифрований пароль на привілейований режим EXEC;

S1(config)# enable secret class
S2(config)# enable secret class

– призначте cisco як пароль на консольній лінії і активуйте авторизацію;

S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login

S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login

– призначте cisco як пароль для віртуальних ліній і активуйте авторизацію;

S1(config)# line vty 0 4

```
S1(config-line)# password cisco
S1(config-line)# login

S2(config)# line vty 0 4
S2(config-line)# password cisco
S2(config-line)# login
```
– зашифруйте всі відкриті текстові паролі;
```
S1(config)# service password-encryption
S2(config)# service password-encryption
```
– створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено;
```
S1(config)# banner motd $ Authorized Users Only! $
S2(config)# exit
S2(config)# banner motd $ Authorized Users Only! $
S2(config)# exit
```
– встановіть час на комутаторі;
```
S1# clock set 14:30:00 27 Aug 2025
S2# clock set 14:30:00 27 Aug 2025
```
– збережіть поточні налаштування у файлі початкової конфігурації;
```
S1# copy running-config startup-config
S2# copy running-config startup-config
```
3) налаштуйте вузли PC:

– зверніться до таблиці адресації для визначення адресної інформації вузлів.

4) створення мереж VLAN і призначення портів комутатора:

– створіть VLAN, як зазначено в таблиці вище, на обох комутаторах, призначите VLAN відповідному інтерфейсу і перевірите свої налаштування конфігурації. Виконайте наступні налаштування на кожному комутаторі;

– Створіть і назвіть необхідні VLAN на кожному комутаторі з таблиці вище.

```
S1(config)# vlan 10
S1(config-vlan)# name Management
S1(config-vlan)# vlan 20
S1(config-vlan)# name Sales
S1(config-vlan)# vlan 30
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 999
S1(config-vlan)# name Parking_Lot
S1(config-vlan)# vlan 1000
S2(config-vlan)# name Native
S1(config-vlan)# exit

S2(config)# vlan 10
S2(config-vlan)# name Management
S2(config-vlan)# vlan 20
S2(config-vlan)# name Sales
S2(config-vlan)# vlan 30
S2(config-vlan)# name Operations
```

S2(config-vlan)# vlan 999
S2(config-vlan)# name Parking_Lot
S2(config-vlan)# vlan 1000
S2(config-vlan)# name Native
S2(config-vlan)# exit

– налаштуйте інтерфейс керування та шлюз за замовчуванням на кожному комутаторі, використовуючи відомості про IP-адресу в таблиці адресації;

S1(config)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1

S2(config)# interface vlan 10
S2(config-if)# ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1

– призначте всі невикористані порти на обох комутаторах у ParkingLot VLAN, налаштуйте їх на статичний режим доступу і адміністративно дезактивуйте.

Примітка. Команда interface range корисна для виконання цього завдання з якомога меншою кількістю команд.

S1(config)# interface range f0/2 - 4 , f0/7 - 24 , g0/1 - 2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown

S2(config)# interface range f0/2 - 17, f0/19 - 24 , g0/1 - 2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown

5) призначте VLAN відповідним інтерфейсам комутатора:

– призначте використовувані порти відповідній VLAN (зазначеній у таблиці VLAN вище) та налаштуйте їх на статичний режим доступу;

S1(config)# interface f0/6
S1(config-if)# switchport mode acces
S1(config-if)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport mode acces
S2(config-if)# switchport access vlan 30

– переконайтеся, що VLAN призначені правильним інтерфейсам;

S1# show vlan brief

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/5
```

```
10 Management active
20 Sales active Fa0/6
30 Operations active
999 Parking_Lot active Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddi-default act/unsup
1005 trnet-default act/unsup
```

S2# show vlan brief

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1
10 Management active
20 Sales active
30 Operations active Fa0/18
999 Parking_Lot active Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddi-default act/unsup
1005 trnet-default act/unsup
```

6) налаштуйте інтерфейс магістрального каналу F0/1 вручну на комутаторах S1 і S2:

– налаштуйте статичний магістральний канал на інтерфейсі F0/1 для обох комутаторів;

S1(config)# interface f0/1
S1(config-if)# switchport mode trunk

S2(config)# interface f0/1
S2(config-if)# switchport mode trunk

– встановіть для native VLAN 1000 на обох комутаторах;

S1(config-if)# switchport trunk native vlan 1000

S2(config-if)# switchport trunk native vlan 1000

– уточніть, що VLAN 10, 20, 30 і 1000 дозволені на магістральному каналі;

S1(config-if)# switchport trunk allowed vlan 10,20,30,1000

S2(config-if)# switchport trunk allowed vlan 10,20,30,1000

– перевірте магістральні порти, Native VLAN і дозволені VLAN на магістральному каналі;

S1# show interfaces trunk

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk
Fa0/1 10,20,30,1000

Port Vlans allowed and active in management domain
Fa0/1 10,20,30,1000

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,20,30,1000
```

S2# show interfaces trunk

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk
Fa0/1 10,20,30,1000

Port Vlans allowed and active in management domain
Fa0/1 10,20,30,1000

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,20,30,1000
```

8) вручну налаштуйте магістральний інтерфейс S1 F0/5:

– налаштуйте інтерфейс S1 F0/5 з тими ж параметрами магістралі, що і F0/1. Це магістральний канал до маршрутизатора;

– збережіть поточні налаштування у файлі початкової конфігурації;

S1# copy running-config startup-config

S2# copy running-config startup-config

– перевірка магістрального каналу.

Дайте відповідь на запитання. Що станеться, якщо G0/0/1 на R1 вимкнеться?

9) налаштуйте маршрутизацію між VLAN на маршрутизаторі:

– активуйте інтерфейс G0/0/1 на маршрутизаторі;

R1(config)# interface g0/0/1
R1(config-if)# no shutdown
R1(config-if)# exit

– налаштуйте підінтерфейси для кожної VLAN, як зазначено в таблиці IP-адресації. Всі підінтерфейси використовують інкапсуляцію 802.1Q. Переконайтеся, що підінтерфейс для native VLAN не має IP-адреси. Налаштуйте опис для кожного під-інтерфейсу;

R1(config)# interface g0/0/1.10
R1(config-subif)# description Management Network
R1(config-subif) # encapsulation dot1q 10

```
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/0/1.20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# description Sales Network
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# interface g0/0/1.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# description Operations Network
R1(config-subif)# ip address 192.168.30.1 255.255.255.0
R1(config-subif)# interface g0/0/1.1000
R1(config-subif)# encapsulation dot1q 1000 native
R1(config-subif)# description Native VLAN
```

– перевірте, чи працюють під-інтерфейси;

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM down down
GigabitEthernet0/0/1 unassigned YES NVRAM up up
Gi0/0/1.10 192.168.10.1 YES manual up up
Gi0/0/1.20 192.168.20.1 YES manual up up
Gi0/0/1.30 192.168.30.1 YES manual up up
Gi0/0/1.1000 unassigned YES unset up up
GigabitEthernet0 unassigned YES NVRAM down down
```

10) перевірка працездатності маршрутизації між VLAN:

Проведіть наступні тести з PC-A. Усі повинні бути успішними:

Примітка. Для успішного використання ping може знадобитися тимчасово відключити брандмауер Windows.

– відправте запит ping від PC-A до його шлюзу за замовчуванням;

– відправте запит ping від PC-A до PC-B;

– відправте запит ping від PC-A до S2.

Проведіть наступні тести з PC-B:

– у командному рядку на PC-B виконайте команду tracert на адресу PC-A.

Дайте відповідь на запитання. Які проміжні IP-адреси відображаються в результатах?

Примітка. Щоб дізнатися, як налаштований маршрутизатор, подивіться на інтерфейси, щоб визначити тип маршрутизатора та скільки інтерфейсів у маршрутизатора.

Лабораторна робота 5
Відстеження DNS-перетворень

Мета роботи: набуття практичних навичок моніторингу та аналізу процесу перетворення доменних імен у IP-адреси за допомогою системи доменних імен (DNS), а також дослідження особливостей функціонування DNS-запитів і відповідей у комп'ютерній мережі шляхом використання мережевих утиліт і засобів трасування.

Завдання: зробити огляд перетворення за допомогою протоколу DNS URL-адреси на IP-адресу, дослідити DNS-пошук адреси веб-сайту та поштових серверів за допомогою команди nslookup [2].

Теоретичний матеріал

Система доменних імен (Domain Name System, DNS) викликається під час уведення в адресному рядку веб-браузера Уніфікованого покажчика ресурсів (Uniform Resource Locator, URL), наприклад http://www.cisco.com. Перша частина URL описує протокол, який використовується. Традиційно до них належать протокол передавання гіпертексту (HTTP), протокол передавання гіпертексту через рівень захищених сокетів (Secure Socket Layer, SSL) - (HTTPS) і протокол передавання файлів (FTP) [2].

DNS використовує другу частину URL-адреси, у даному прикладі - www.cisco.com. DNS перетворює доменне ім'я (www.cisco.com) на IP-адресу, щоб вихідний вузол зміг досягти кінцевого сервера. У цій лабораторній роботі ви матимете можливість спостерігати за протоколом DNS у дії і скористаєтесь командою nslookup (пошук сервера імен) для отримання додаткової інформації про DNS.

Хід роботи

Спостереження за перетвореннями протоколу DNS URL-адрес на IP-адреси:

1) відкрийте вікно командного рядка Windows;

2) у командному рядку пропінгуйте URL-адресу Інтернет-корпорації з призначення імен і номерів (ICANN) за адресою www.icann.org. ICANN координує DNS, IP-адреси, системи керування доменними іменами верхнього рівня та функції керування кореневими серверами. Комп'ютеру потрібно перетворити cisco.com на IP-адресу, щоб знати, куди надсилати пакети Інтернет-протоколу керуючих повідомлень (Internet Control Message Protocol, ICMP).

Перший рядок виводу відображає виконане за допомогою DNS перетворення www.icann.org на IP-адресу (рис. 5.1). Результат роботи DNS повинен бути доступний для перегляду, навіть якщо у вашому закладі використовується міжмережний екран, який запобігає пінгуванню, або якщо сервер призначення забороняє звертатися за допомогою команди ping до свого веб-сервера.

Примітка. Якщо ім'я домену перетворюється на адресу IPv6, використовуйте команду ping -4 www.icann.org для переходу на адресу IPv4, якщо потрібно.

```
C:\ > ping www.icann.org

Pinging www.vip.icann.org [2620:0:2d0:200::7] with 32 bytes of data:
Reply from 2620:0:2d0:200::7: time=43ms
Reply from 2620:0:2d0:200::7: time=41ms
Reply from 2620:0:2d0:200::7: time=44ms
Reply from 2620:0:2d0:200::7: time=39ms

Ping statistics for 2620:0:2d0:200::7:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 44ms, Average = 41ms

C:\> ping -4 www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=41ms TTL=241
Reply from 192.0.32.7: bytes=32 time=42ms TTL=241
Reply from 192.0.32.7: bytes=32 time=42ms TTL=241
Reply from 192.0.32.7: bytes=32 time=43ms TTL=241

Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 41ms, Maximum = 43ms, Average = 42ms
```

Рисунок 5.1 − Виконане за допомогою DNS перетворення

Дайте відповідь на запитання. Запишіть IP-адреси для www.icann.org.

3) замість URL-адреси використайте для звернення у веб-браузері адреси IPv4 з пункту 2. Введіть https://192.0.32.7 у веб-браузері. Якщо вдалося отримати IPv6-адресу, її також можна застосувати: https://[2620:0:2d0:200::7].

4) зверніть увагу, що домашня веб-сторінка ICANN відображається без використання DNS. Людям здебільшого легше запам’ятовувати слова, аніж цифри. Якщо ви скажете комусь перейти на www.icann.org, вони, ймовірно, пам’ятатимуть саме цю адресу, а не 192.0.32.7, яка, мабуть, важча для сприйняття. Комп’ютери оперують числами. DNS − це процес перекладу слів у числа. Окрім цього, має місце ще одне перетворення інформації. Люди сприймають десяткові числа. Комп’ютери обробляють дані у двійковому форматі. Десяткова IP-адреса 192.0.32.7 у двійковому форматі має вигляд 11000000.00000000.00100000.00000111.

Дайте відвовідь на запитання. Що станеться, якщо скопіювати ці двійкові значення і використати їх у браузері?

4) у режимі командного рядка пропінгуйте www.cisco.com (рис. 5.2).

Примітка: Якщо для доменного імені визначено адресу IPv6, скористайтесь командою ping -4 www.cisco.com для перетворення на IPv4, якщо потрібно.

C:\> ping www.cisco.com

```
C:\> ping www.cisco.com

Pinging origin-www.cisco.com [2600:1408:7:1:9300::90] with 32 bytes of data:
Reply from 2600:1408:7:1:9300::90: time=70ms
Reply from 2600:1408:7:1:9300::90: time=74ms
Reply from 2600:1408:7:1:9300::90: time=72ms
Reply from 2600:1408:7:1:9300::90: time=71ms

Ping statistics for 2600:1408:7:1:9300::90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 74ms, Average = 71ms
C:\> ping -4 www.cisco.com

Pinging e2867.dsca.akamaiedge.net [172.230.155.162] with 32 bytes of data:
Reply from 172.230.155.162: bytes=32 time=7ms TTL=54
Reply from 172.230.155.162: bytes=32 time=6ms TTL=54
Reply from 172.230.155.162: bytes=32 time=7ms TTL=54
Reply from 172.230.155.162: bytes=32 time=6ms TTL=54

Ping statistics for 172.230.155.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Рисунок 5.2 – Перевірка з’єднання з www.cisco.com

Дайте відповідь на запитання. 1. При використанні команди ping www.cisco.com чи отримали ви таку ж IP-адресу, що й у прикладі? Поясніть. 2. У адресному рядку браузера введіть IP-адресу, яку ви отримали при пінгуванні www.cisco.com. Чи відображається веб-сайт? Поясніть.

5) дослідження DNS-пошуку адреси веб-сайту за допомогою команди nslookup (рис. 5.3):

– у командному рядку введіть команду nslookup. Ваш результат може відрізнятися від наведеного у прикладі.

```
C:\> nslookup
Default Server: one.one.one.one
Address: 1.1.1.1
```

Рисунок 5.3 – Результат виконання команди nslookup

Дайте відповідь на запитання. Який DNS-сервер використовується за замовчуванням?

6) зверніть увагу на зміну позначки командного рядка на більше (>). Це ознака команди nslookup. З появою цієї позначки можна вводити команди, пов’язані з DNS. У полі курсора введіть ? для перегляду списку всіх команд, доступних для використання у режимі nslookup .

Введіть www.cisco.com (рис. 5.4).

```
> www.cisco.com
Default Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2600:1404:a:395::b33
          2600:1404:a:38e:b33
          172.230.155.162
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgikey.net
          wwwds.cisco.com.edgakey.net.globalredir.akadns.net
```

Рисунок 5.4 – Результат виконання команди www.cisco.com

Дайте відповідь на запитання. Яка адреса IPv4 відповідає уведеному доменному імені? (Для визначеного розташування, 172.230.155.162).

Примітка. IP-адреса, що відповідає вашому розташуванню, найімовірніше, буде відрізнятися, оскільки Cisco використовує дзеркальні сервери у різних локаціях по всьому світу.

Дайте відповідь на запитання. Чи збігається вона з IP-адресою, виявленою за допомогою команди ping?

Окрім IP-адреси 172.230.155.162, відображаються такі числа: 2600:1404:a:395::b33 і 2600:1404:a:38e::b33. Що вони позначають?

7) У режимі nslookup введіть IP-адресу веб-сервера Cisco, яку ви щойно виявили. За допомогою nslookup можна отримати доменне ім’я, якщо URL-адреса вам невідома.

```
> 172.230.155.162
Default Server: one.one.one.one
Address: 1.1.1.1

Name: a172-230-155-162.deploy.static.akamaitechnologies.com
Address: 172.230.155.162
```

Інструмент nslookup можна використовувати для перетворення доменних імен на IP-адреси. Також він дозволяє виконувати зворотні перетворення IP-адрес на доменні імена.

Дайте відповідь на питання. Використовуючи інструмент nslookup, запишіть IP-адреси, пов'язані з www.google.com.

6) дослідження DNS-пошуку поштових серверів за допомогою команди nslookup:

– у режимі nslookup введіть set type=mx, щоб використати nslookup для визначення поштових серверів:

> set type=mx

– у режимі nslookup введіть cisco.com (рис. 5.5):

```
> cisco.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
cisco.com MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
cisco.com MX preference = 30, mail exchanger = aer-mx-01.cisco.com
cisco.com MX preference = 10, mail exchanger = alln-mx-01.cisco.com
```

Рисунок 5.5 – Результат виконання команди www.cisco.com

Резервування (налаштування більше одного поштового сервера) є одним з основоположних принципів побудови мережі. За його впровадження, у разі відмови одного з поштових серверів, комп'ютер намагається звернутися із запитом до іншого поштового сервера. Адміністратори електронної пошти використовують параметр MX preference аби визначити, до якого поштового сервера слід звертатися у першу чергу. Насамперед звертаються до поштового сервера з найнижчим показником MX preference.

Дайте відповідь на запитання. Беручи до уваги отримані вище дані, до якого поштового сервера спершу йтиме звернення при надсиланні листа до cisco.com?

– у режимі nslookup введіть, щоб повернутися до звичайного режиму командного рядка ПК;

– введіть ipconfig /all.

Дайте відповідь на питання. Запишіть IP-адреси усіх DNS-серверів, які використовує ваш навчальний заклад. Яке основне призначення DNS?

Оформіть звіт до роботи.

Лабораторна робота №6
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. 6.1).

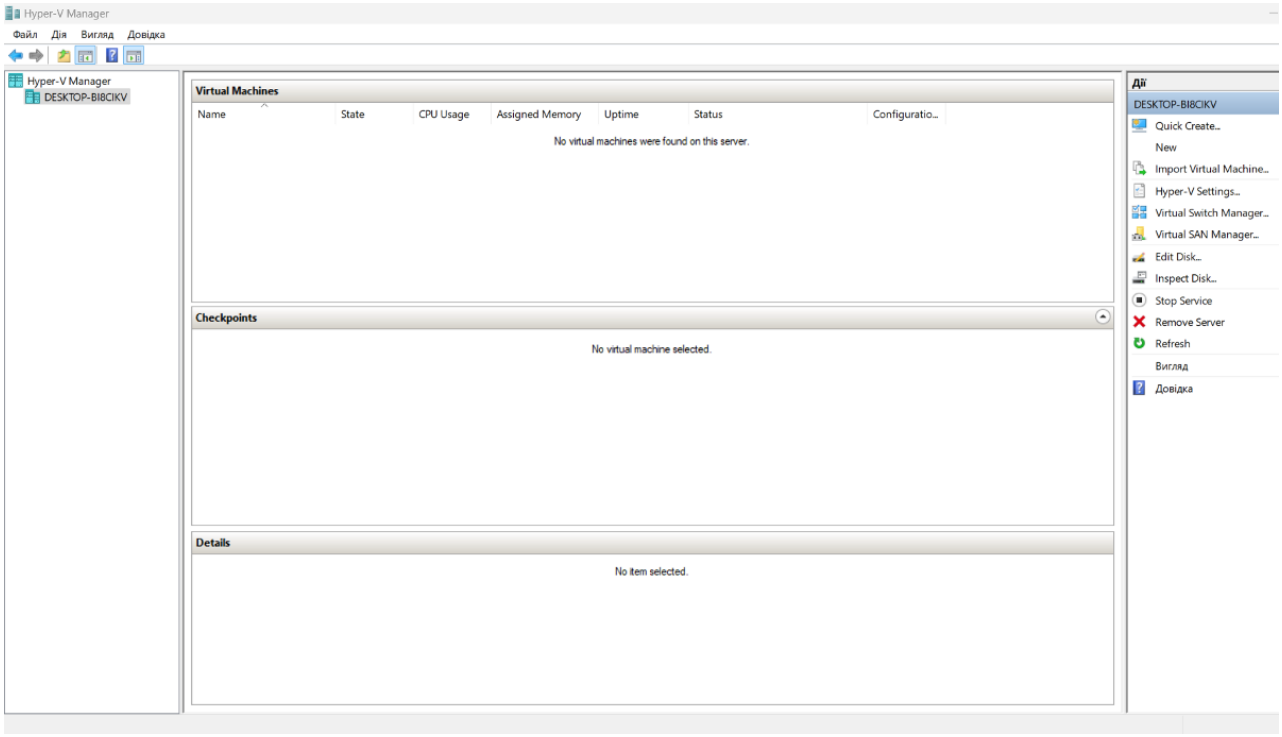

Рисунок 6.1 – Вікно Hyper-V

Після цього натиснути на назву комп’ютера – «New» – «Virtual Machine» (рис. 6.2).

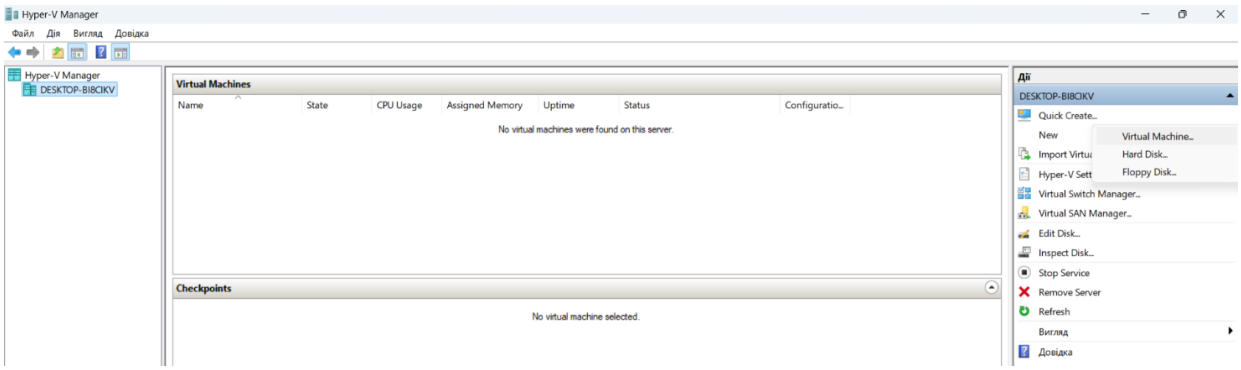

Рисунок 6.2 – Створення нової віртуальної машини для ВС25

Внаслідок цих дій відкривається майстер створення нової віртуальної машини. В першій вкладці (вступній) натискаємо «Next» (рис. 6.3).

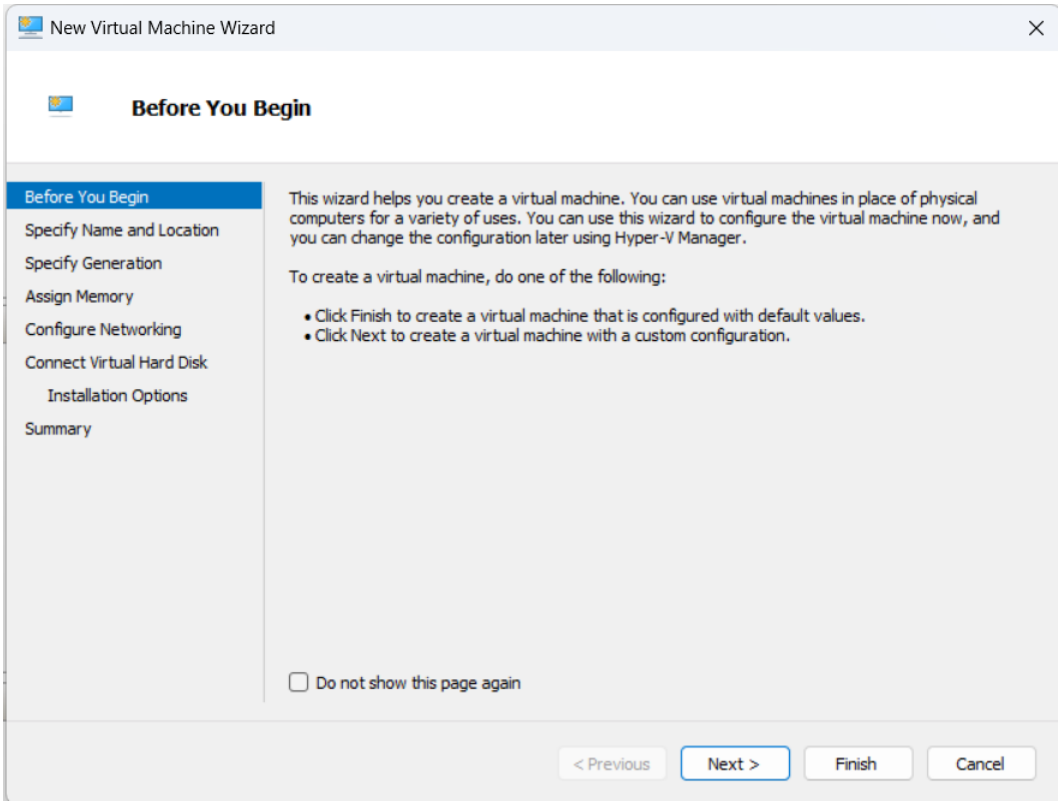

Рисунок 6.3 – Вітальне вікно майстра створення нової віртуальної машини

В наступній вкладці надати ім’я новій віртуальній машині та обирати місце зберігання для її файлів (рис. 6.4).

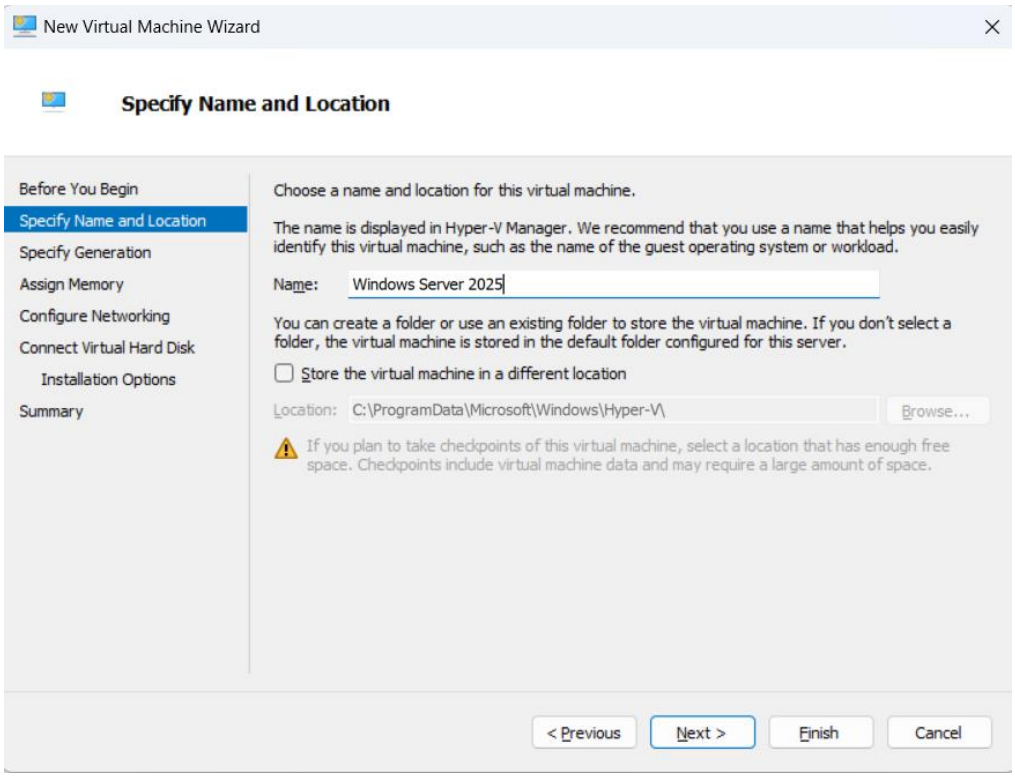

Рисунок 6.4 – Надання імені новій ВМ та вибір місця для зберігання її файлів

Далі обирається специфікація покоління ВМ – «Generation 2» і знову тиснути «Next» (рис. 6.5).

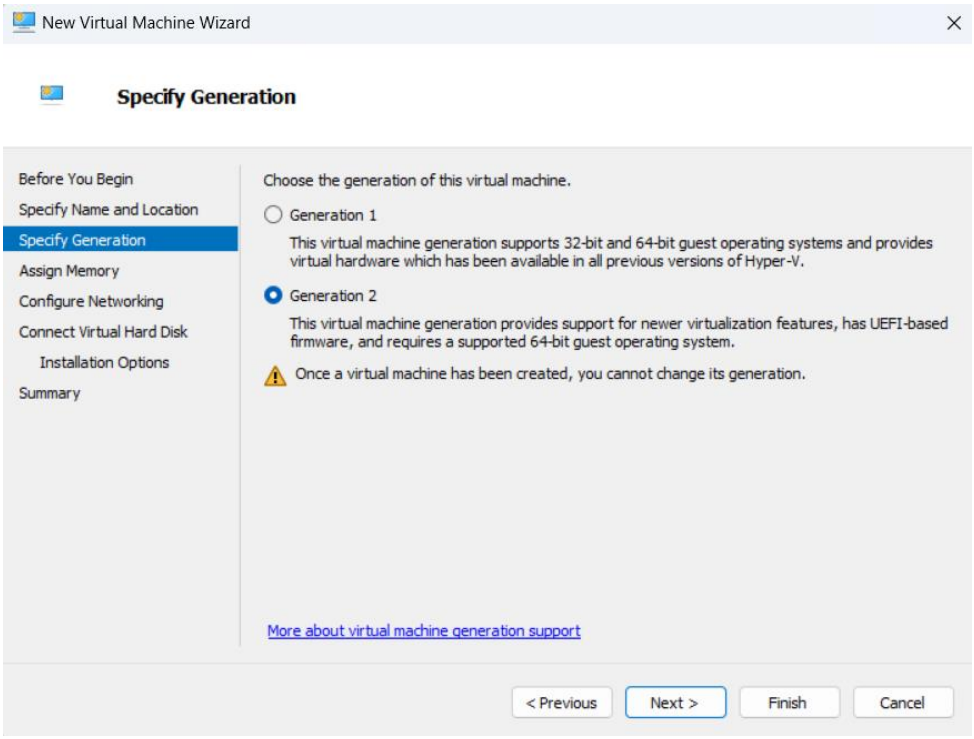

Рисунок 6.5 – Вибір «покоління» для ВМ, що створюється

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. 6.6).

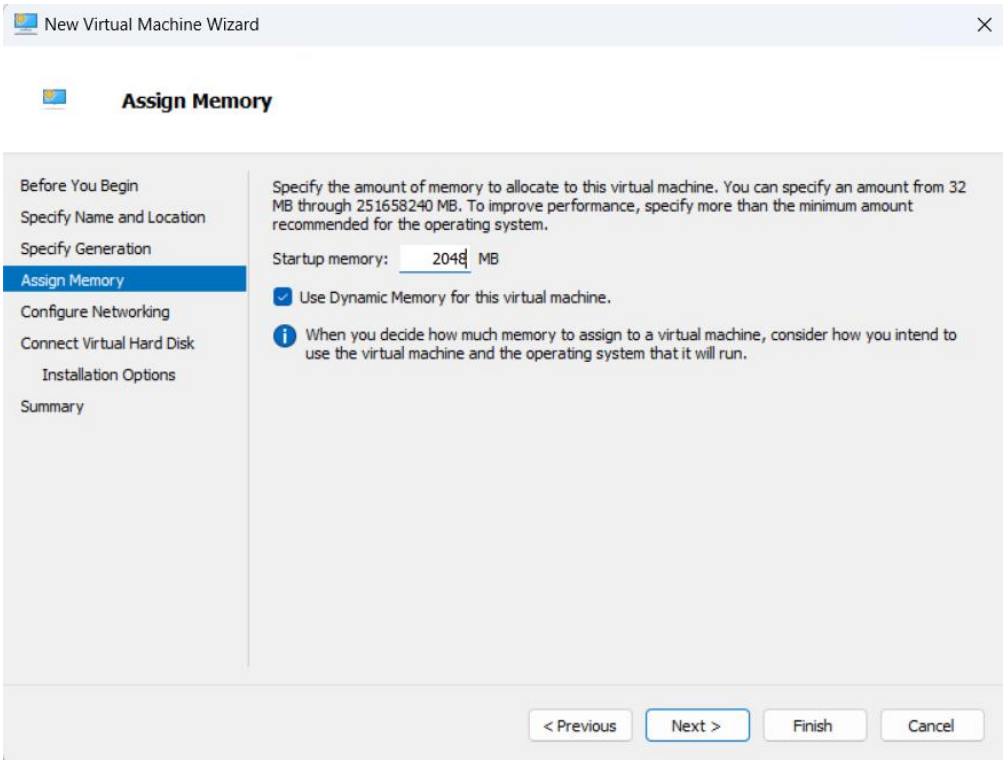

Рисунок 6.6 – Вибір розміру оперативної пам’яті для нової ВМ (вказано мінімальний потрібний об’єм)

Потім провести мережеві налаштування та в полі «Connection» обирати «Default Switch» і знову натиснути «Next» (рис. 6.7).

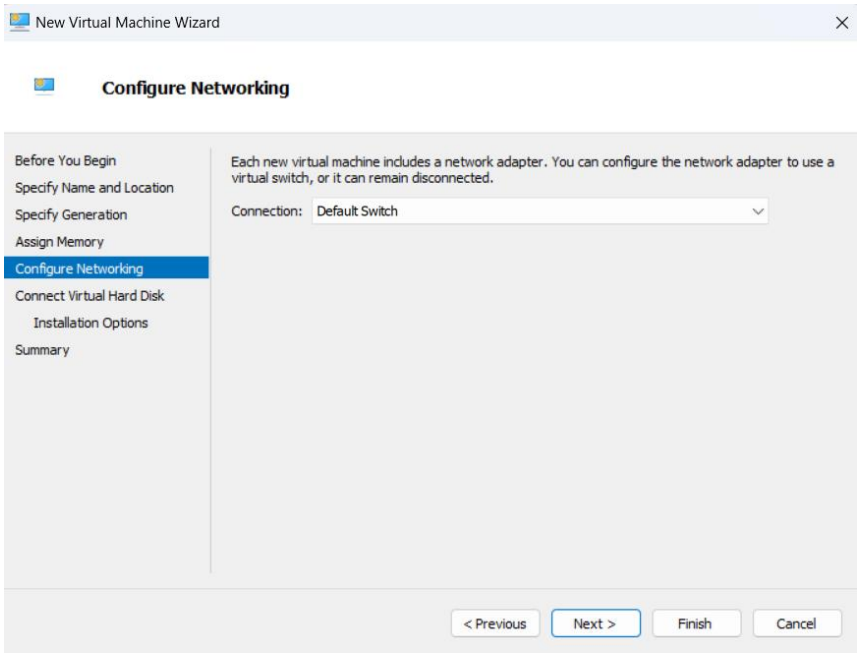

Рисунок 6.7 – Мережеві налаштування

Далі створити віртуальний жорсткий диск та вказати місце його зберігання і обсяг та натиснути «Next». Мінімальний обсяг – 30 ГБ (рис. 6.8).

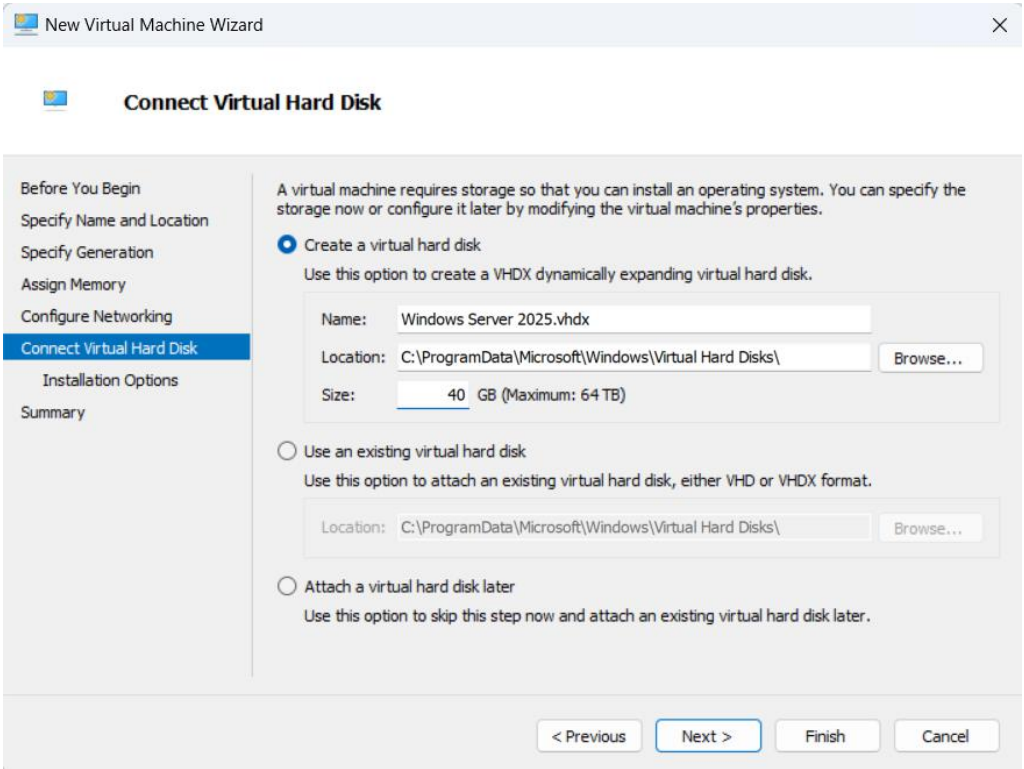

Рисунок 6.8 – Створення віртуального жорсткого диска для ВМ та місця його зберігання на фізичному комп’ютері

Згодом обирати джерело встановлення ОС – завантажений попередньо ISO образ Windows Server 2025 та натиснути «Next» (рис. 6.9).

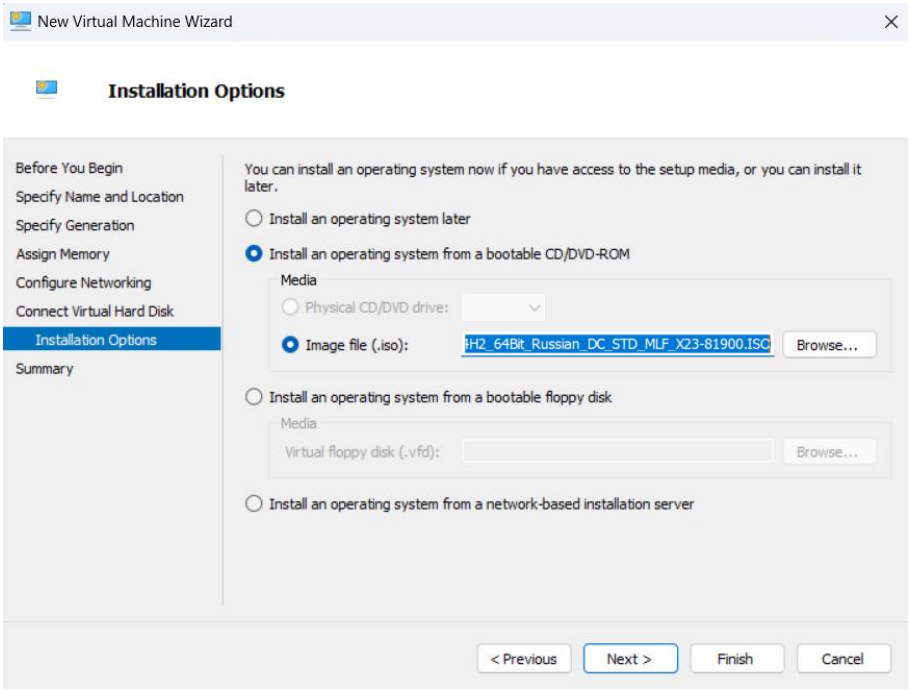

Рисунок 6.9 – Налаштування встановлення ОС – вибір джерела встановлення (ISO образ)

В останній вкладці перевірити проведені налаштування та натиснути «Finish» (рис. 6.10).

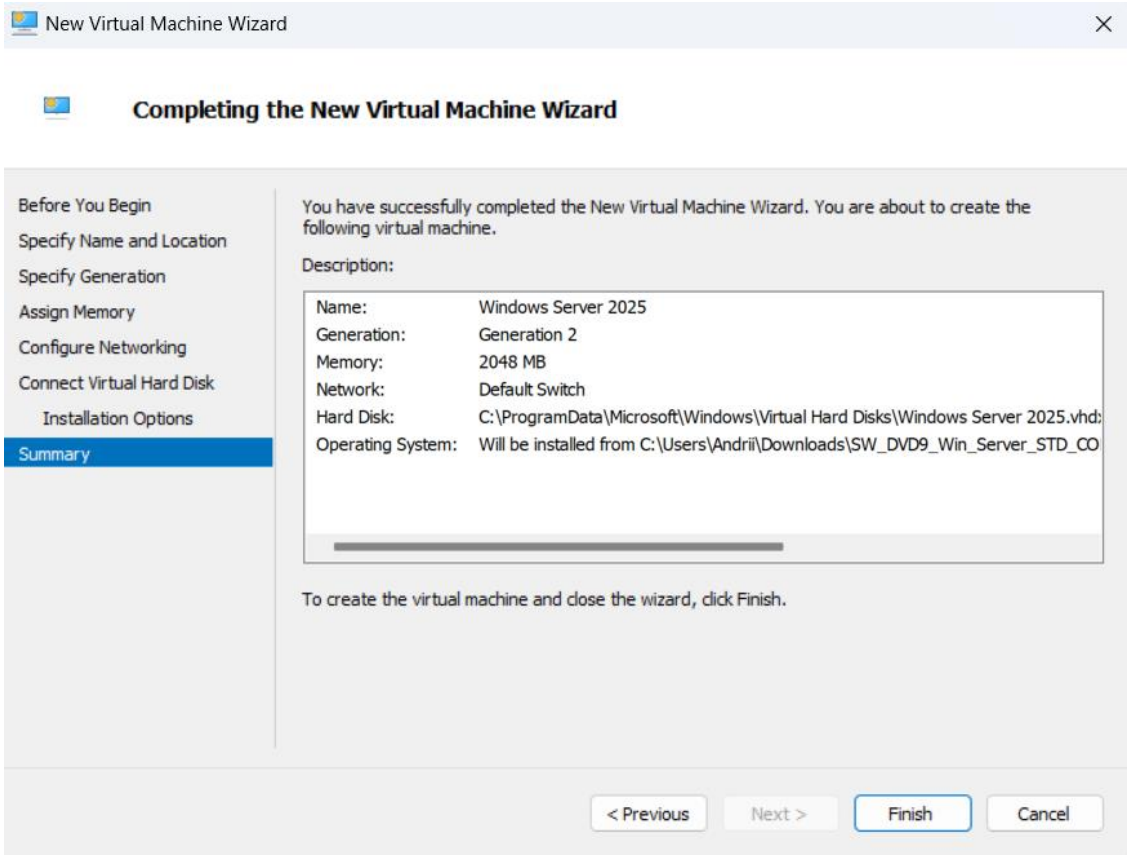

Рисунок 6.10 – Підсумки проведених налаштувань створюваної віртуальної машини

В результаті нова віртуальна машина для розгортання на ній Windows Server 2025 створена та відображається в Hyper-V Manager (рис. 6.11).

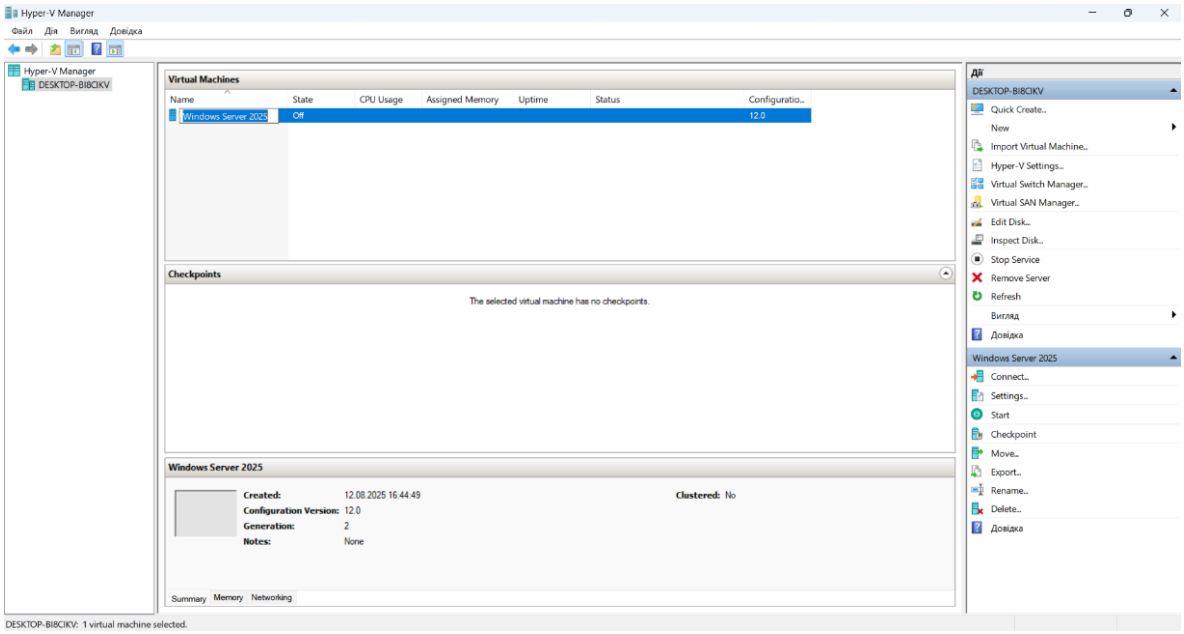

Рисунок 6.11 – Створена віртуальна машина для Windows Server 2025

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. 6.12-6.13).

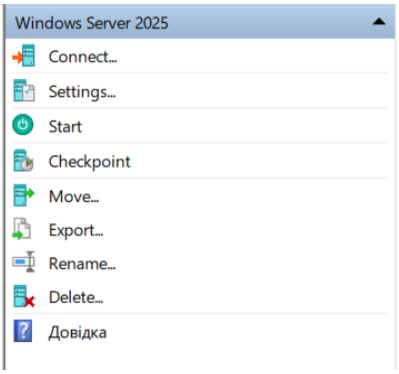

Рисунок 6.12 – Меню роботи зі створеною ВМ у середовищі Hyper-V

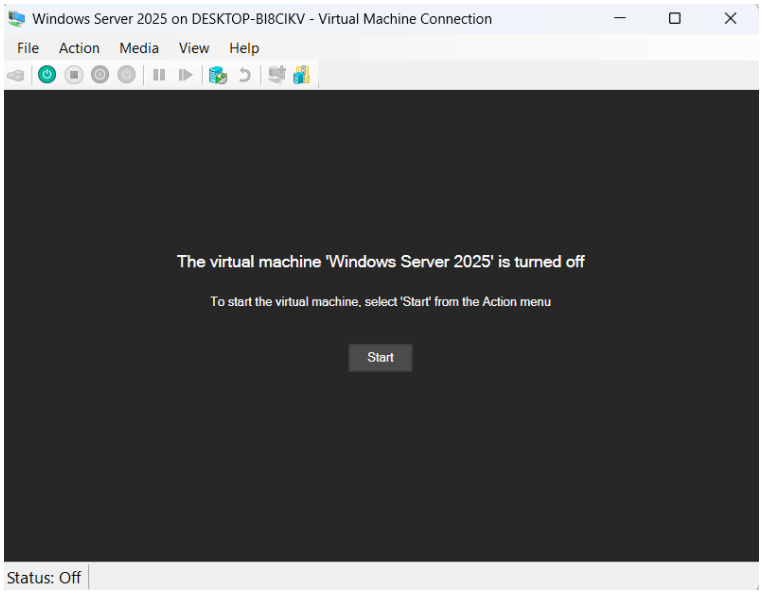

Рисунок 6.13 – Запуск ВМ

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. 6.14).

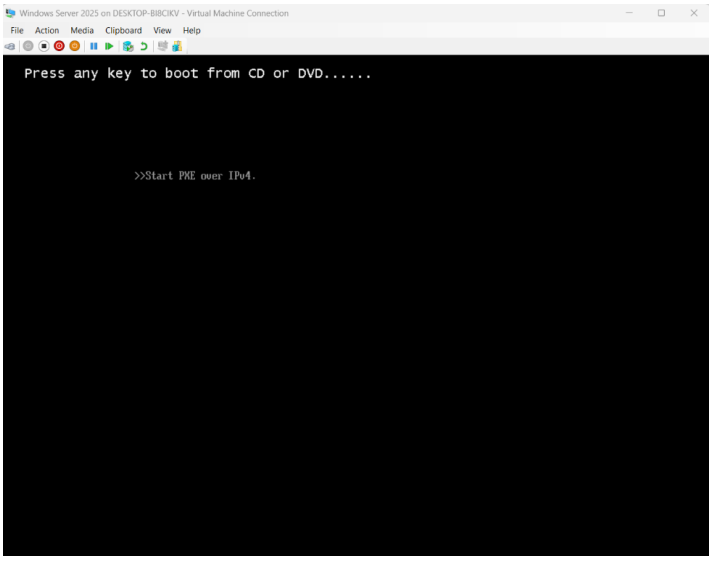

Рисунок 6.14 – Вікно підтвердження вивантаження образу ОС на ВМ

Після цього автоматично починається процес встановлення операційної системи на віртуальний комп'ютер. На першій вкладці налаштування встановлення вибрати мовні параметри та натиснути «Далі» (рис. 6.15).

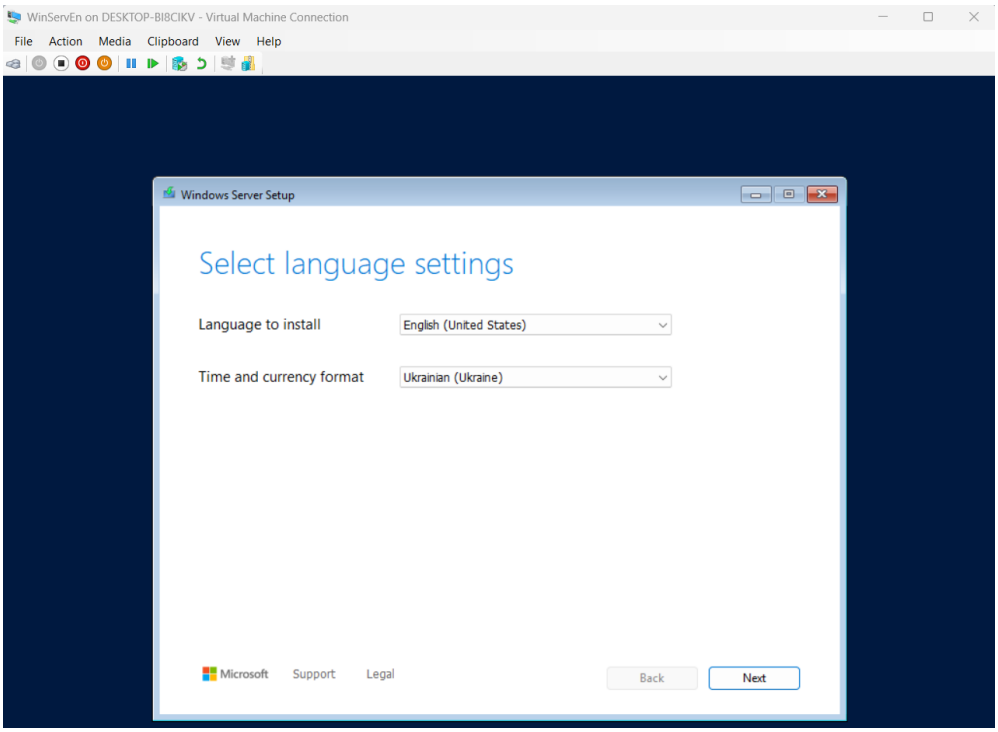

Рисунок 6.15 – Вибір мовних параметрів для встановлюваної ОС

Згодом налаштувати параметри клавіатури, вони автоматично виставляються, відповідно до обраних мовних параметрів, потім натиснути «Далі» (рис. 6.16).

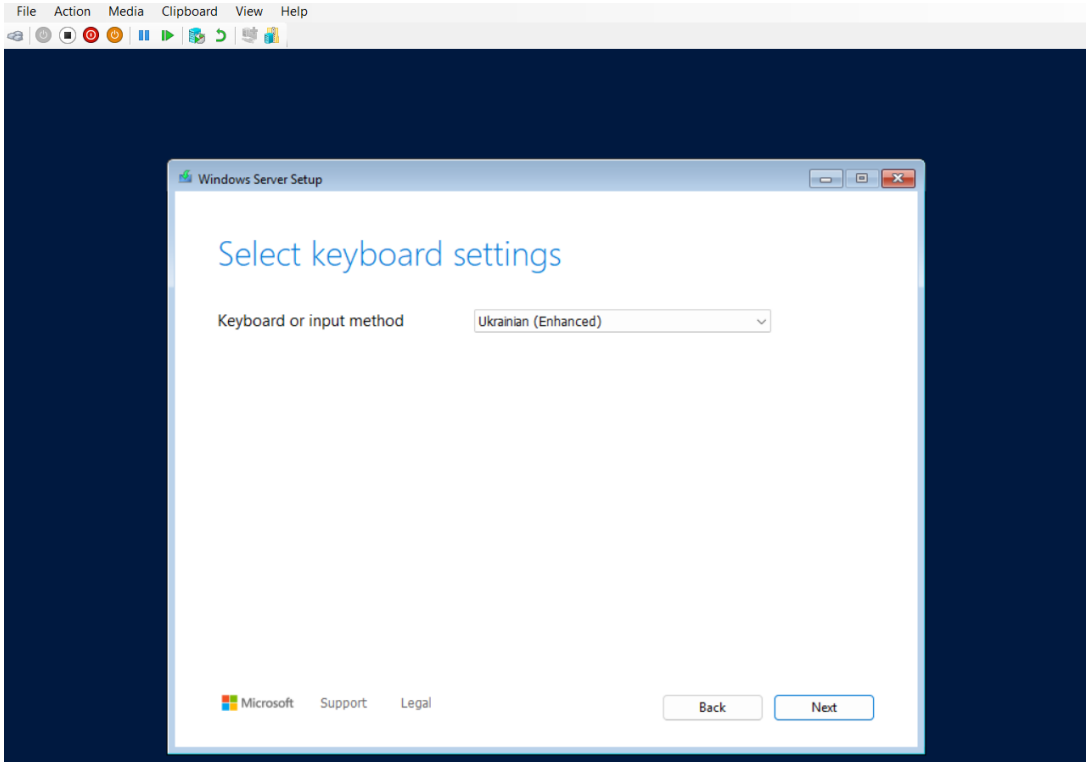

Рисунок 6.16 – Вибір параметрів клавіатури

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. 6.17).

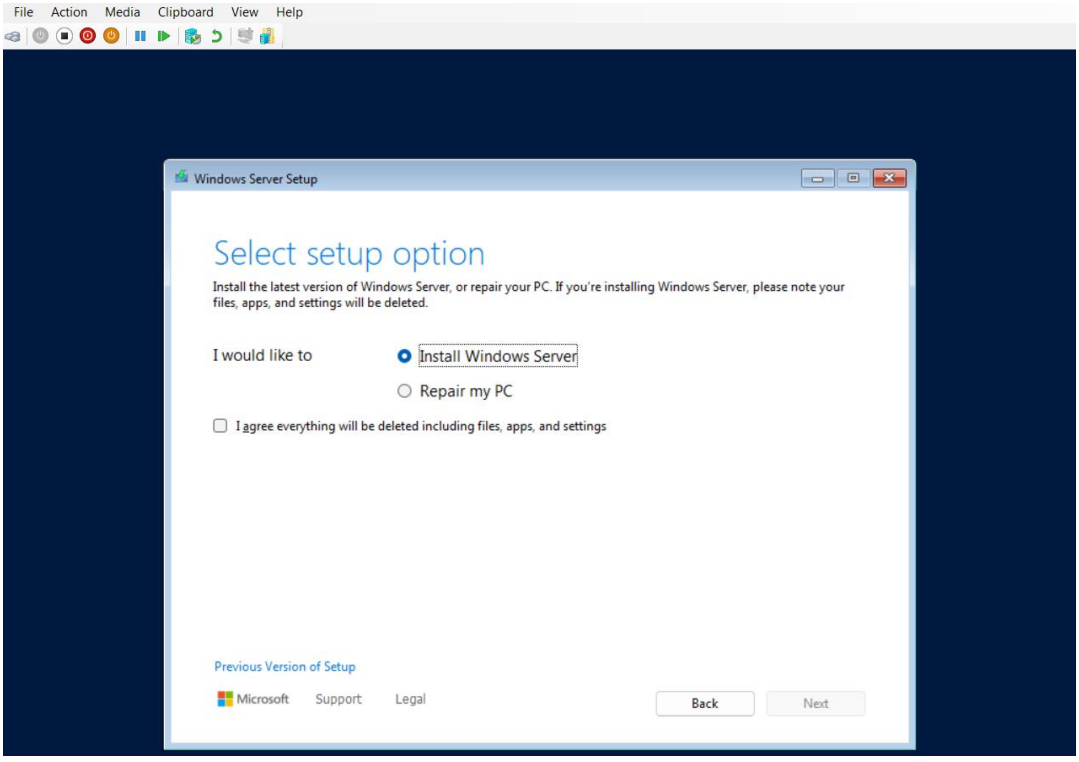

Рисунок 6.17 – Вибір варіанту встановлення Windows Server 2025

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. 6.18).

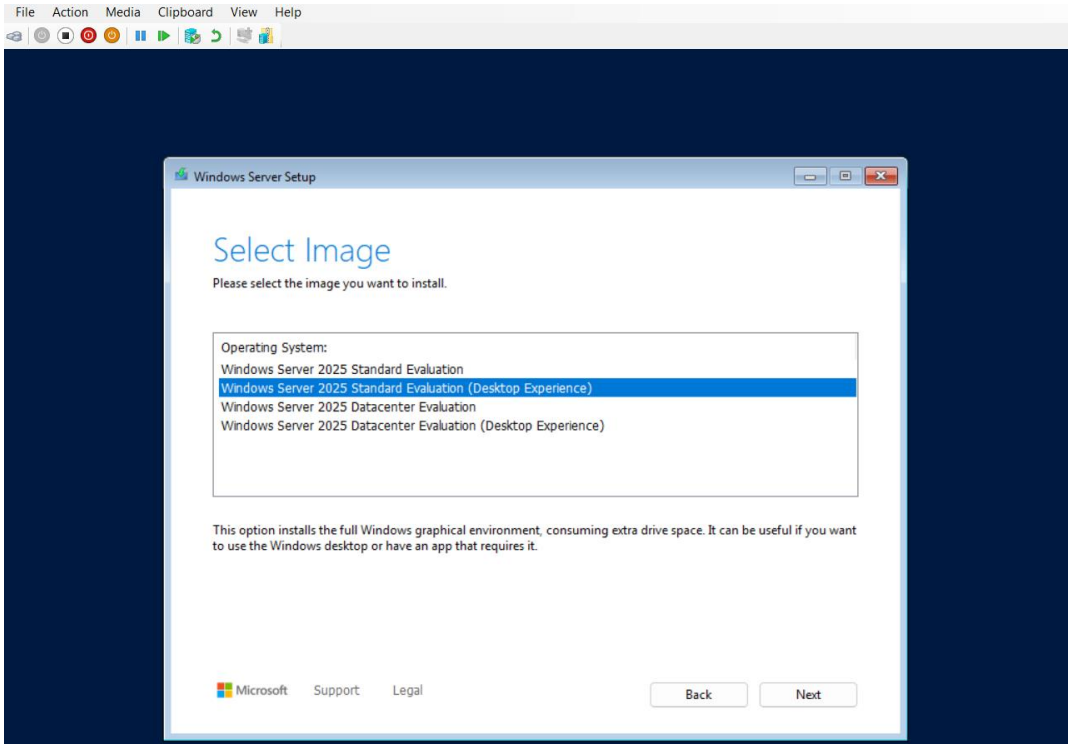

Рисунок 6.18 – Вибір типу ОС Windows Server 2025, який потрібно встановити

Після цього прийняти умови ліцензії та натиснути «Далі» (рис. 6.19).

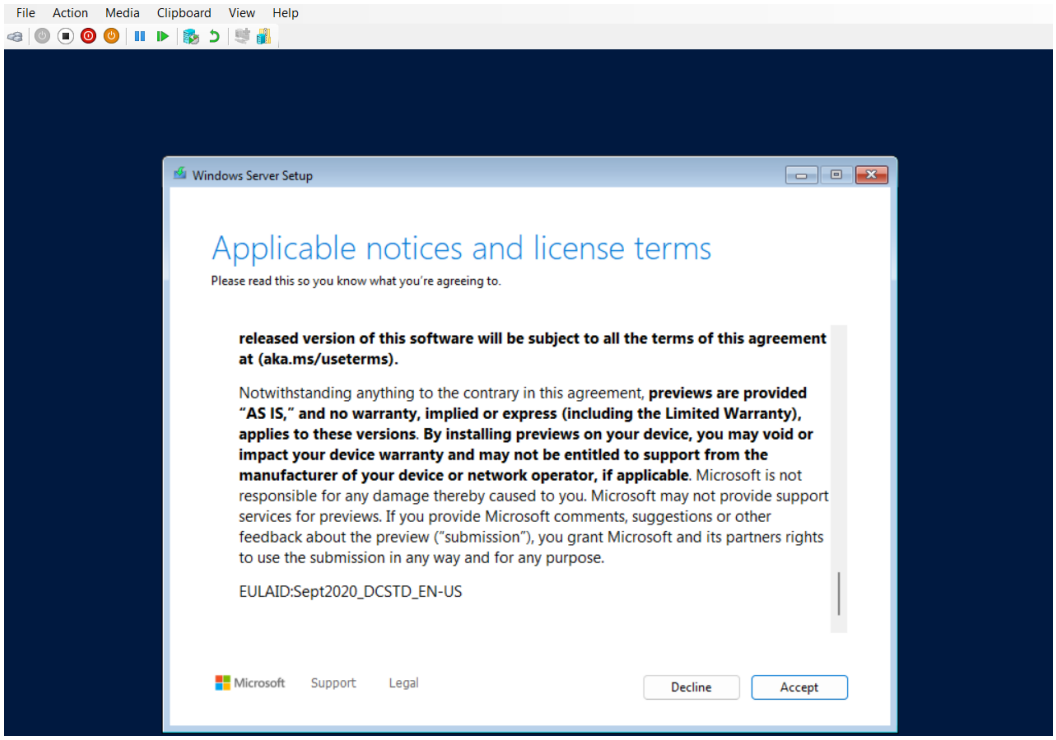

Рисунок 6.19 – Прийняття умов ліцензії

Далі вибрати розташування для встановлення ОС та натиснути «Далі» (рис. 6.20).

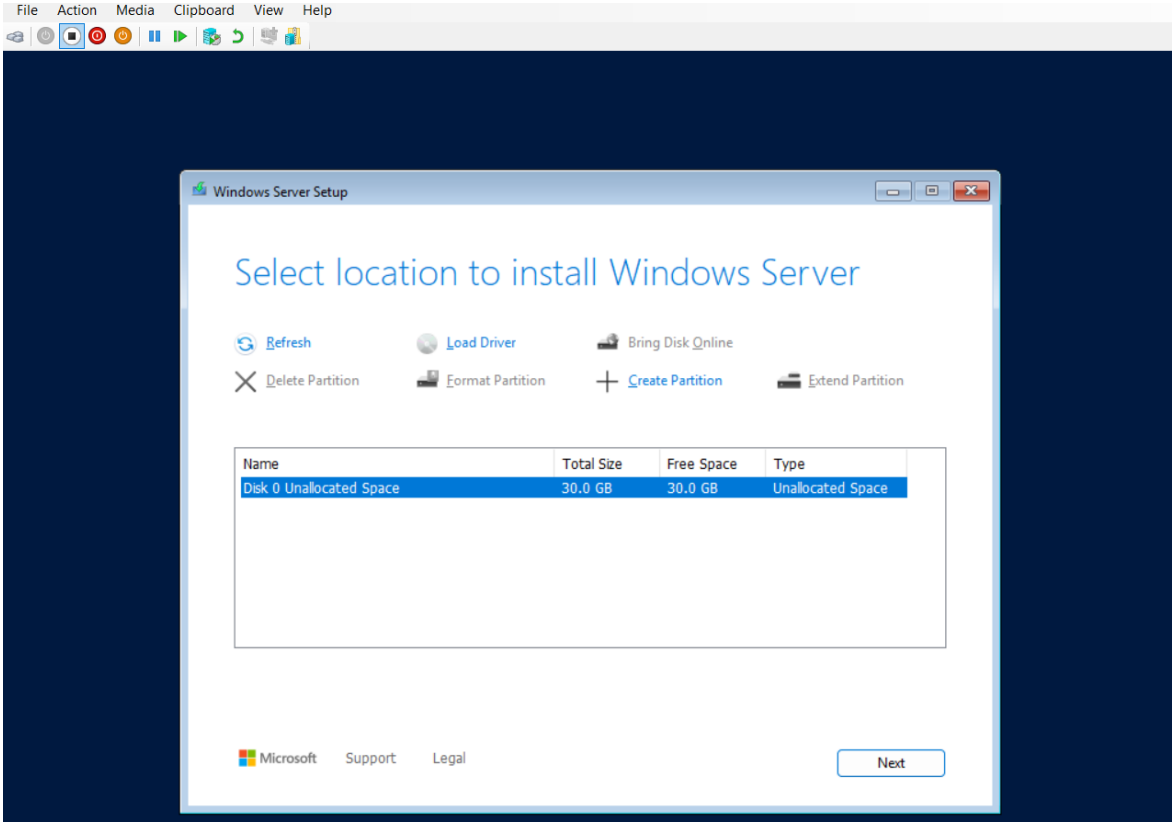

Рисунок 6.20 – Вибір місця (диска) для встановлення ОС

Після цього натиснути «Встановити». Розпочинається процес інсталяції операційної системи на комп’ютер (рис. 6.21-6.22).

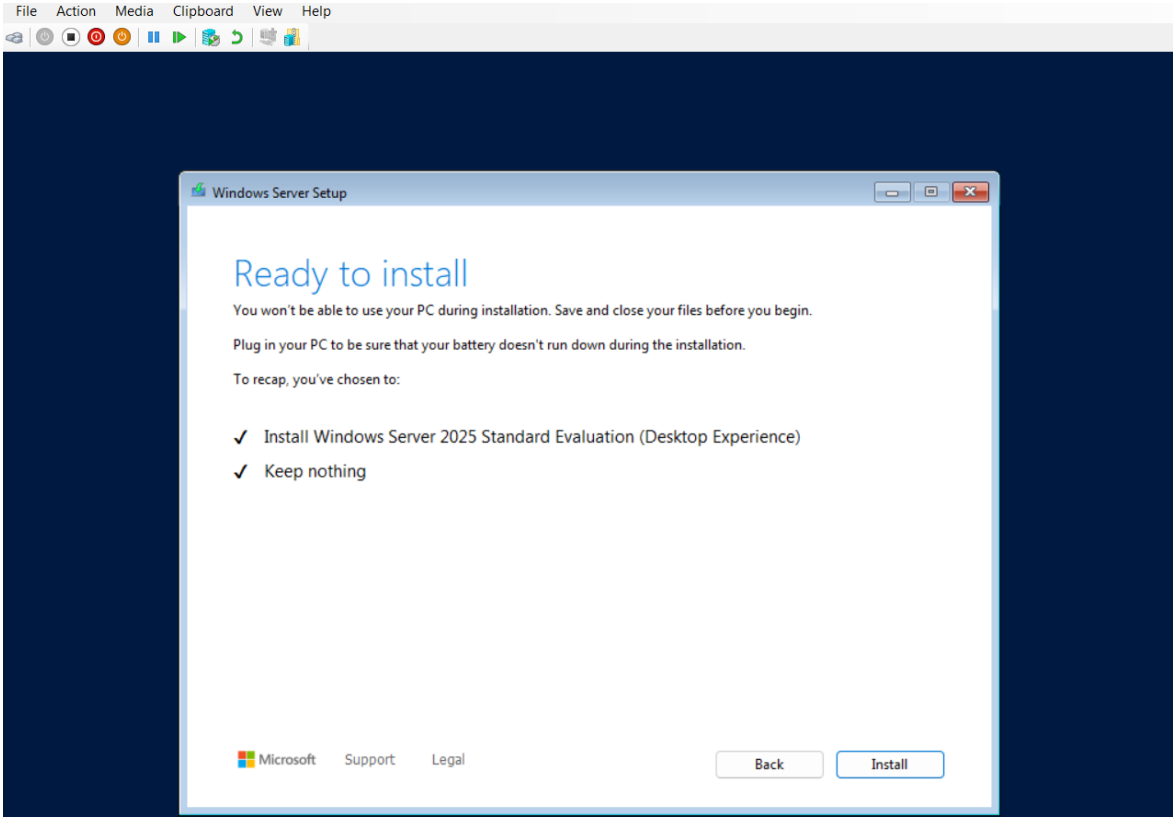

Рисунок 6.21 – Фінальне вікно підтвердження встановлення Windows Server 2025

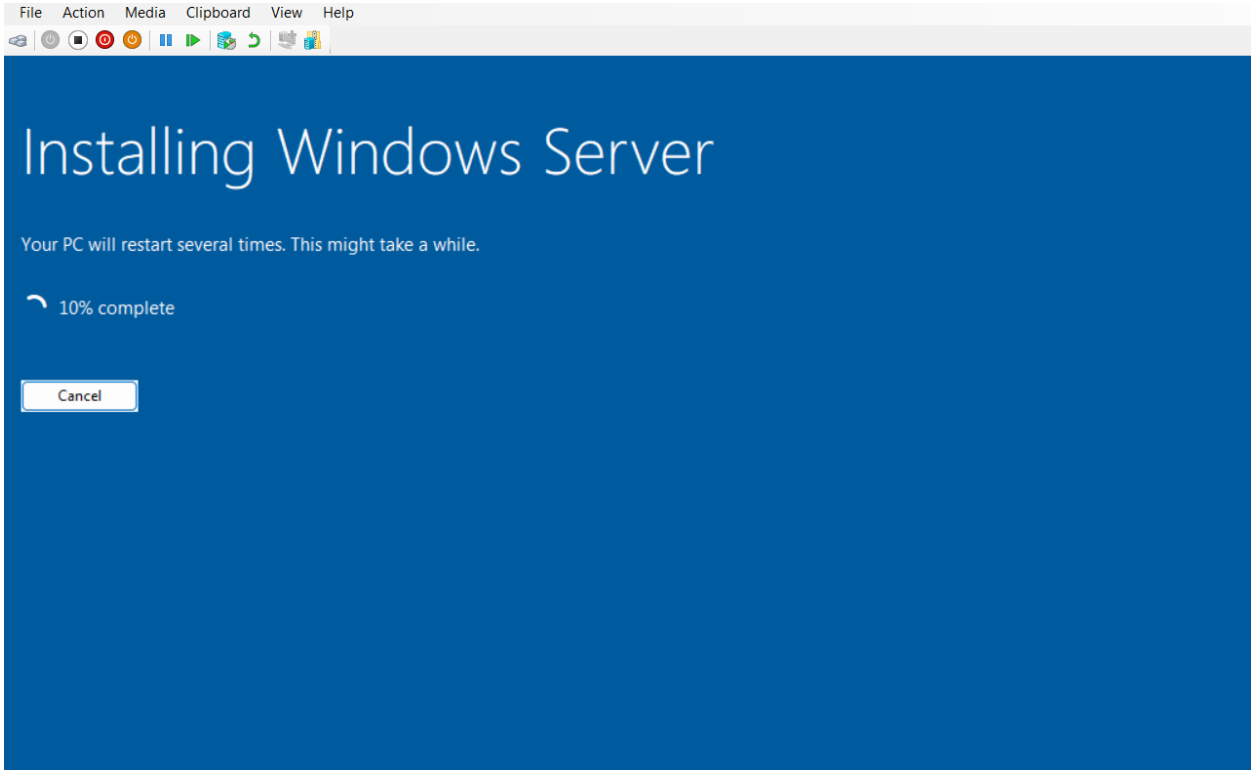

Рисунок 6.22 – Процес встановлення

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. 6.23-6.24).

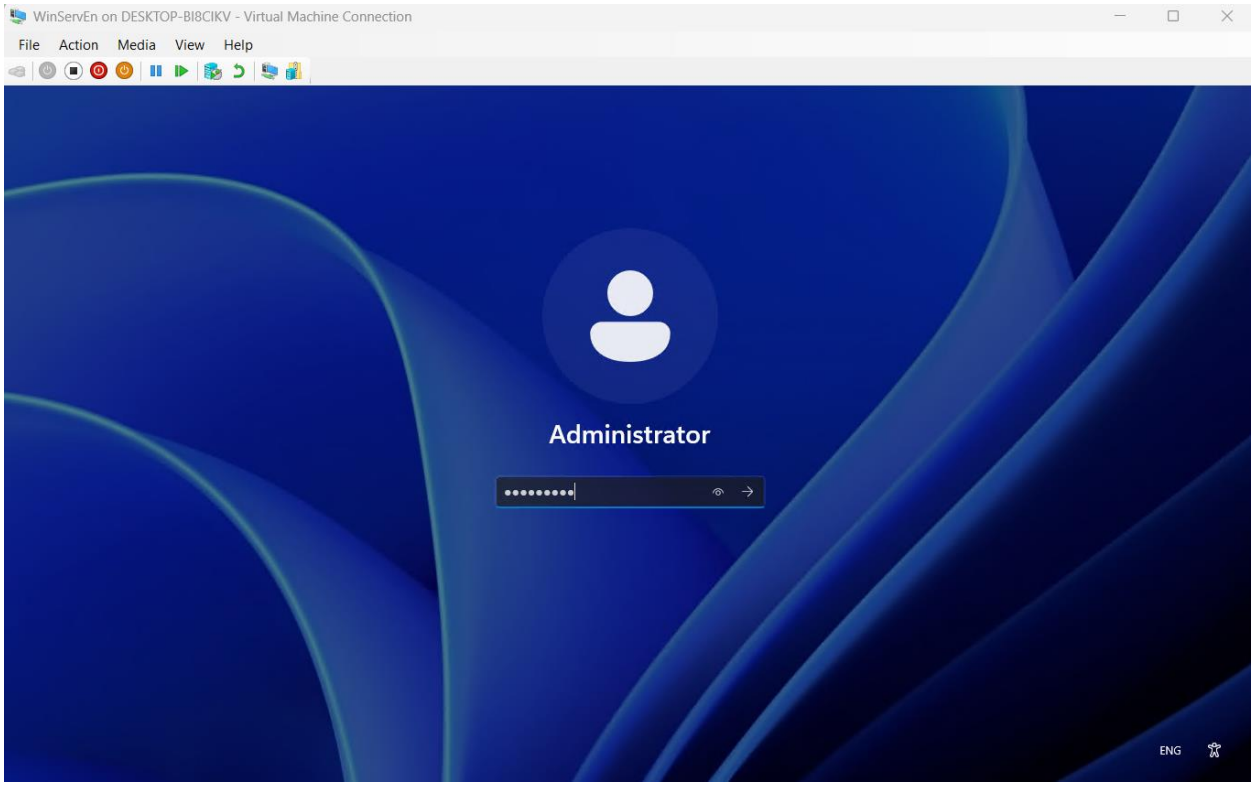

Рисунок 6.23 – Виконання входу в ОС Windows Server 2025

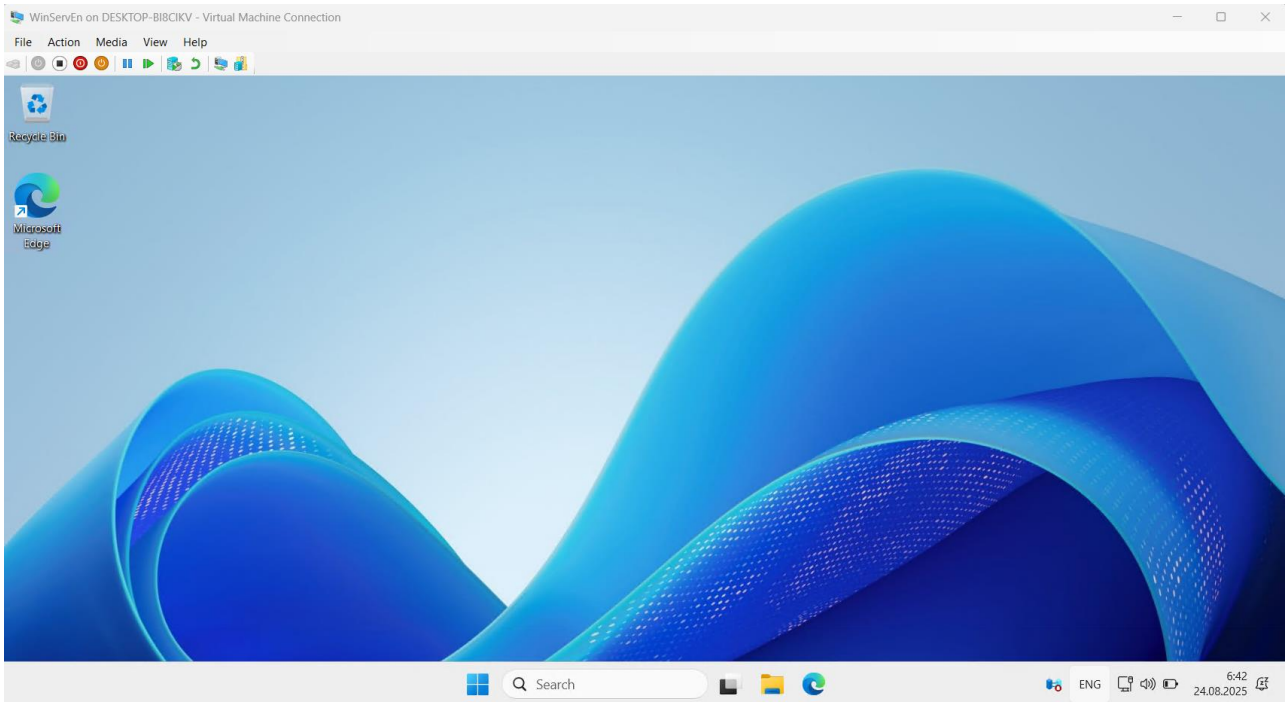

Рисунок 6.24 – Робочий стіл Windows Server 2025 після першого входу в систему

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. 6.25-6.27).

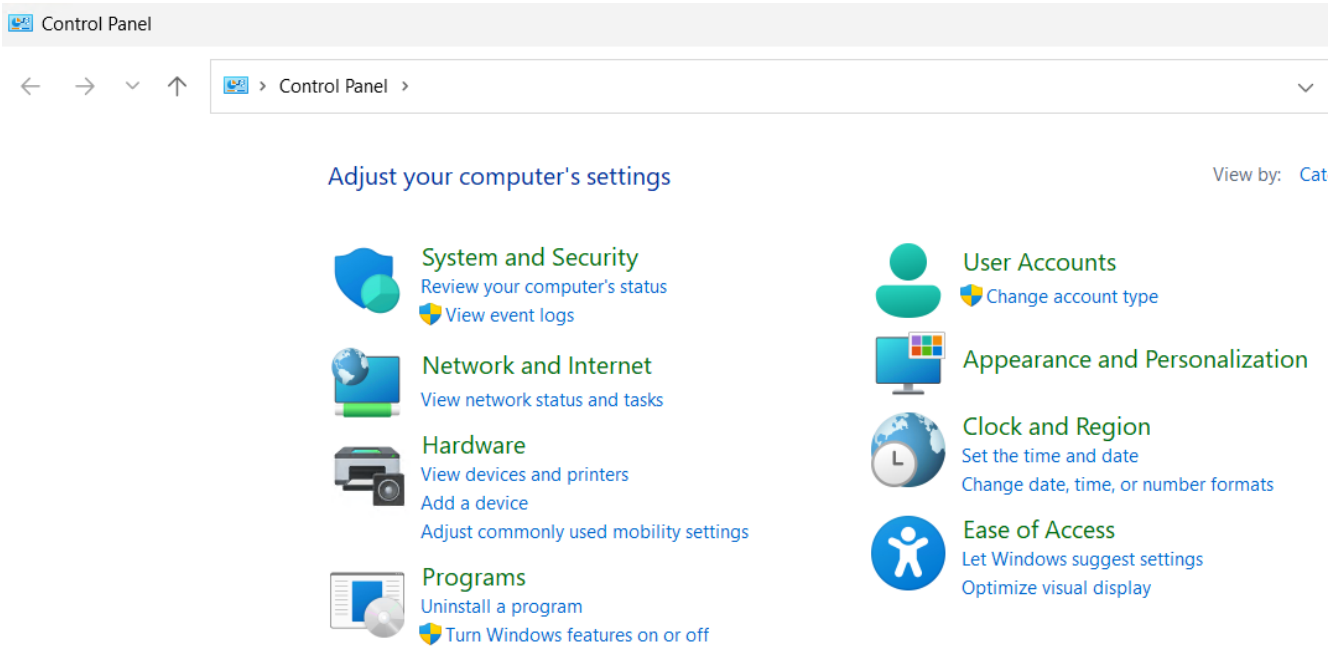

Рисунок 6.25 – Вікно «Панель керування»

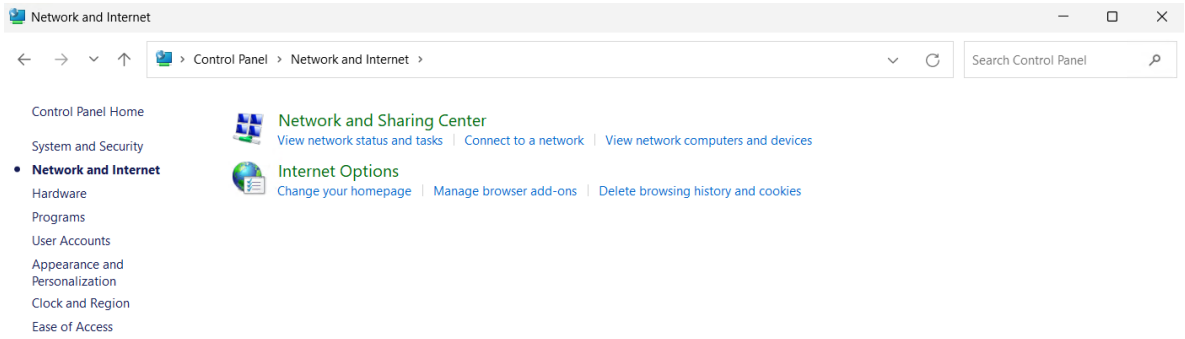

Рисунок 6.26 – Вікно «Мережа та Інтернет»

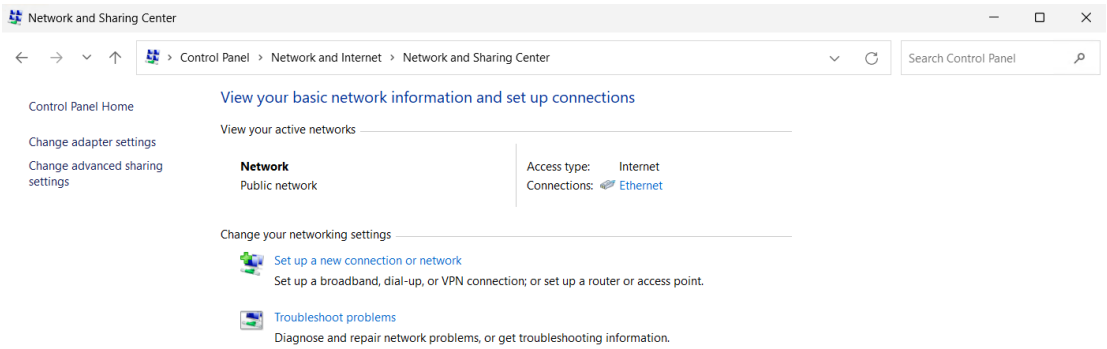

Рисунок 6.27 – Вікно «Центр управління мережами та загальним доступом»

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. 6.28-6.29).

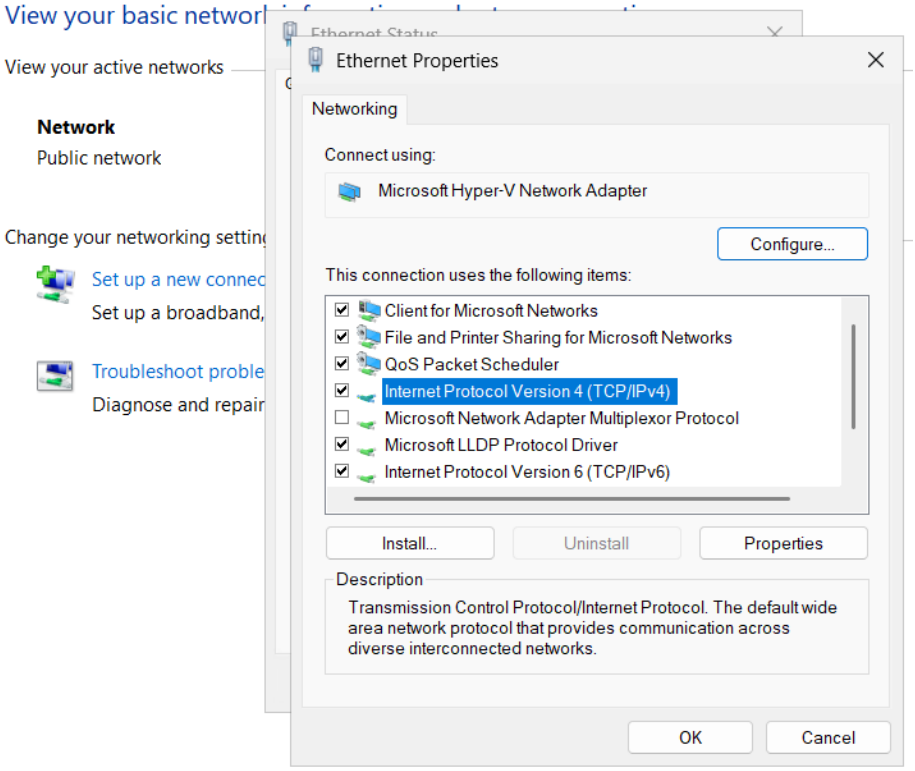

Рисунок 6.28 – Властивості мережевого адаптера

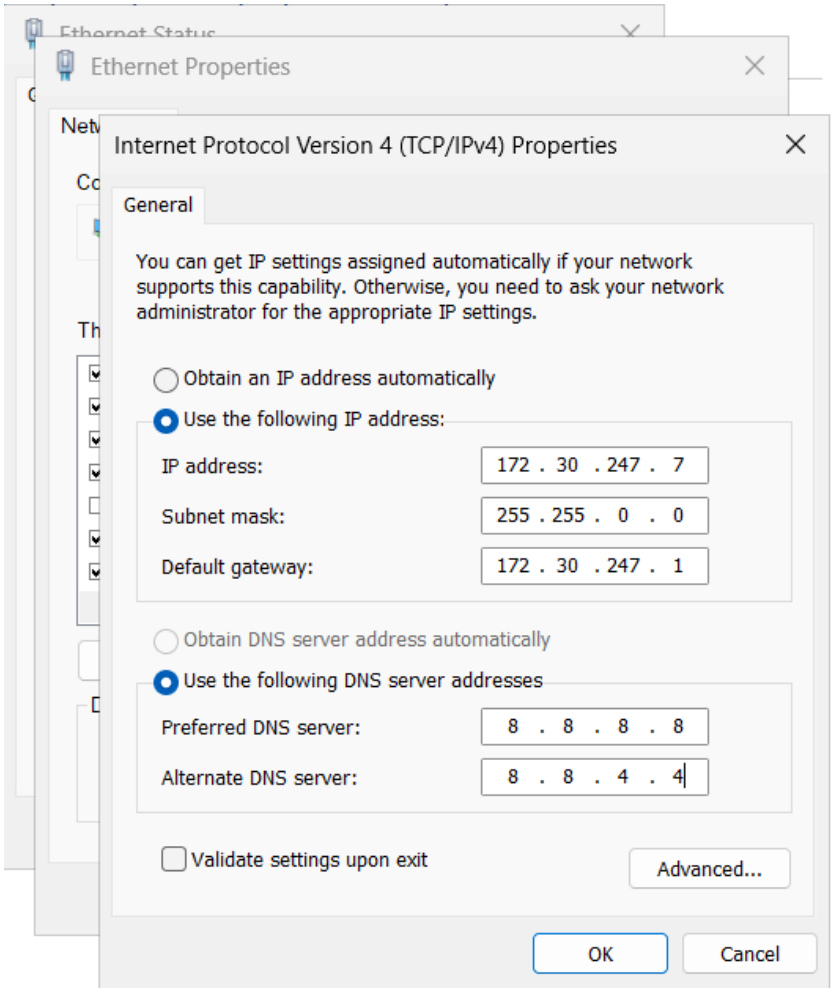

Рисунок 6.29 – Зміна IP-адреси сервера

Після цього виконати перевірку налаштувань IP-параметрів сервера за допомогою команди «ipconfig» в командному рядку (рис. 6.30).

```
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 6.30 – 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. 6.31).

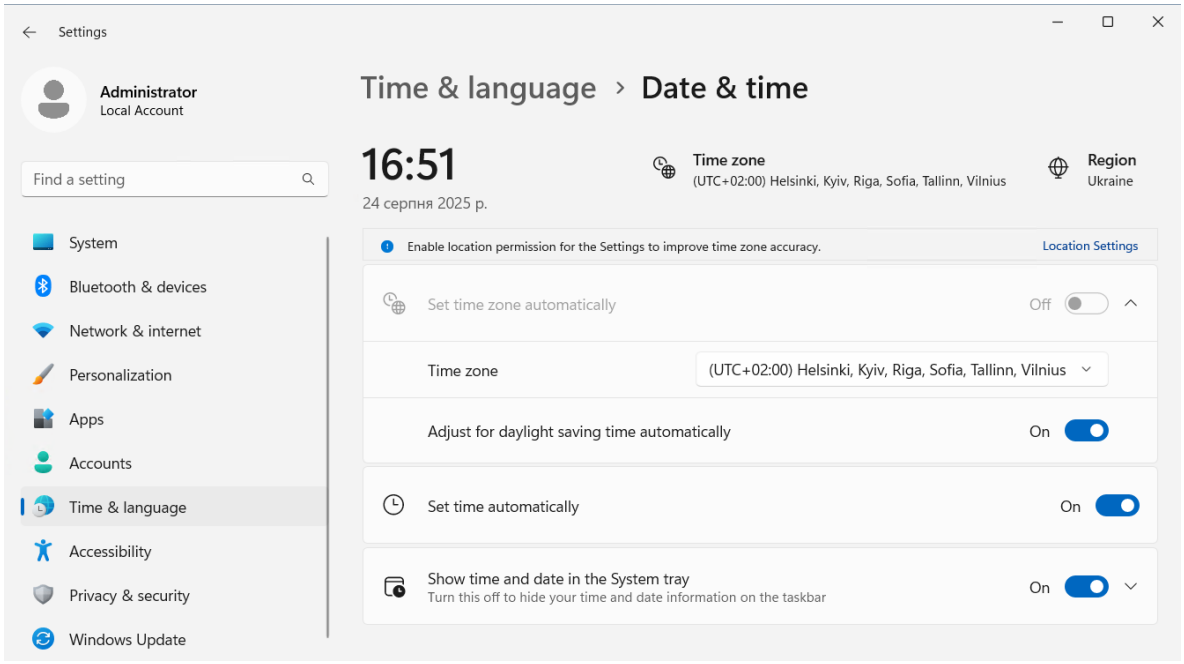

Рисунок 6.31 – Зміна параметрів дати та часу

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. 6.32).

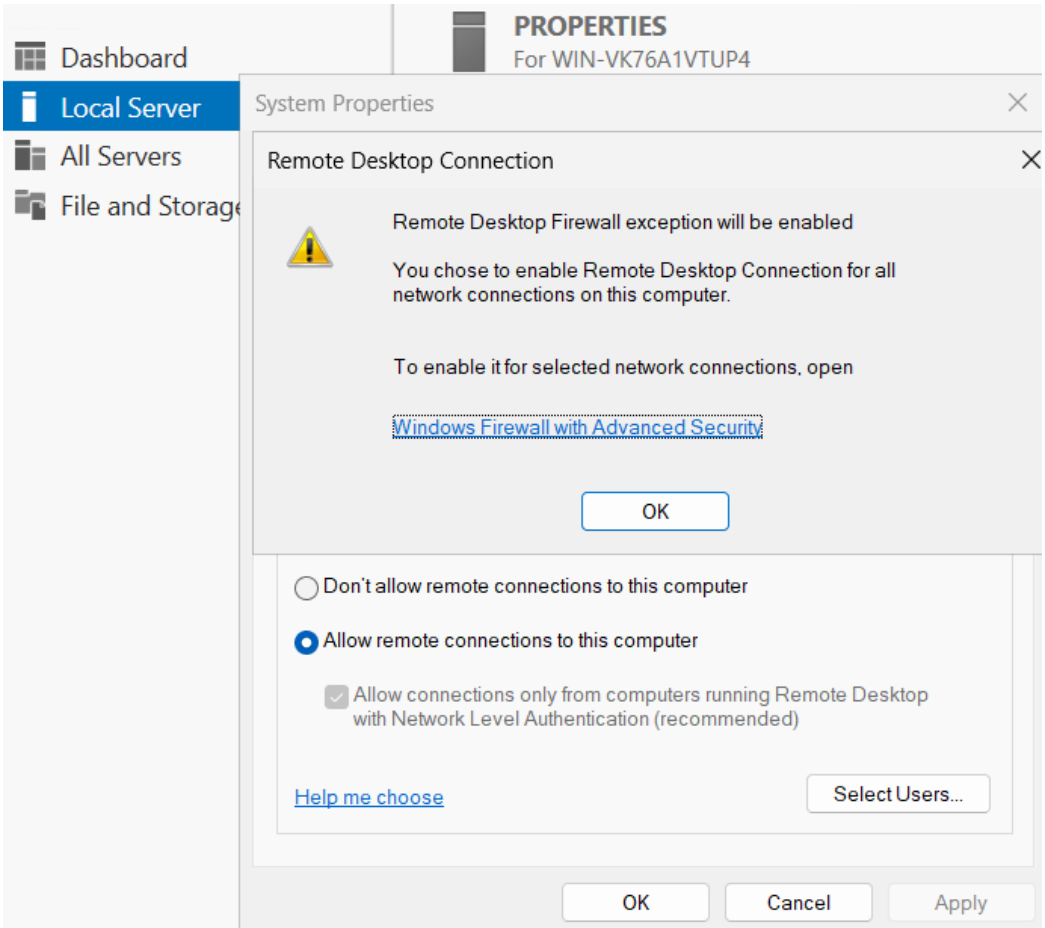

Рисунок 6.32 – Ввімкнення віддаленого доступу до сервера

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. 6.33-6.34).

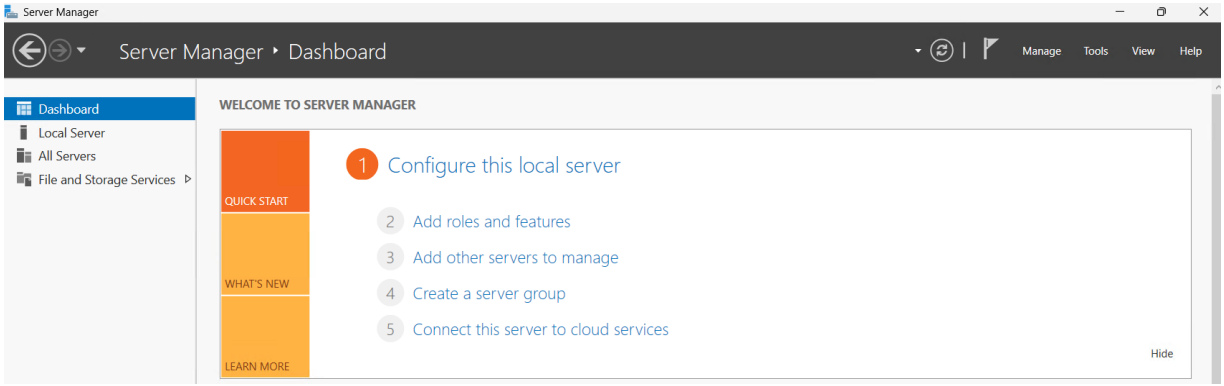

Рисунок 6.33 – Меню налаштування локального сервера

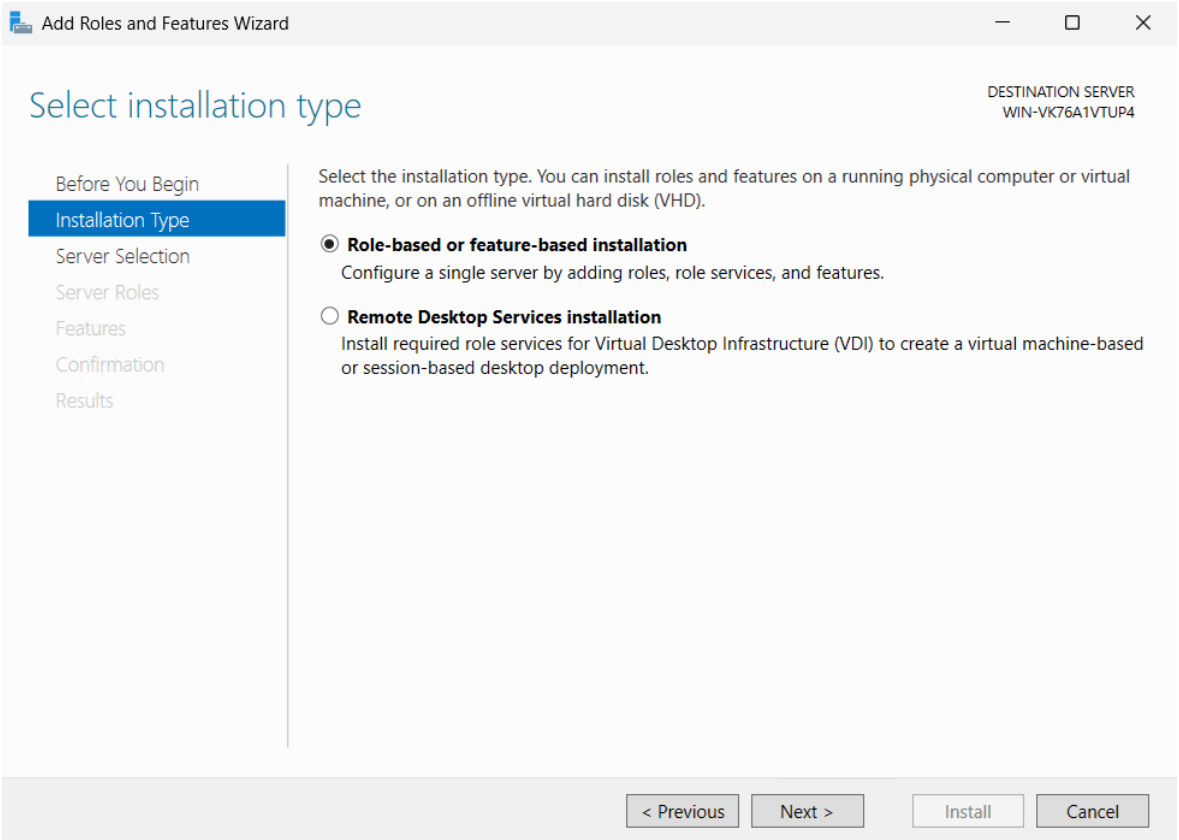

Рисунок 6.34 – Вибір типу встановлення в «Майстрі встановлення ролей та компонентів»

В наступній вкладці майстра вибирати наш сервер, як цільовий для встановлення ролей та компонентів та натиснути «Далі» (рис. 6.35).

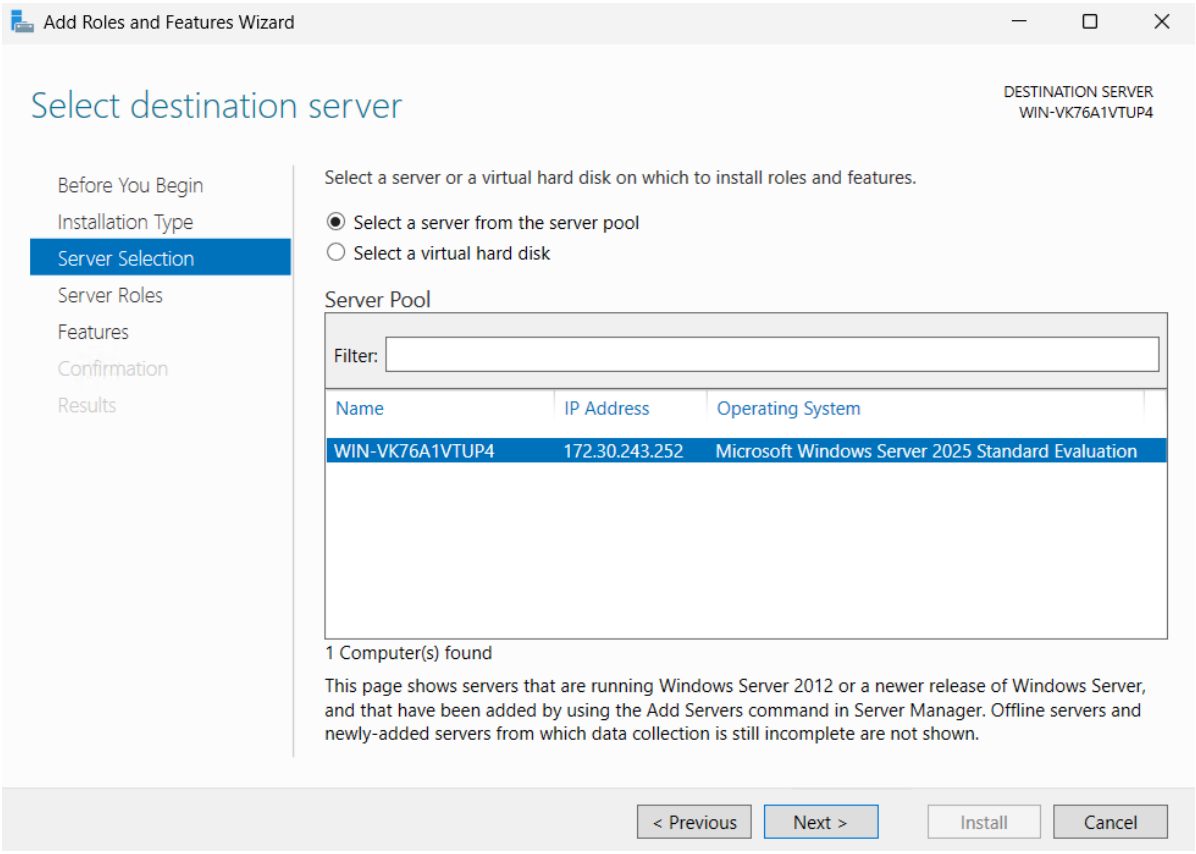

Рисунок 6.35 – Вибір сервера до якого будуть застосовані дії

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. 6.36-6.37).

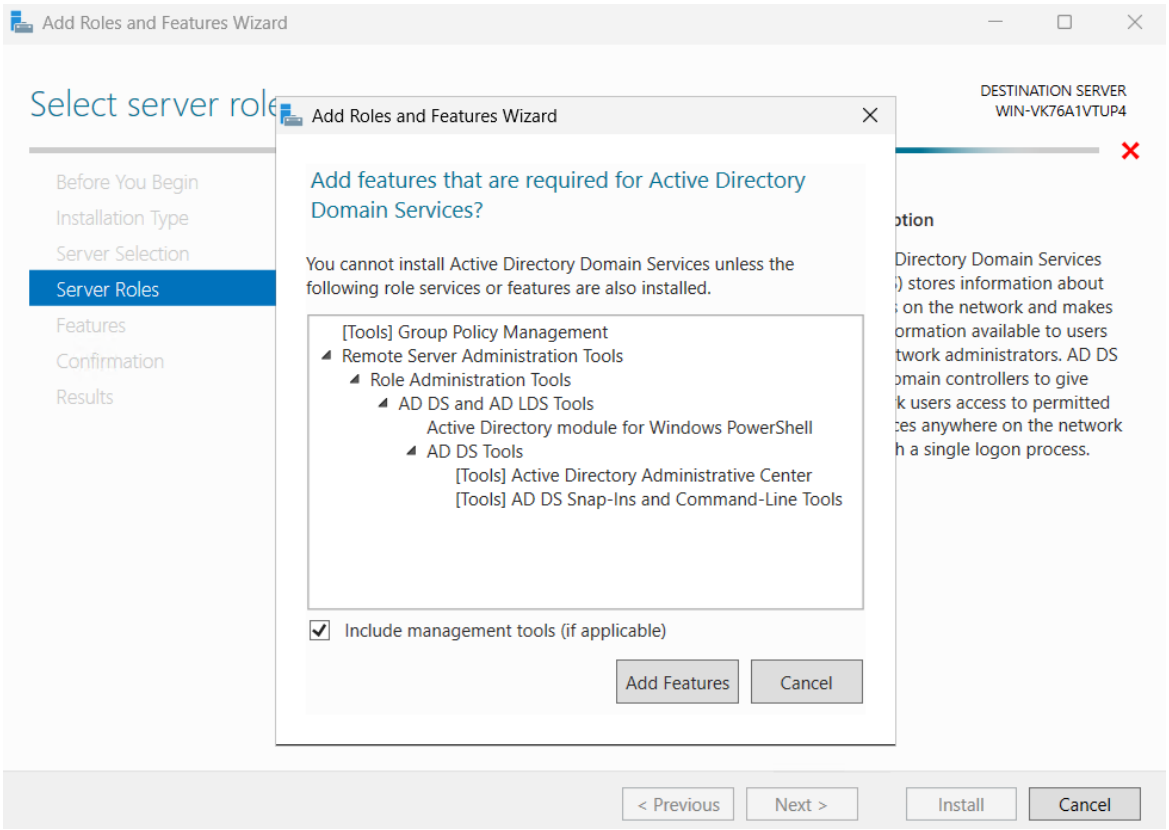

Рисунок 6.36 – Додавання конкретної ролі та її компонентів для сервера

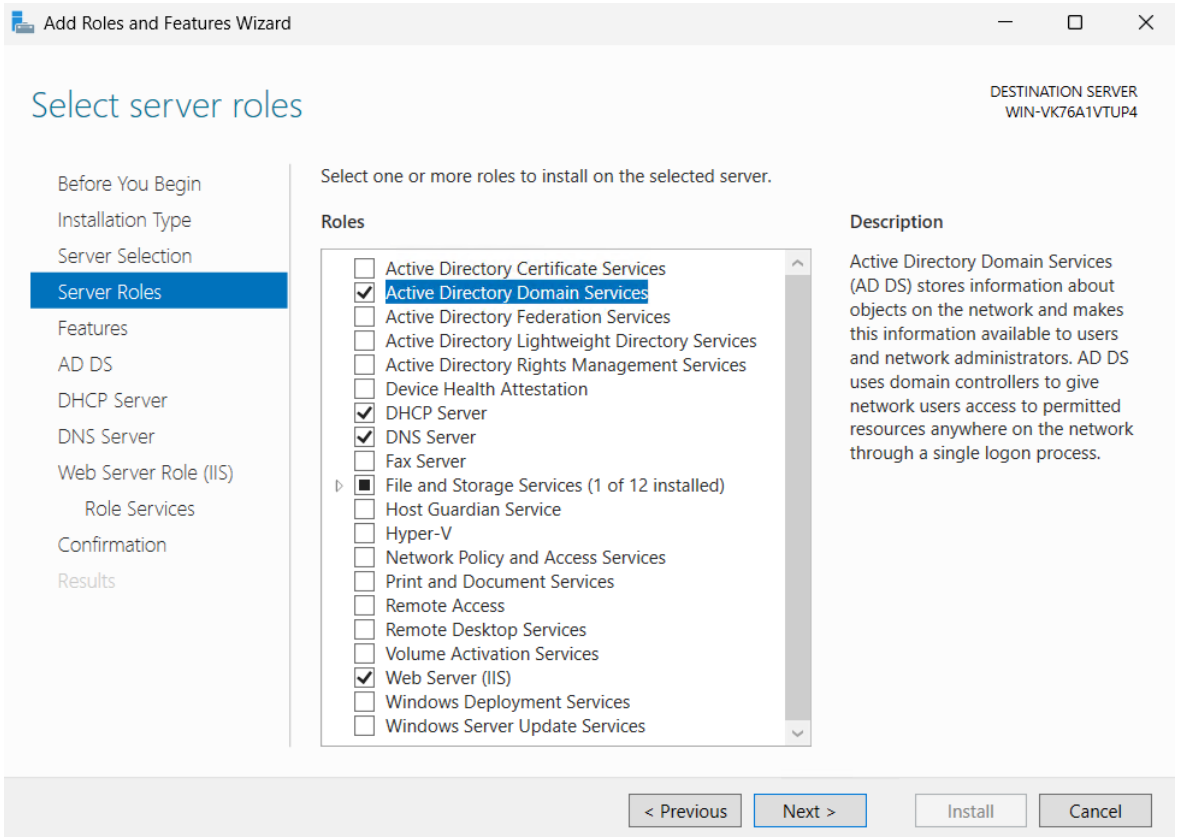

Рисунок 6.37 – Вибір ролей для сервера

В наступній вкладці майстра вибирати компоненти, які слід додати серверу. Для цього ставимо «галочку» навпроти потрібного компонента та після цього натискаємо «Далі» (рис. 6.38).

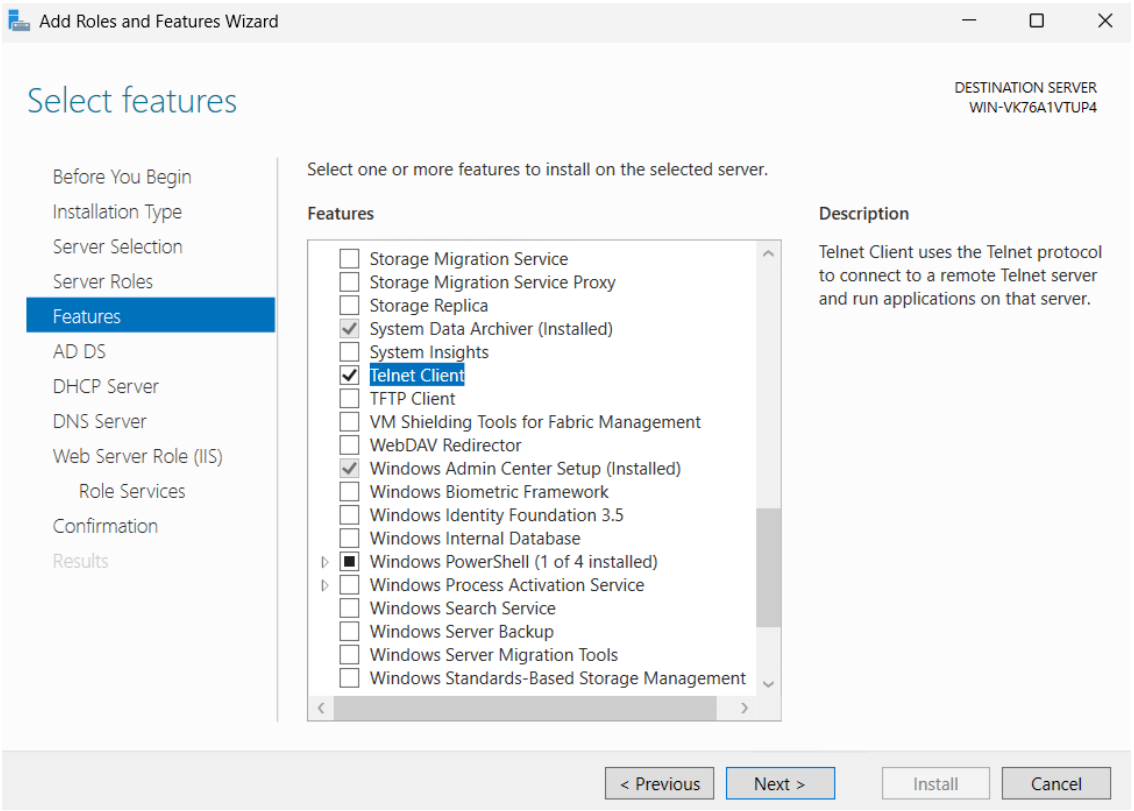

Рисунок 6.38 – Вибір та додавання компонентів

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. 6.39).

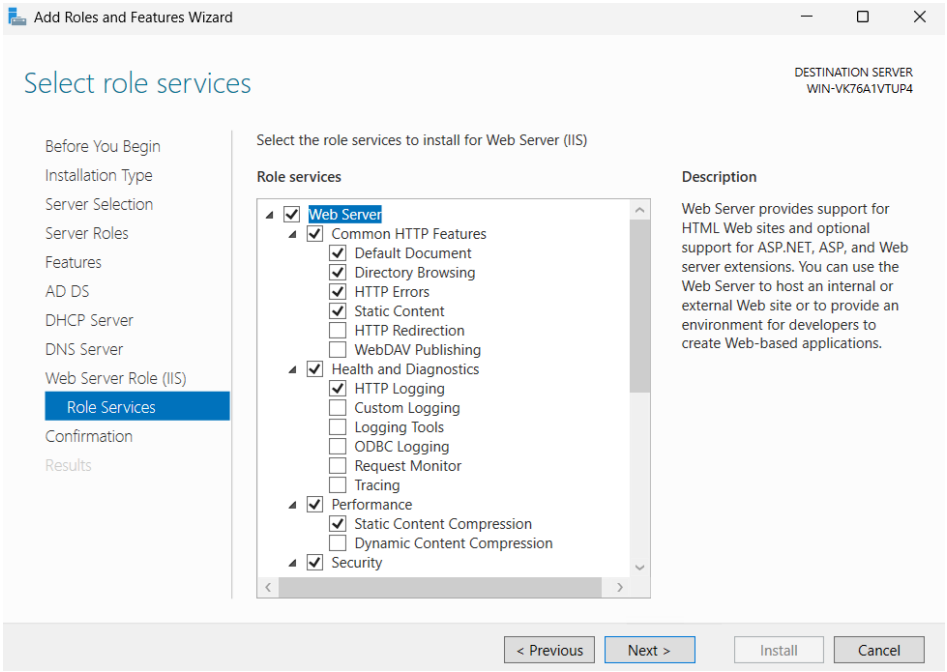

Рисунок 6.39 – Вибір та додавання служб ролей сервера

Далі виконати підтвердження встановлення вибраних ролей та компонентів і натиснути «Встановити». Розпочинається процес встановлення (рис. 6.40-6.41).

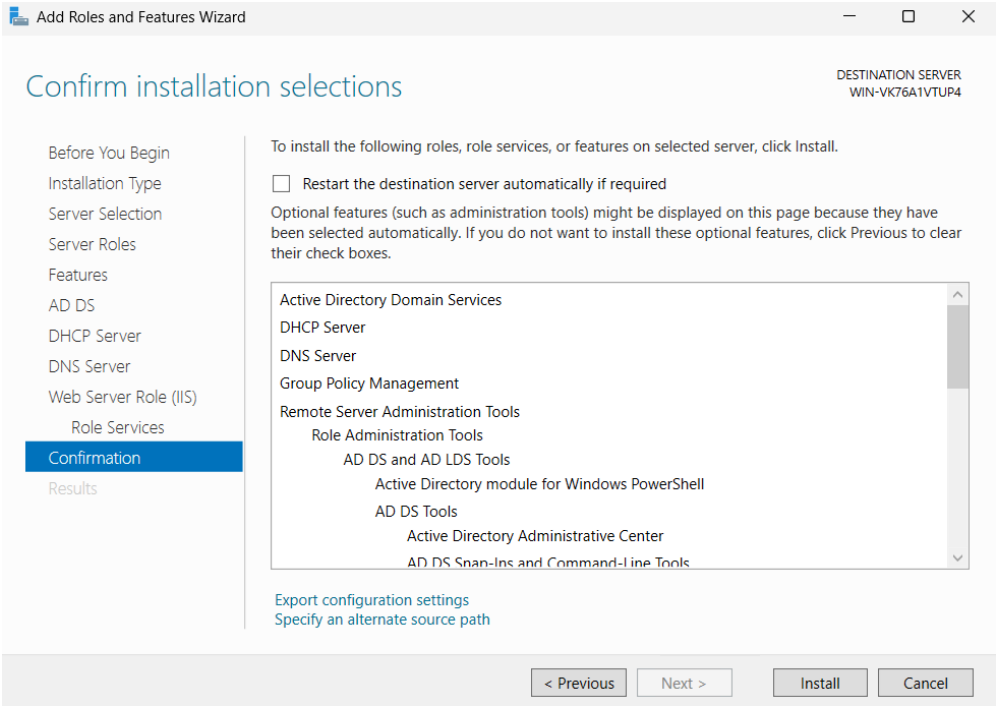

Рисунок 6.40 – Підтвердження встановлення ролей та компонентів для вибраного сервера

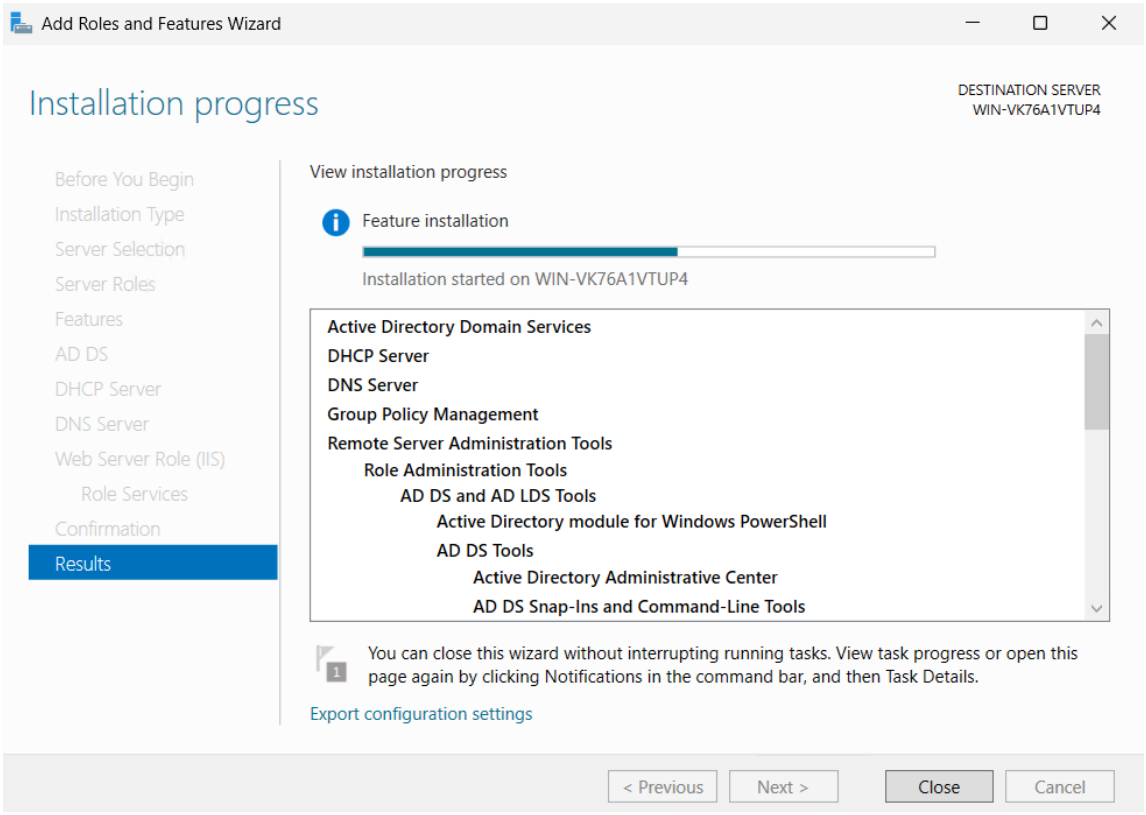

Рисунок 6.41 – Процес встановлення ролей та компонентів після вибору та підтвердження

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. 6.42-6.44).

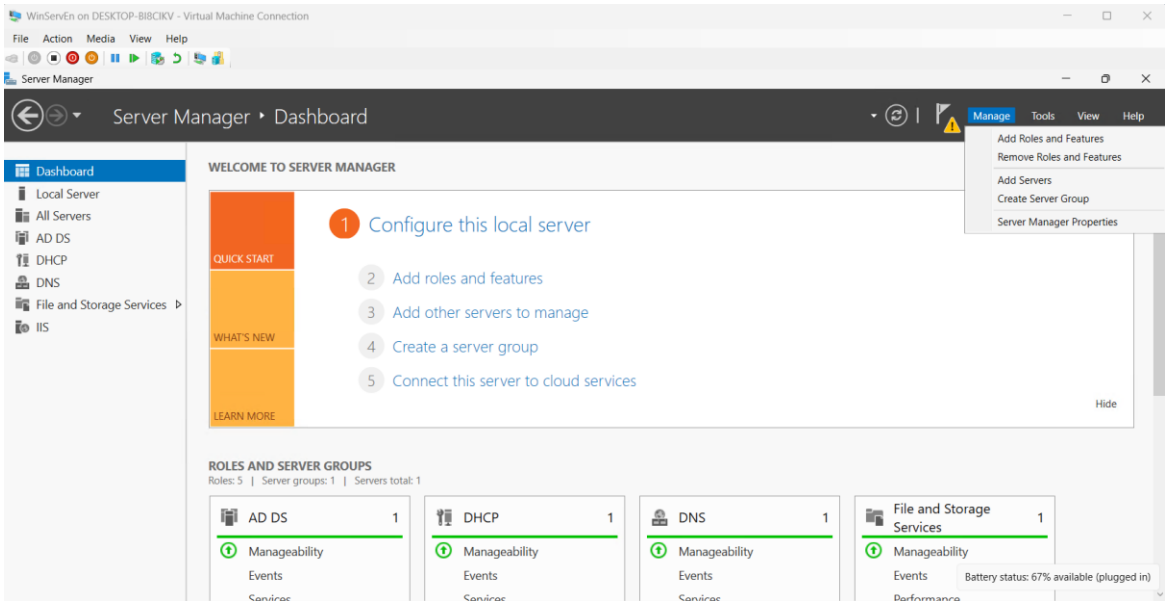

Рисунок 6.42 – Вибір пункту меню «Видалити ролі та компоненти»

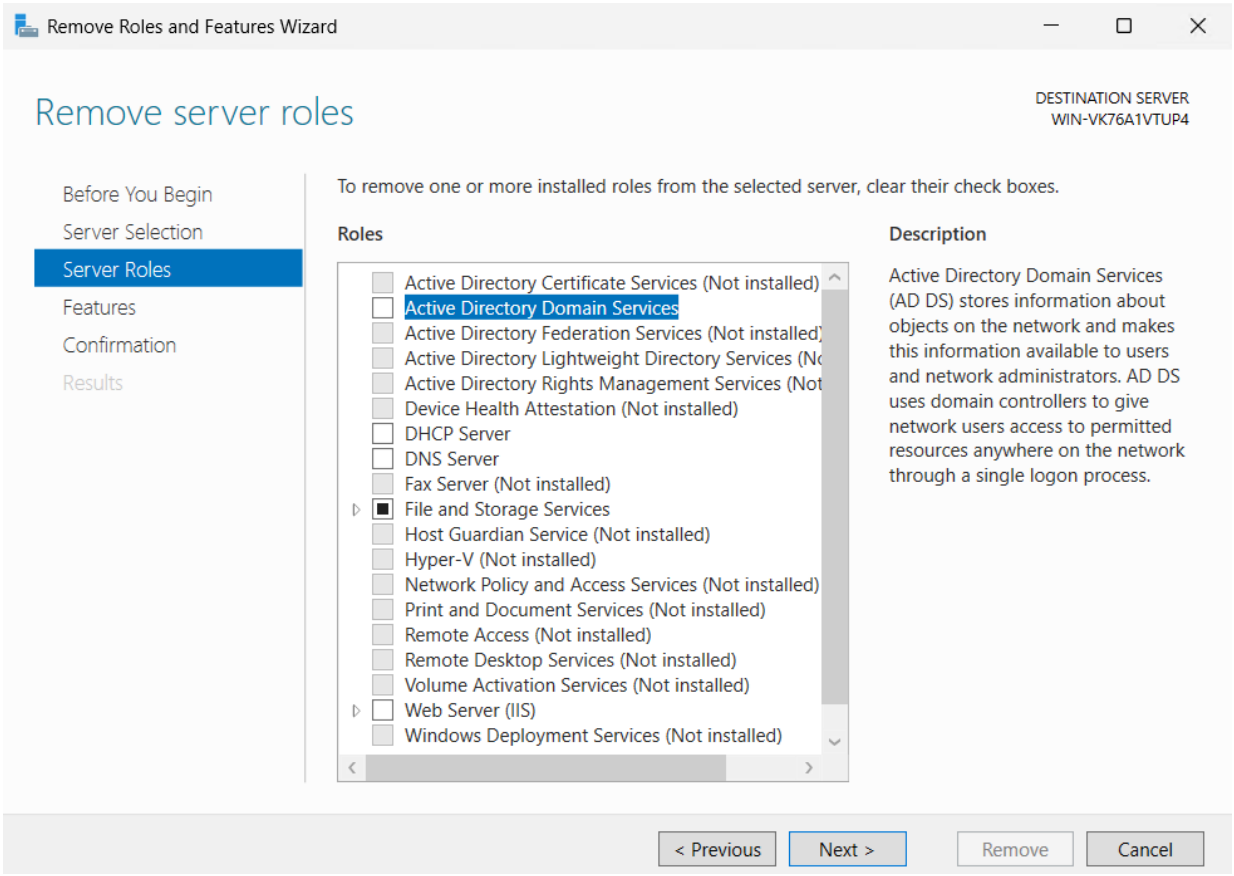

Рисунок 6.43 – Вибір ролі, що буде видалена

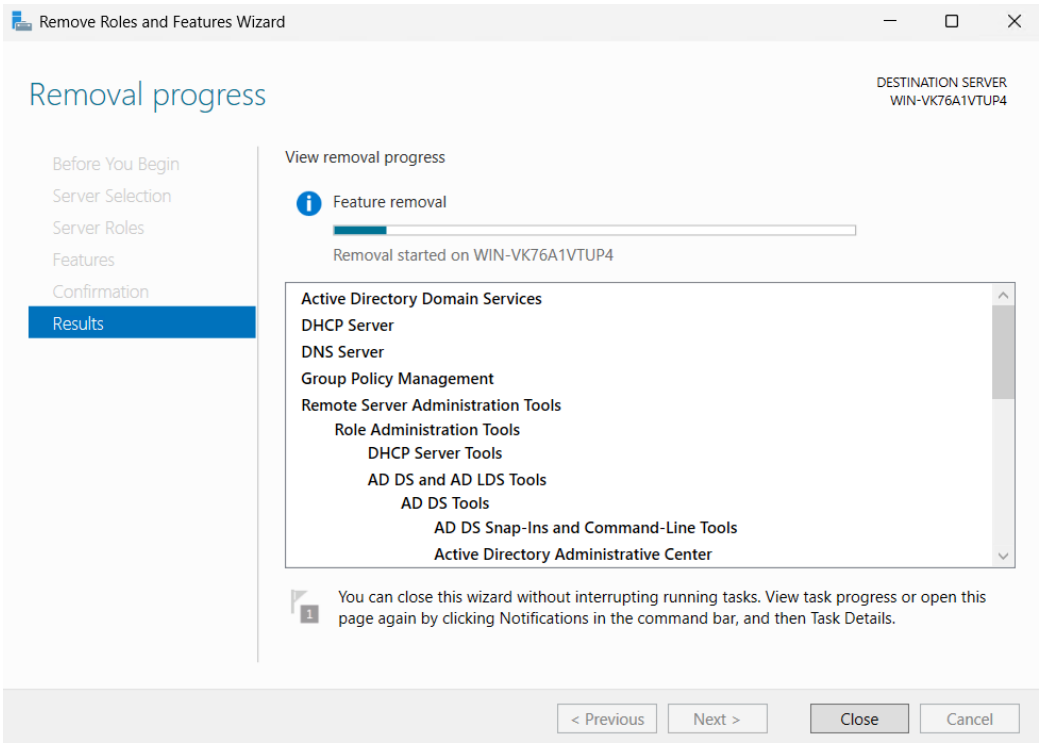

Рисунок 6.44 – Процес видалення вибраних ролей та компонентів

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. 6.45).

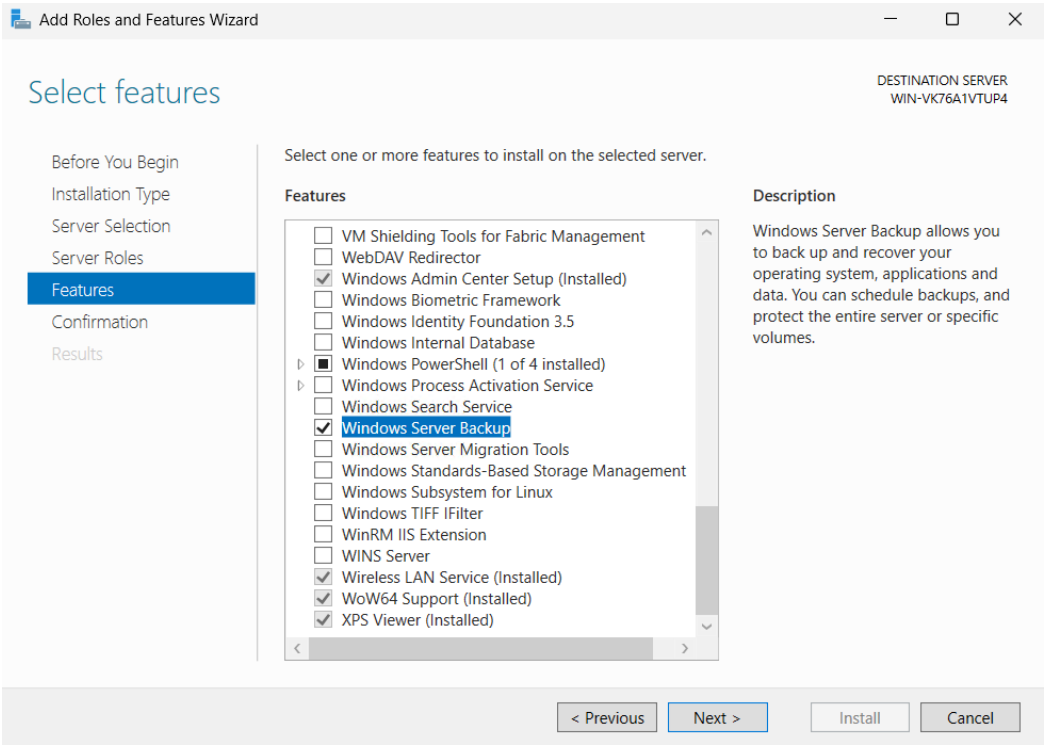

Рисунок 6.45 – Встановлення компонента «Система архівації даних Windows Server»

Відкрити «Систему архівації даних Windows Server» для налаштування резервного копіювання. Натиснути «Інструменти» – «Система архівації даних Windows Server» (рис. 6.46).

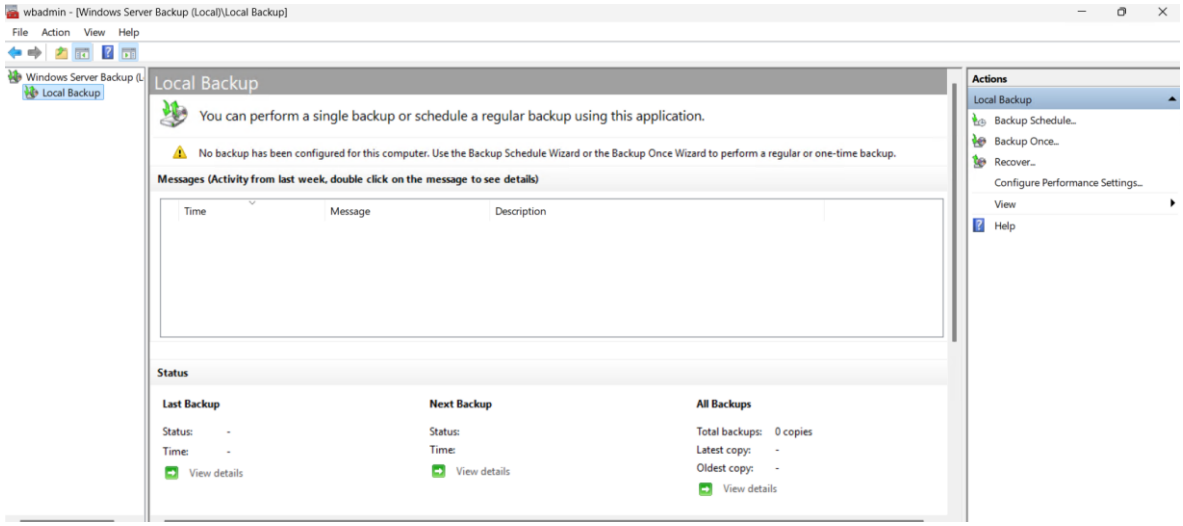

Рисунок 6.46 – Відкрите вікно «Система архівації даних Windows Server»

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. 6.47-6.48).

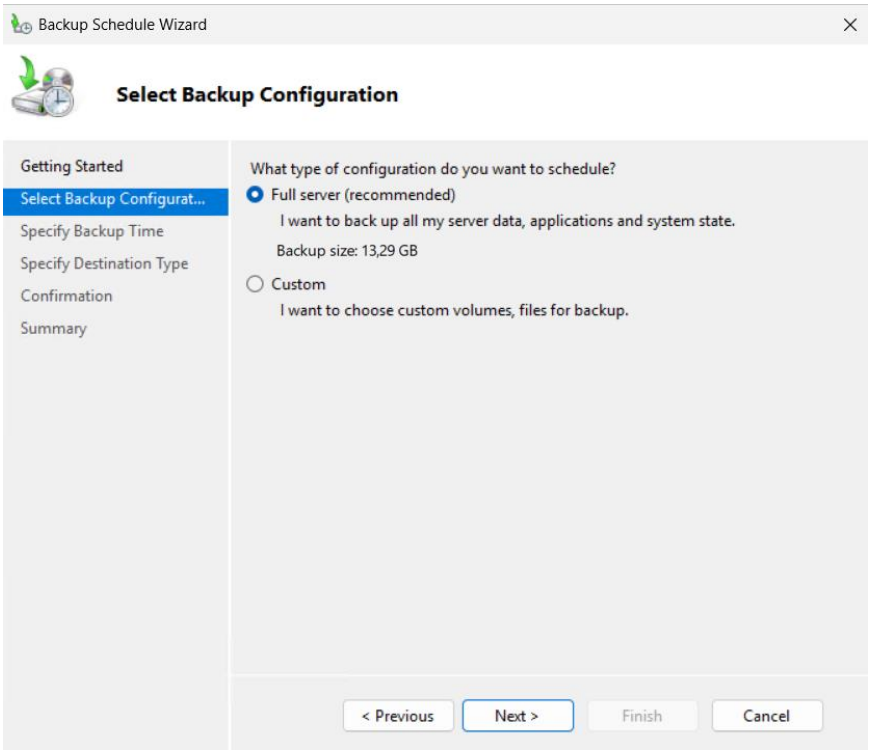

Рисунок 6.47 – Початок налаштування автоматичного резервного копіювання

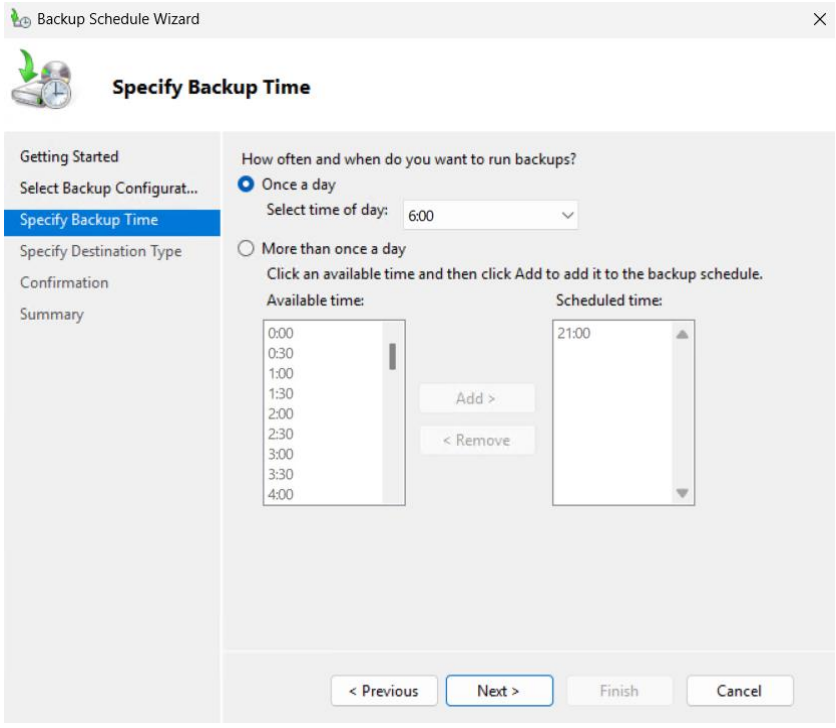

Рисунок 6.48 – Вибір часу та частоти резервного копіювання

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. 6.49).

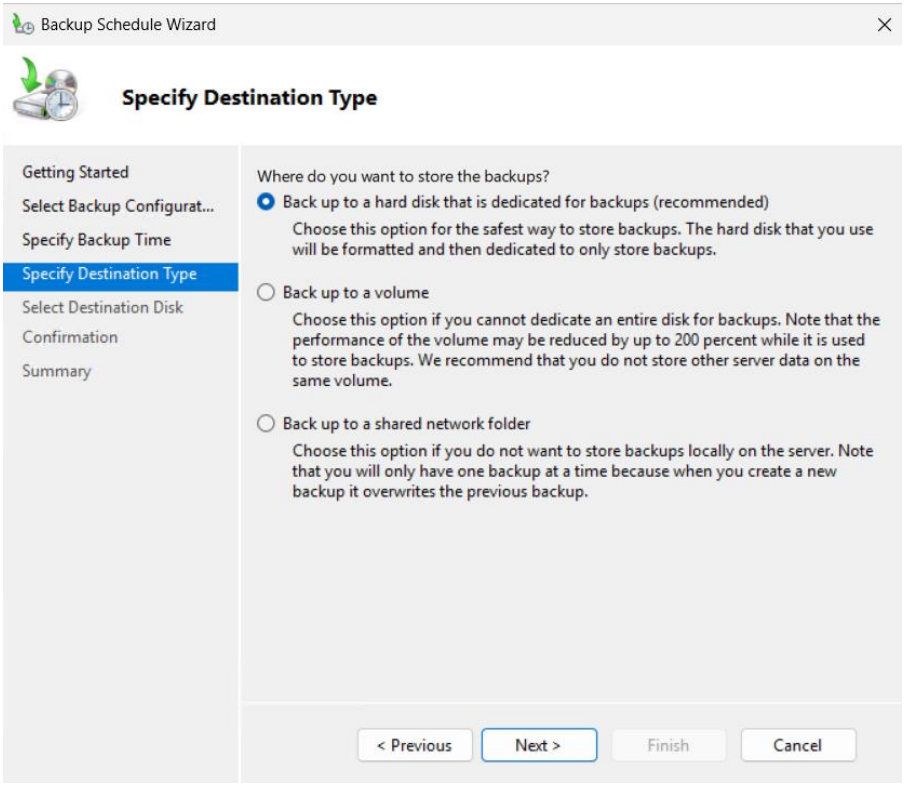

Рисунок 6.49 – Вибір типу місця призначення для автоматичного резервного копіювання сервера

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. 6.50).

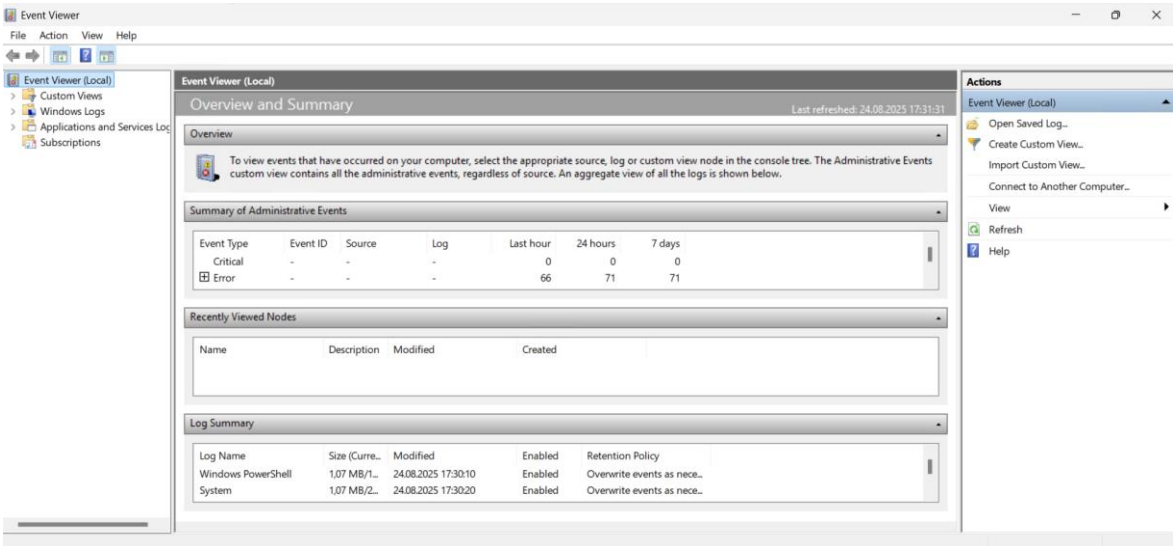

Рисунок 6.50 – Вікно «Перегляд подій»

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. 6.51).

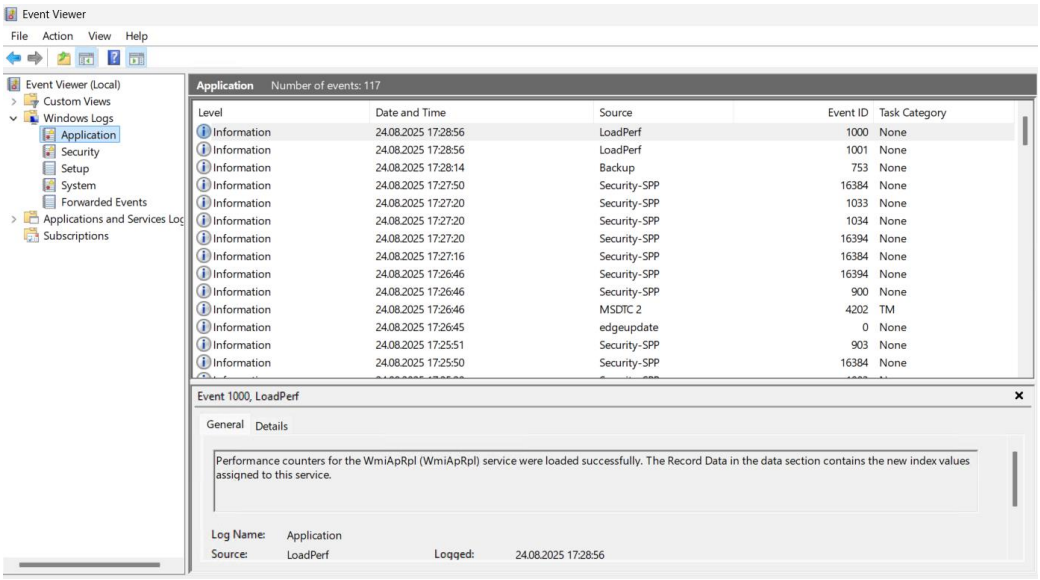

Рисунок 6.51 – Журнал «Застосунки»

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. 6.52).

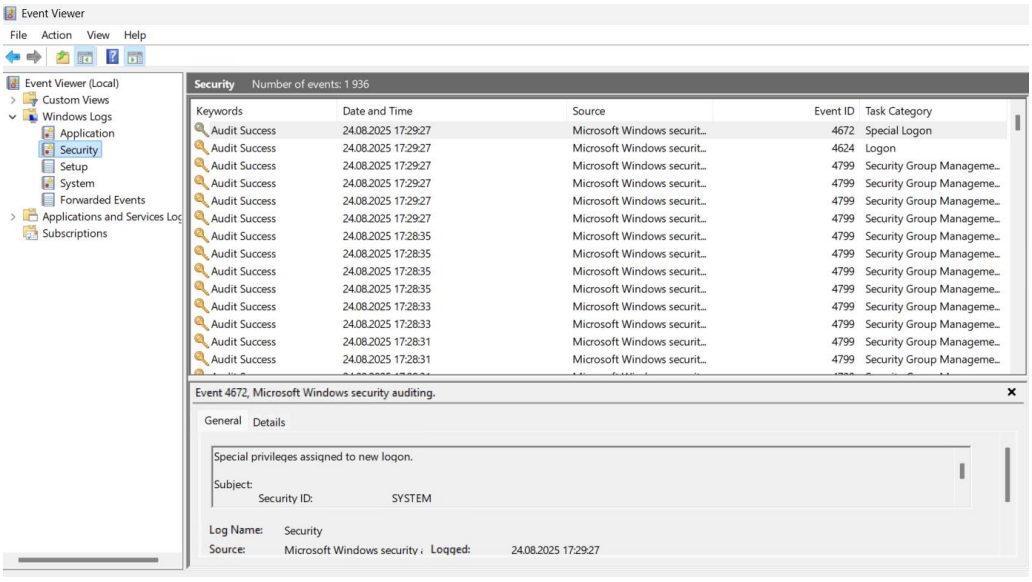

Рисунок 6.52 – Журнал «Безпека»

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. 6.53).

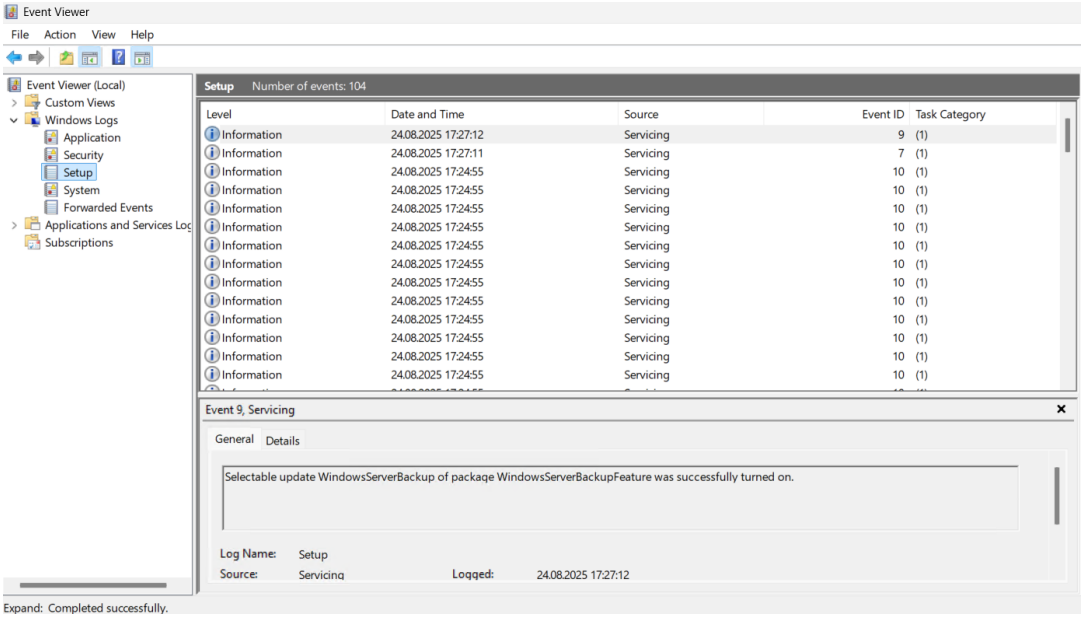

Рисунок 6.53 – Журнал «Встановлення»

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. 6.54).

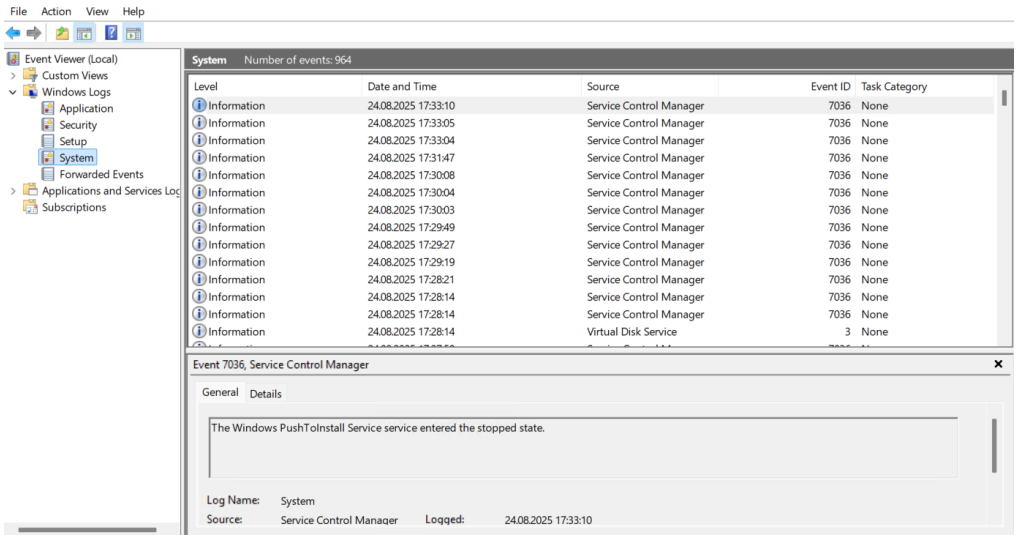

Рисунок 6.54 – Журнал «Система»

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. 6.55).

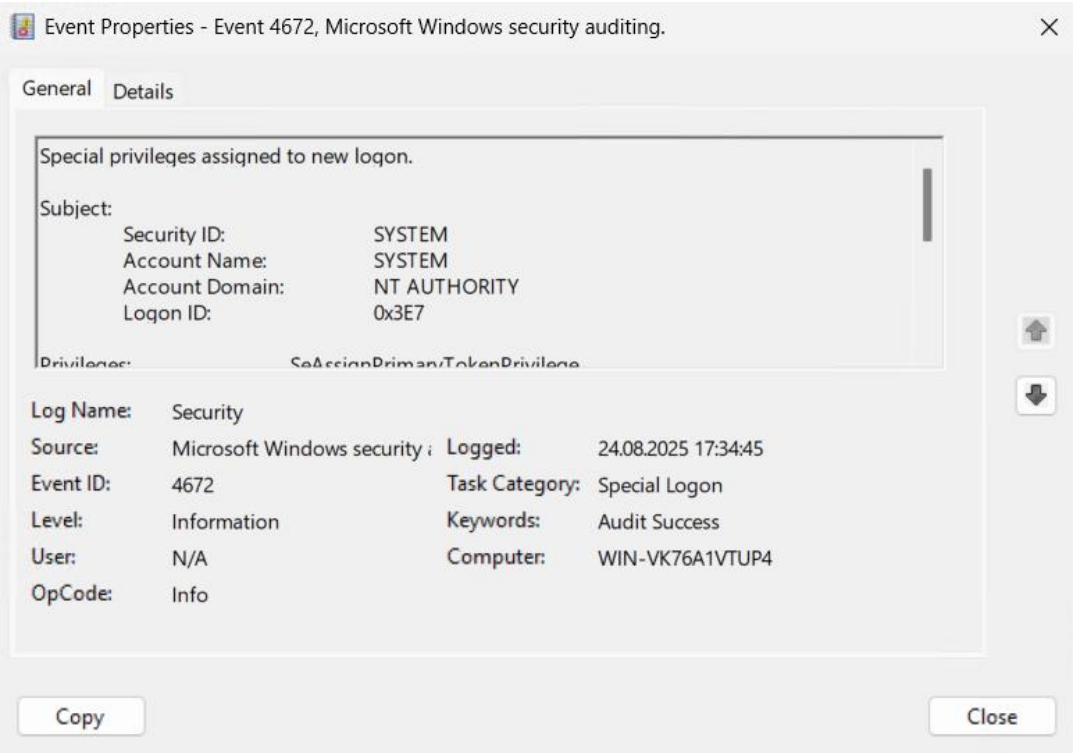

Рисунок 6.55 – Властивості події

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. 6.56-6.57).

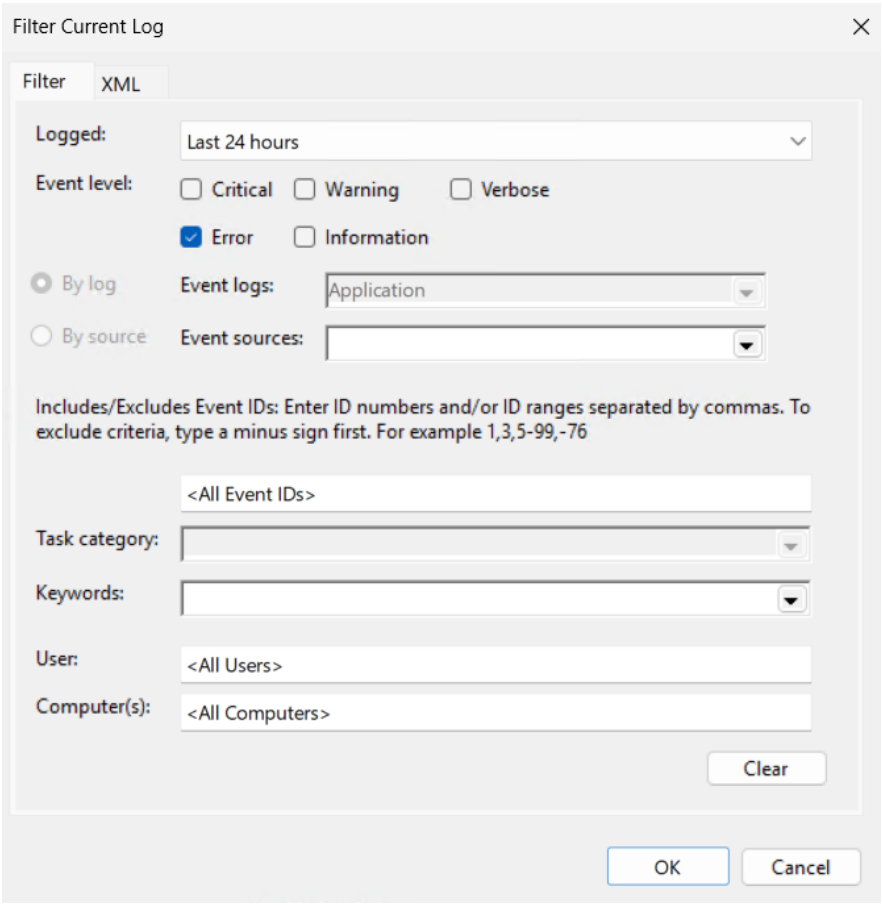

Рисунок 6.56 – Фільтрацію журналу для знаходження помилок за останні 24 години

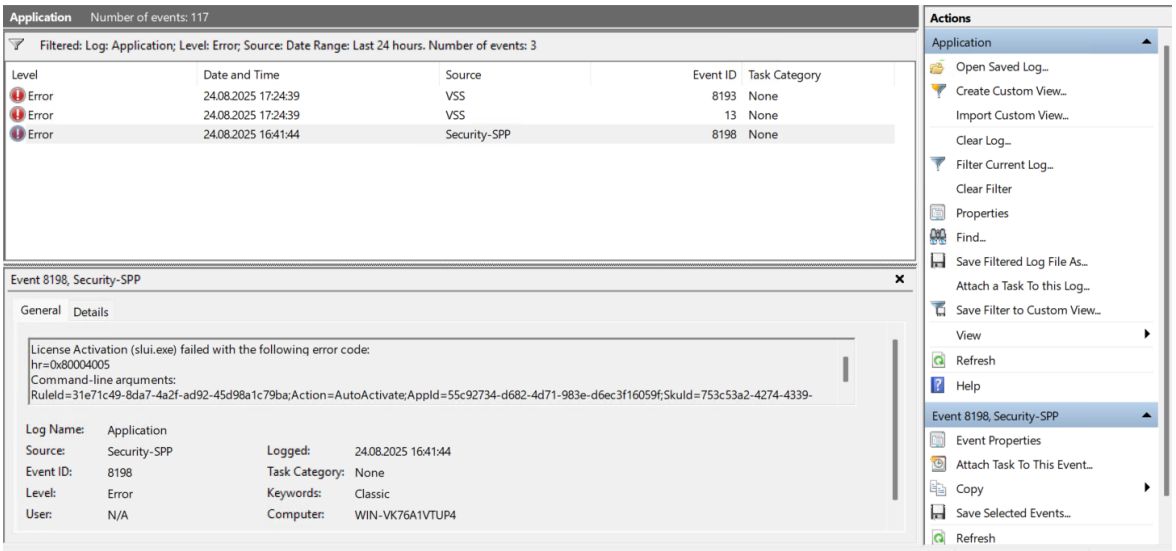

Рисунок 6.57 – Результати фільтрації на знаходження помилок

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. 6.58).

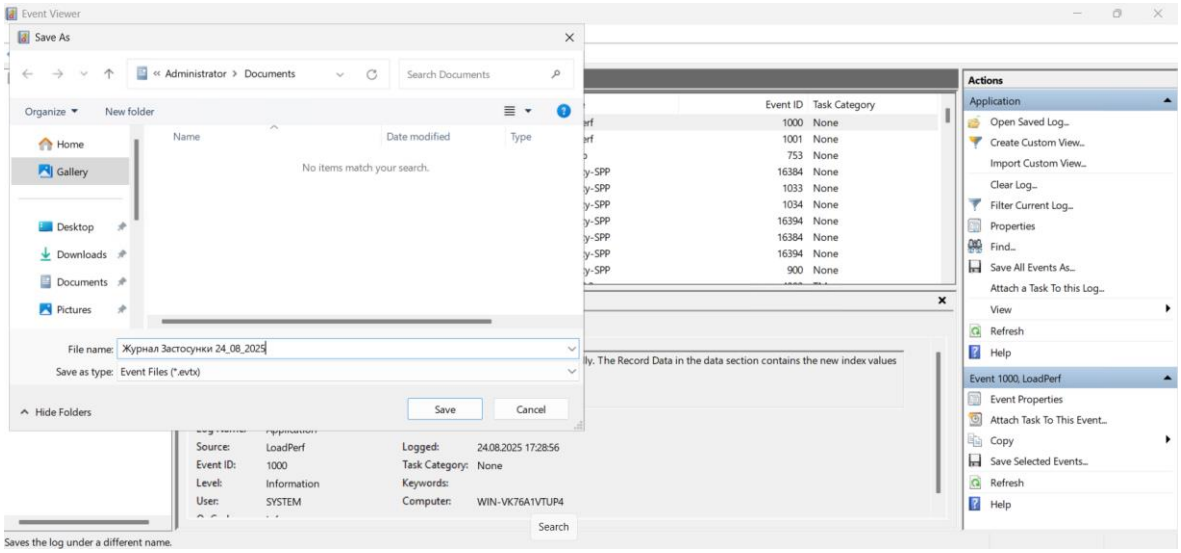

Рисунок 6.58 – Збереження журналу

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. 6.59-6.60).

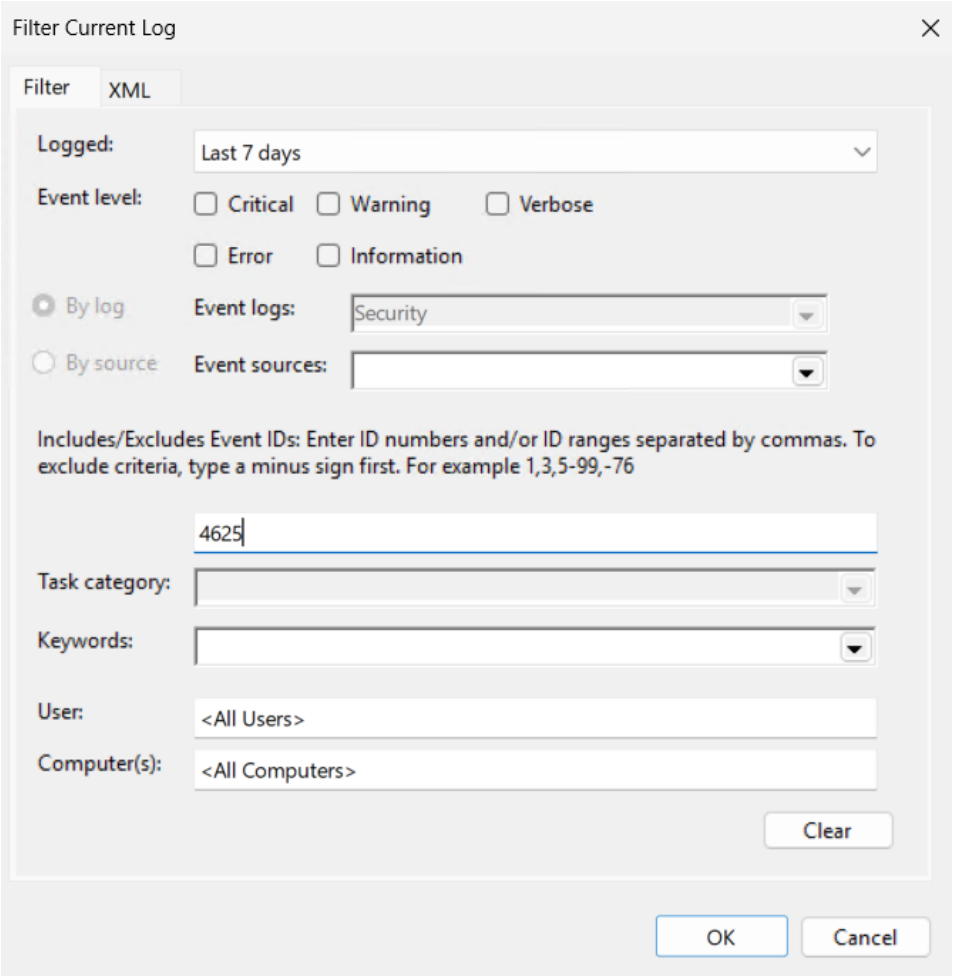

Рисунок 6.59 – Фільтрація журналу за кодом події

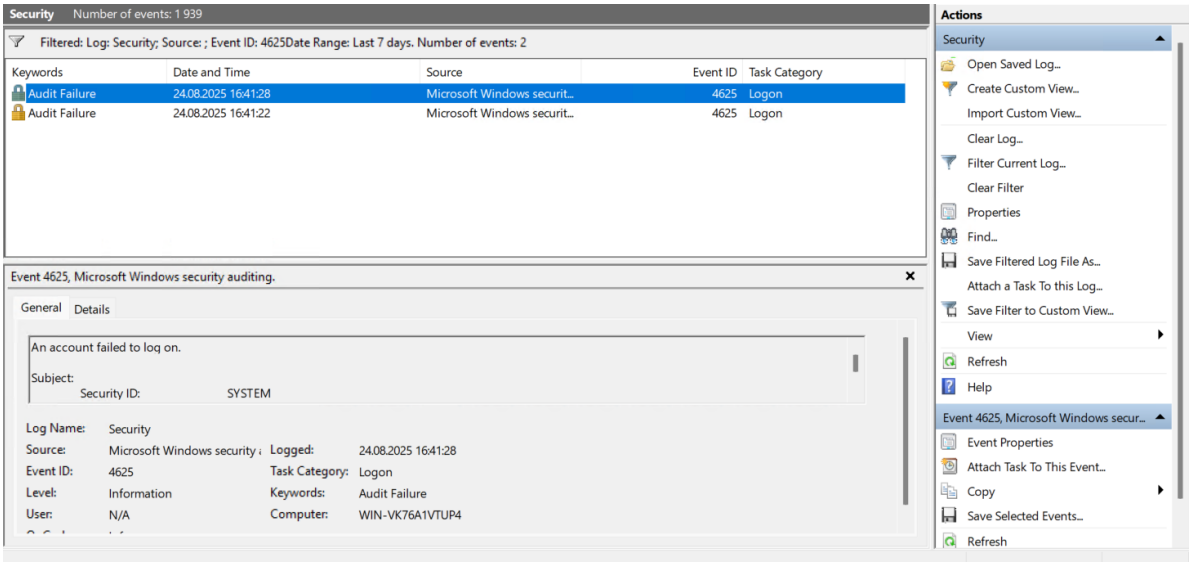

Рисунок 6.60 – Результат фільтрації журналу за кодом події «4625»

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 №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. 7.1).

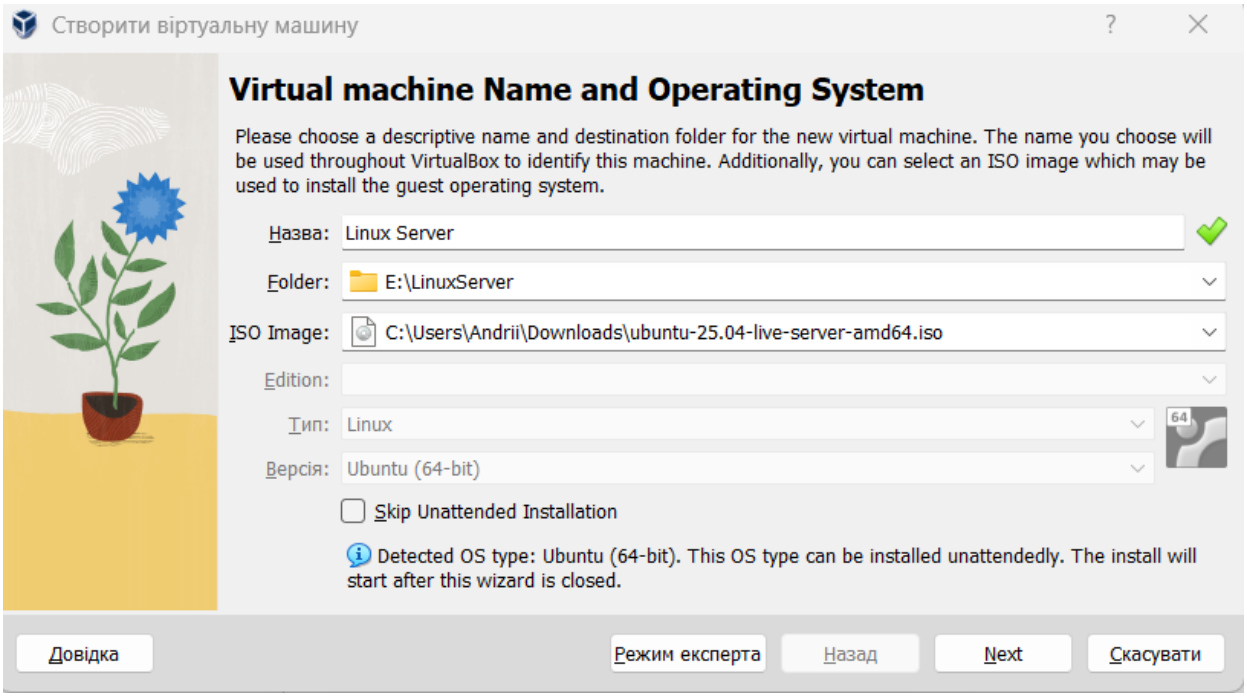

Рисунок 7.1 – Створення нової ВМ Linux Server

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. 7.2).

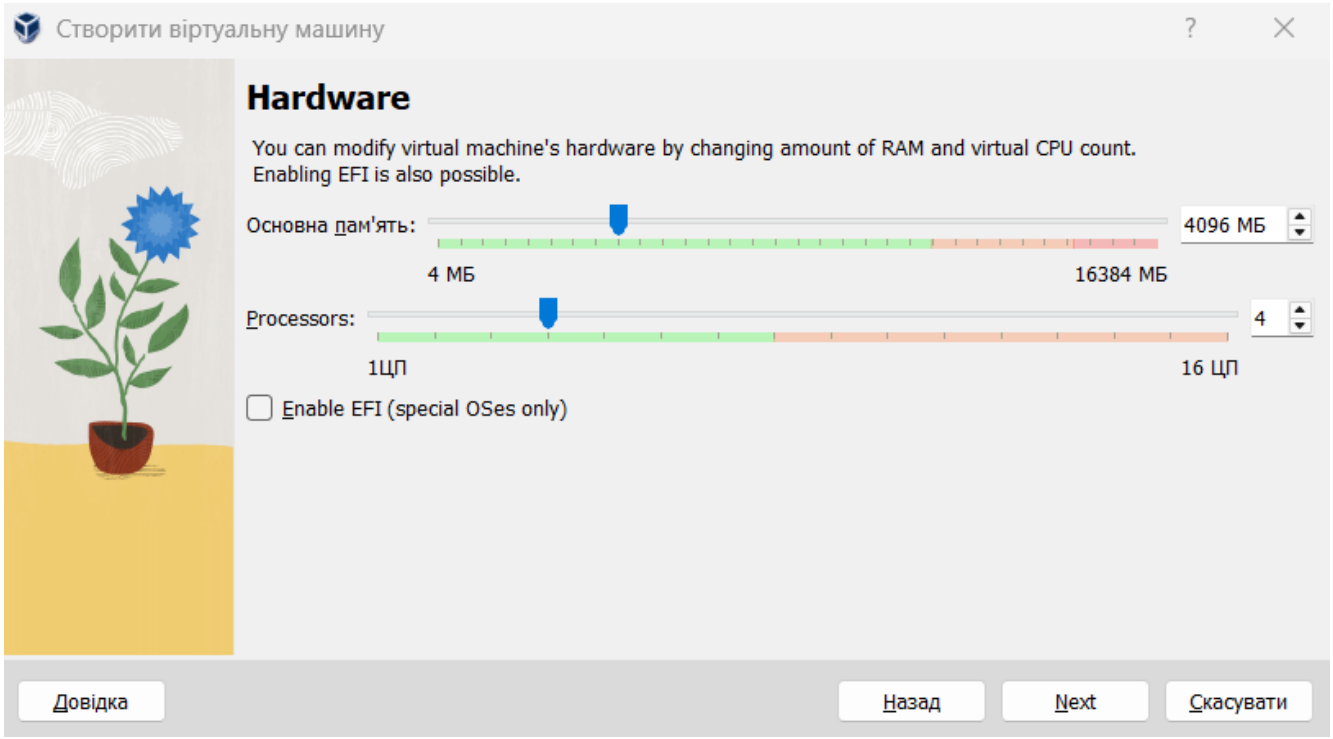

Рисунок 7.2 – Виділення ОП та ядер процесора для ВМ

Далі створити віртуальний жорсткий диск та вказати його розмір (мінімальний розмір 30 ГБ) (рис. 7.3).

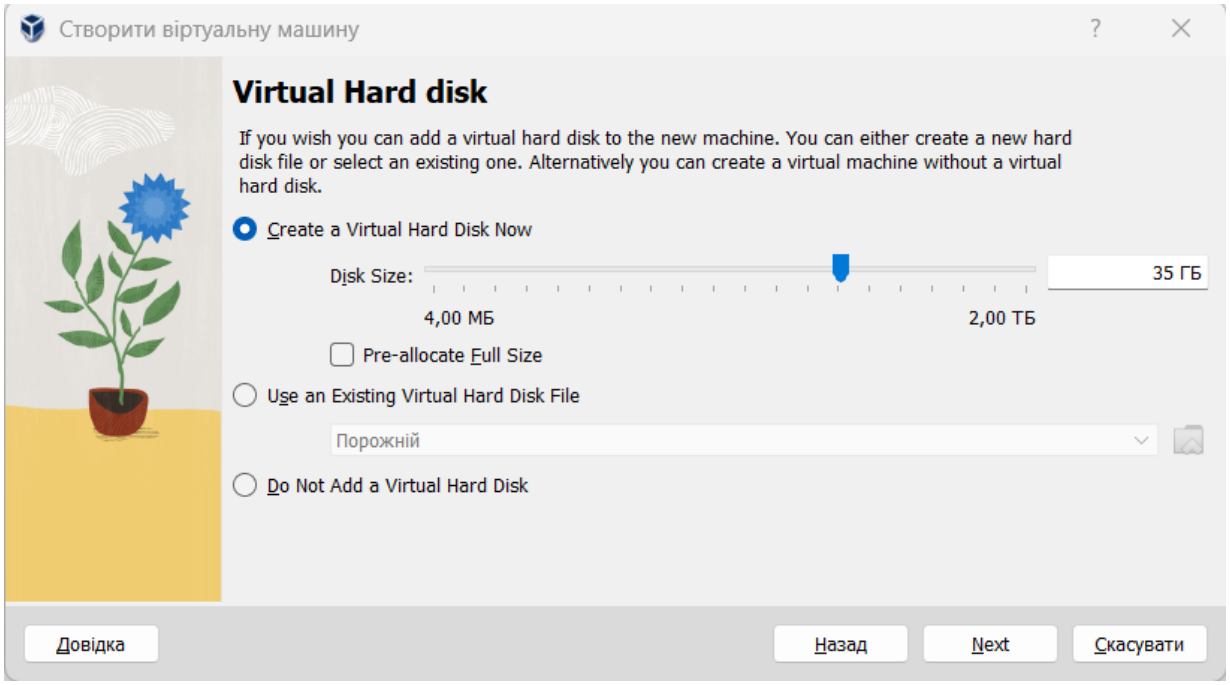

Рисунок 7.3 – Створення віртуального жорсткого диска

На наступній вкладці натиснути «Закінчити». Після цього автоматично запускається створена ВМ (рис. 7.4).

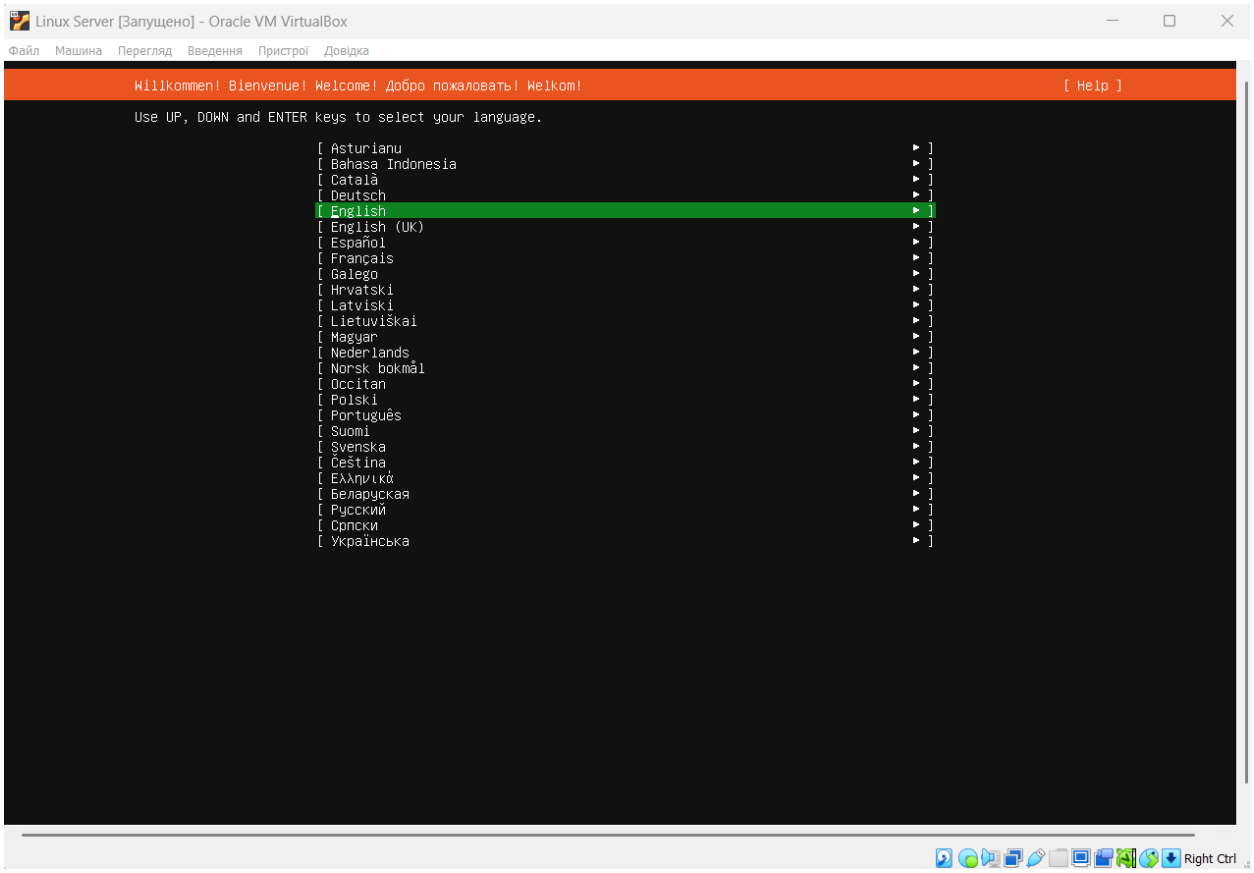

Рисунок 7.4 – Перший запуск ВМ для встановлення ОС

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. 7.5).

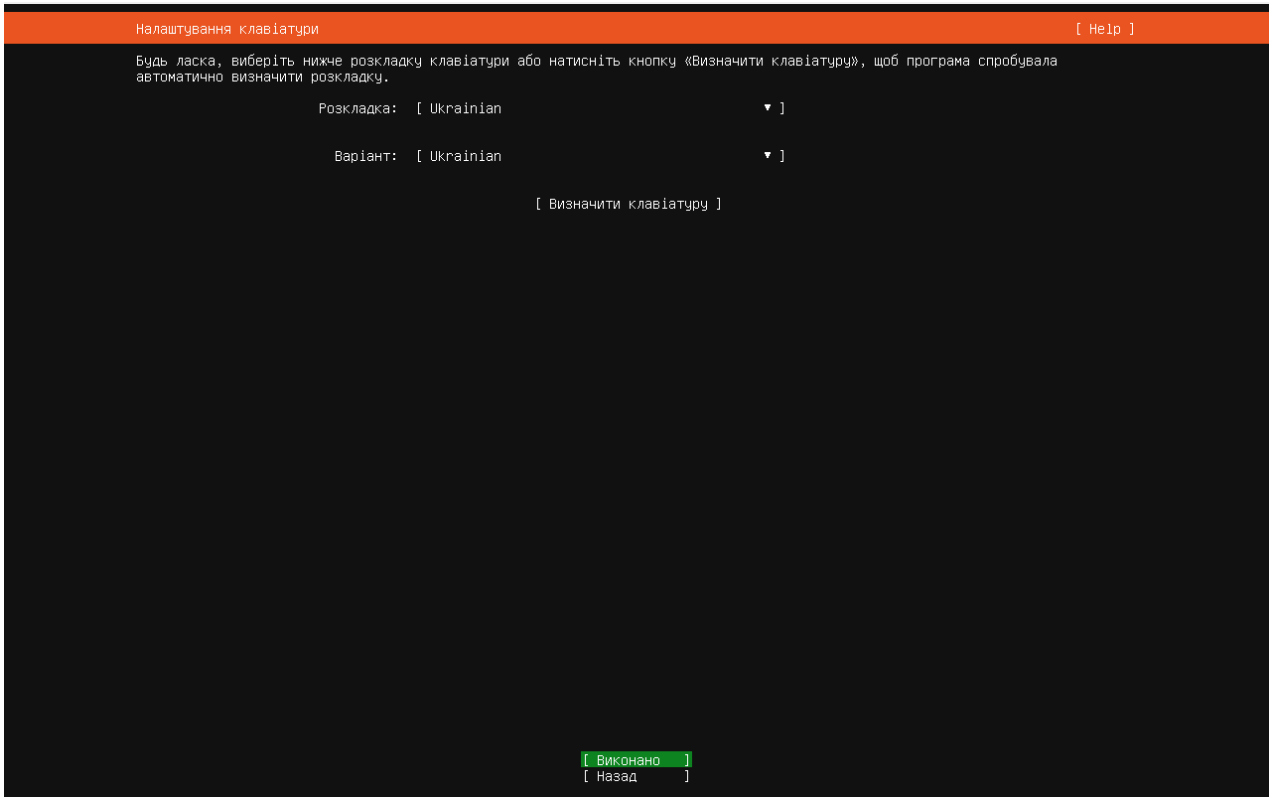

Рисунок 7.5 – Налаштування мови та клавіатури для Linux Server

В наступній вкладці вибирати тип інсталяції – «Ubuntu Server» і знову натиснути «Enter», щоб підтвердити вибір та перейти далі (рис. 7.6).

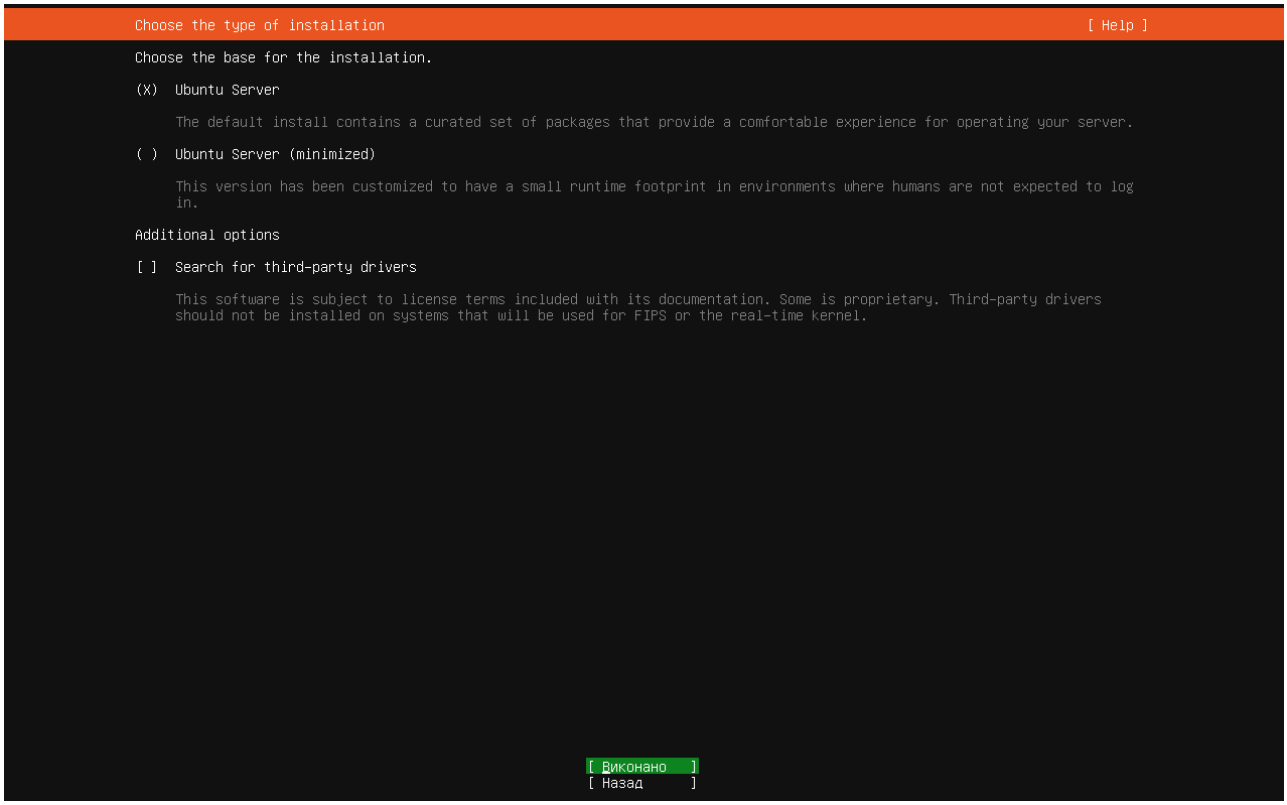

Рисунок 7.6 – Налаштування типу інсталяції для Linux Server

Потім провести початкові налаштування мережевої конфігурації, на цьому етапі все залишаємо без змін та натиснути «Enter» (рис. 7.7).

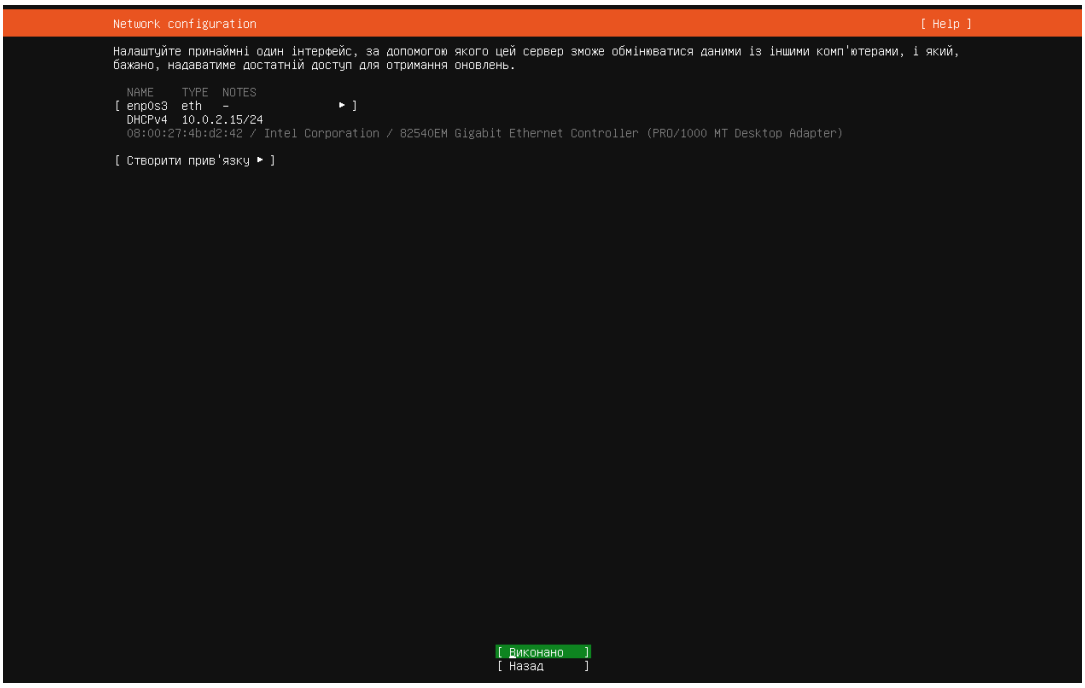

Рисунок 7.7 – Налаштування мережевої конфігурації для Linux Server

В наступній вкладці адресу проксі сервера залишити без змін та просто натиснути «Виконано». Далі «Адреса дзеркала» залишити за замовчуванням і перейти далі (рис. 7.8).

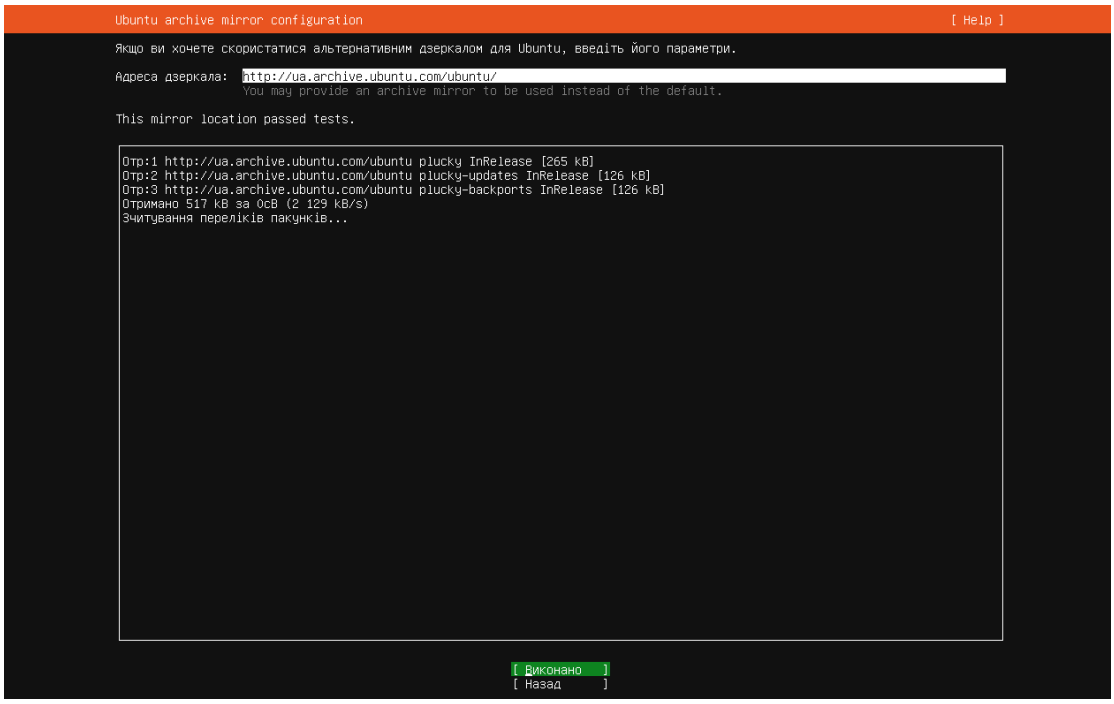

Рисунок 7.8 – Налаштування «Адреса дзеркала» для Linux Server

Згодом, в налаштуваннях сховища даних обирати «Використати увесь диск» та перейти до опції «Виконано» (рис. 7.9).

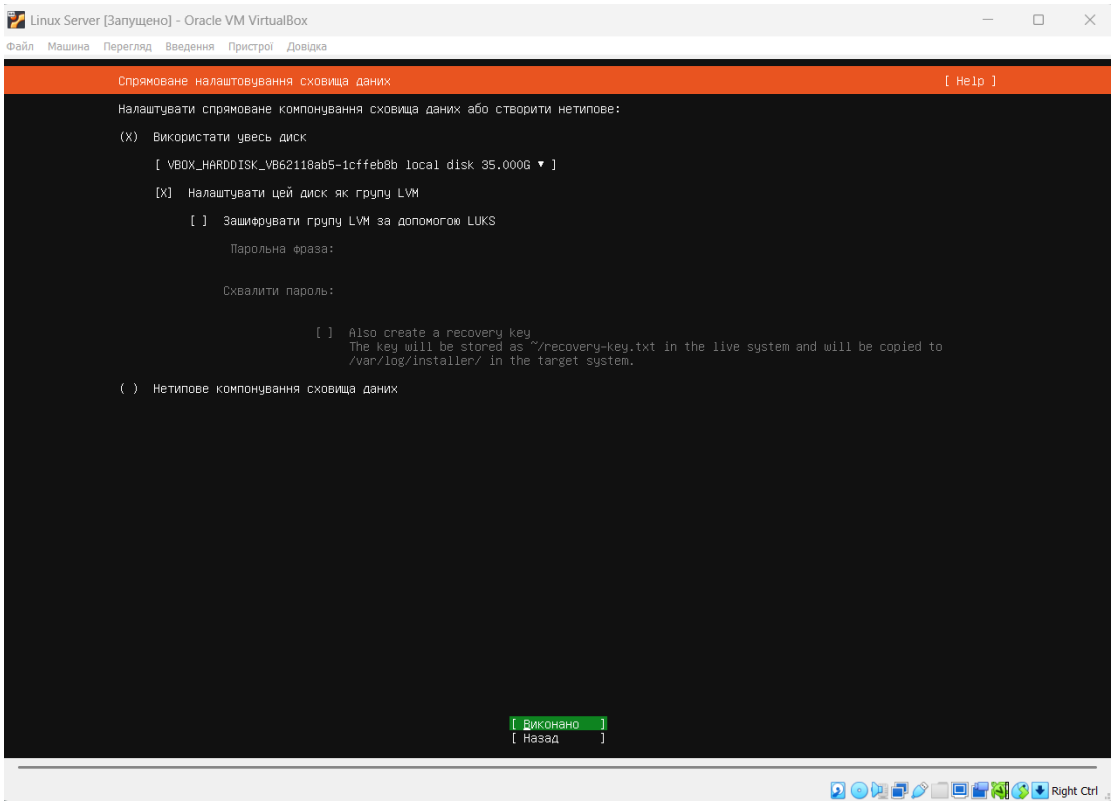

Рисунок 7.9 – Налаштування сховища даних для Linux Server

Після цього, на вкладці «Резюме файлової системи» все залишити без змін і натиснути «Виконано» (рис. 7.10).

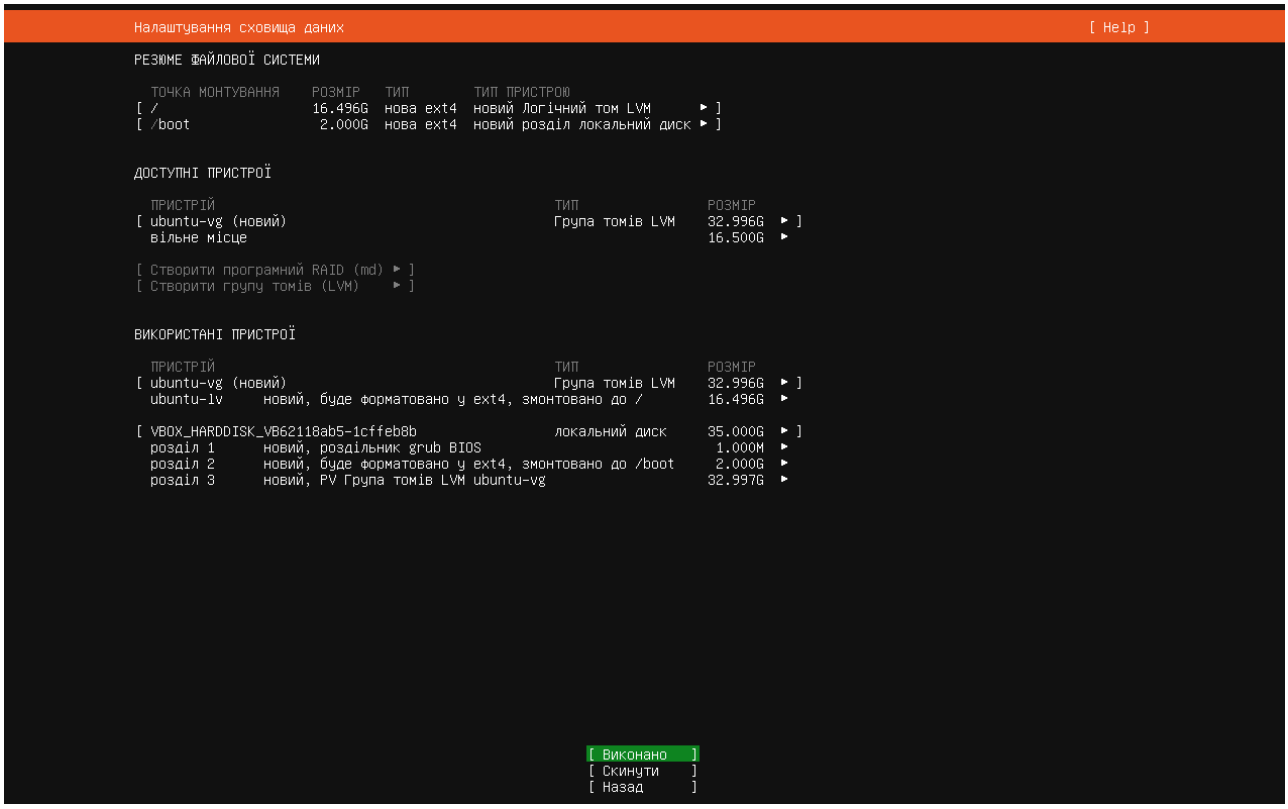

Рисунок 7.10 – Налаштування файлової системи для Linux Server

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. 7.11).

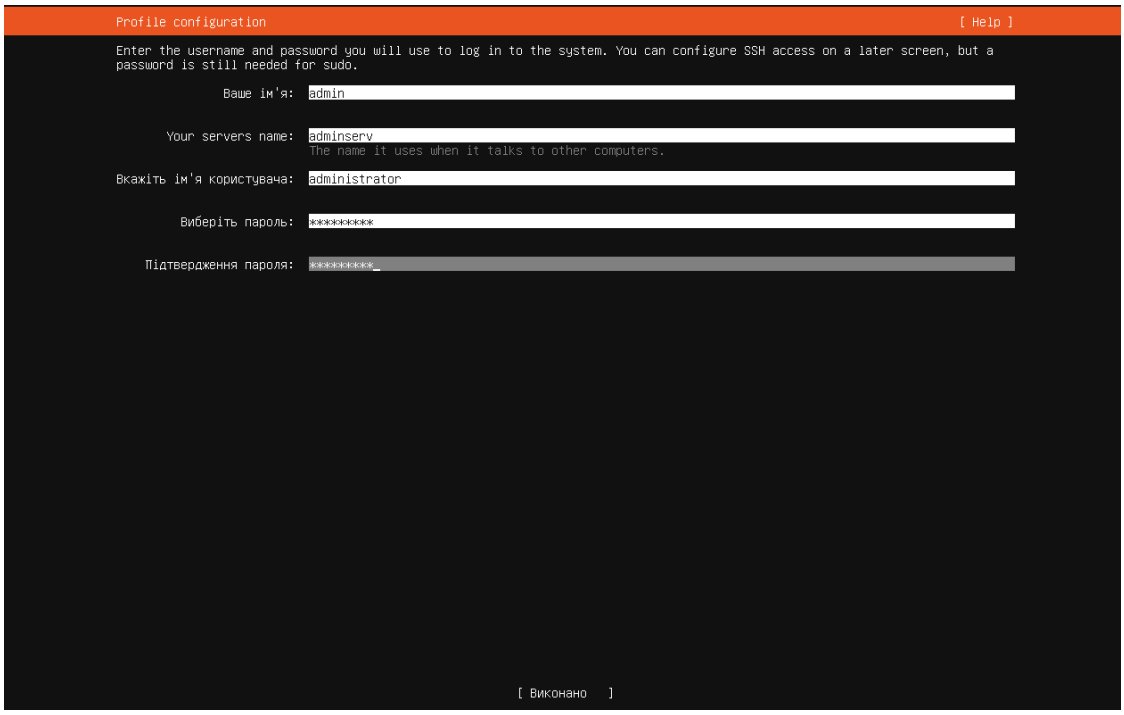

Рисунок 7.11 – Налаштування профіля для Linux Server

В наступному вікні обирати чи встановлювати оболонку SSH для віддаленого доступу на цьому етапі, залишаємо «Не встановлювати» (рис. 7.12).

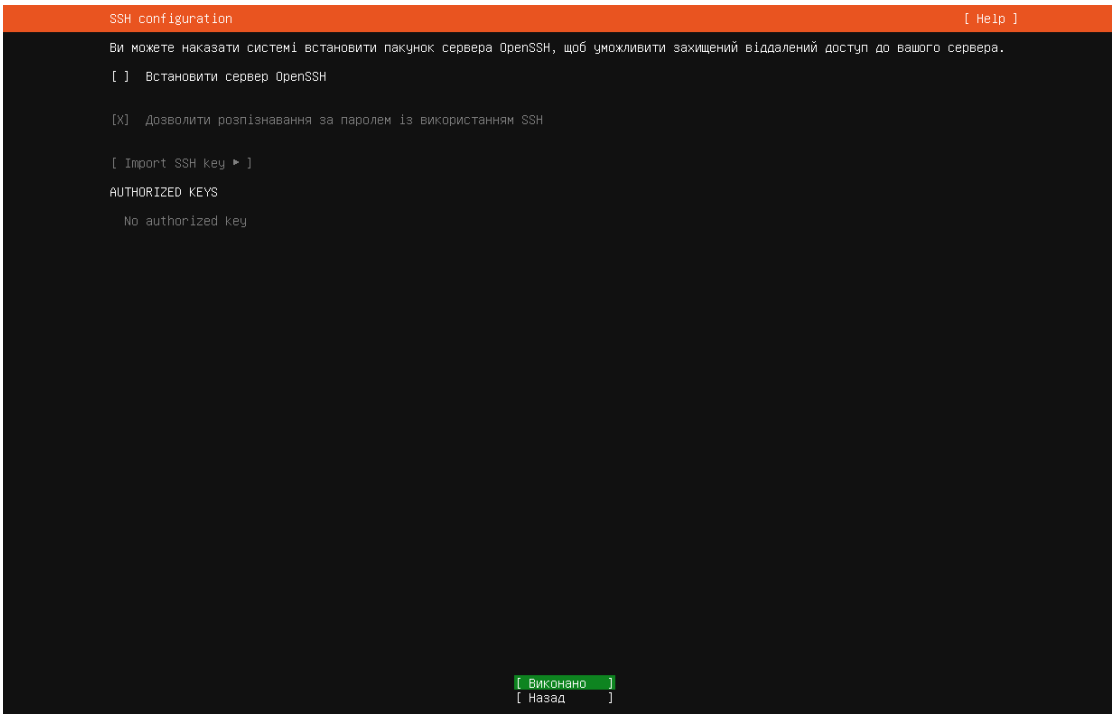

Рисунок 7.12 – Налаштування SSH для Linux Server

На наступному етапі починається встановлення серверної операційної системи Linux Server (рис. 7.13).

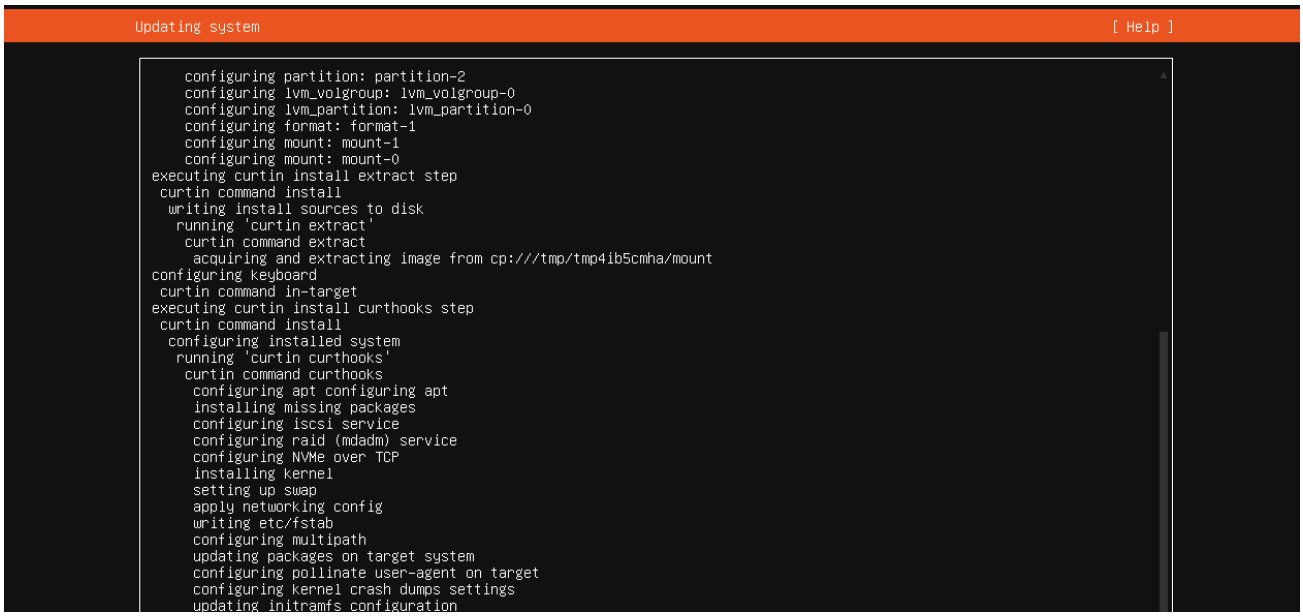

Рисунок 7.13 – Процес встановлення Linux Server

Коли встановлення завершено (вгорі пише «Installation Complete») натиснути «Перезавантажити» (рис. 7.14).

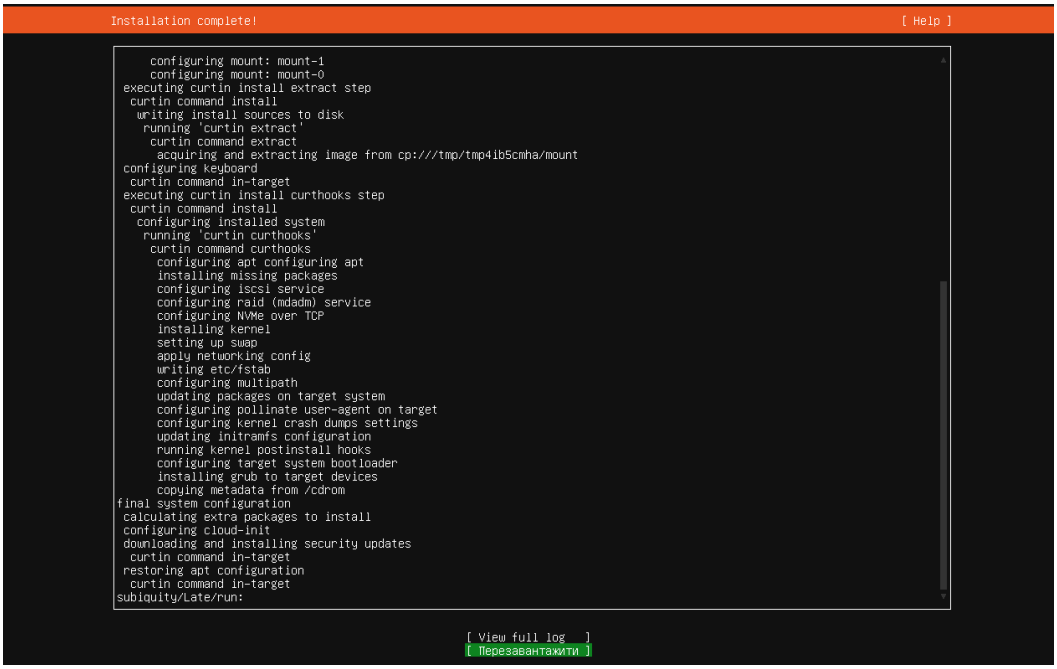

Рисунок 7.14 – Завершення встановлення Linux Server

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. 7.15).

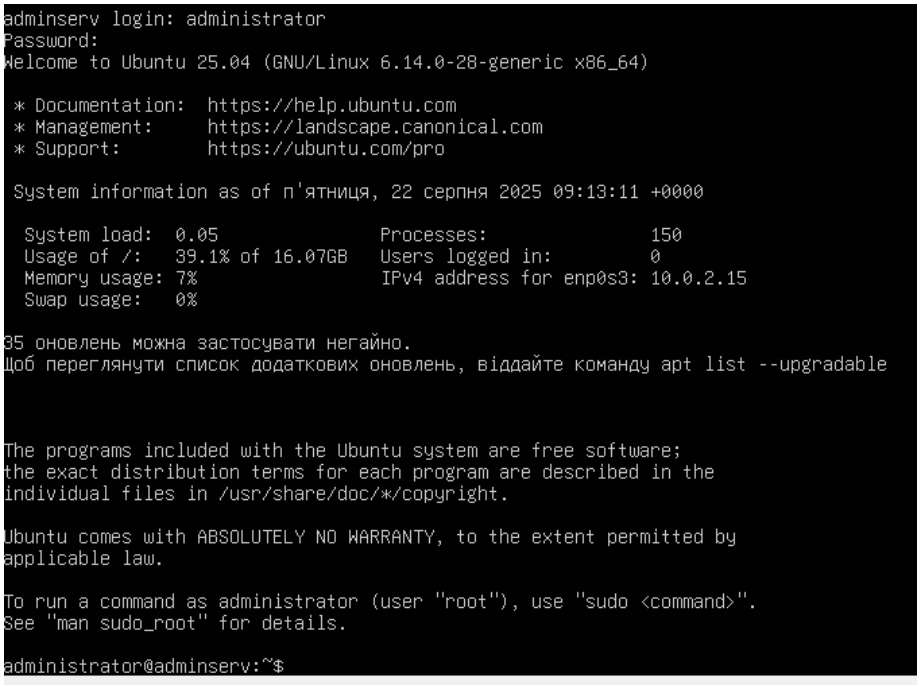

Рисунок 7.15 – Вхід в ОС Linux Server

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. 7.16).

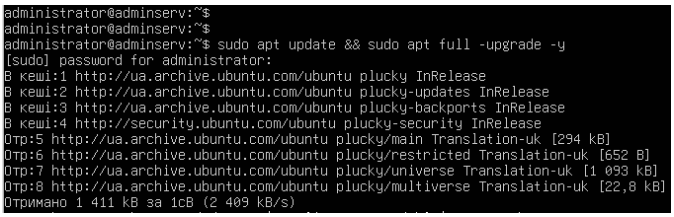

Рисунок 7.16 – Оновлення Linux Server

Далі налаштувати дату та час для сервера. Для цього ввести команду «sudo timedatectl set-timezone Europe/Kyiv» та перевірити потім командою «timedatectl» (рис. 7.17).

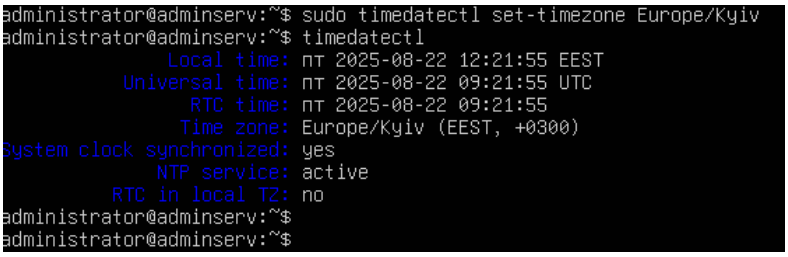

Рисунок 7.17 – Налаштування дати та часу в Linux Server

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. 7.18).

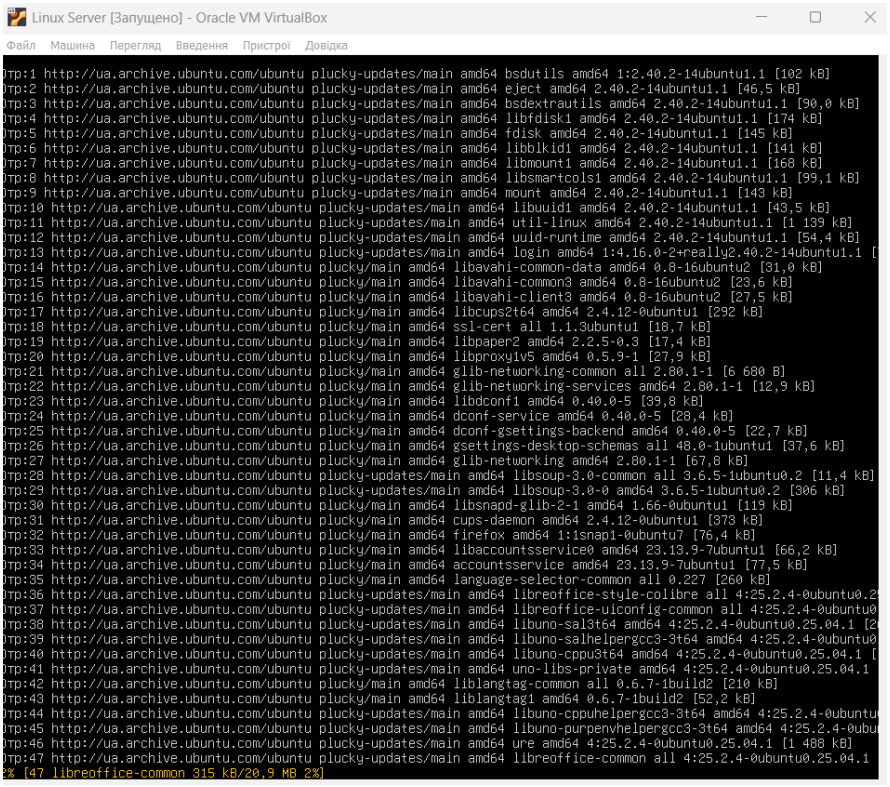

Рисунок 7.18 – Процес встановлення графічного інтерфейсу для Linux Server

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. 7.19).

```
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 7.19 – Команда для автоматичного відкриття графічного інтерфейсу

Після перезавантаження система запускається в графічному режимі, отже налаштування здійснені успішно (рис. 7.20).

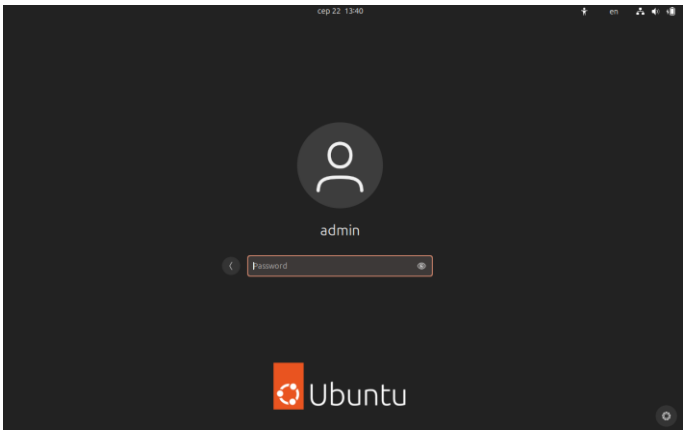

Рисунок 7.20 – Запуск системи Linux Server у графічному режимі роботи

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. 7.21).

```
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 7.21 – 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. 7.22).

```
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 7.22 – 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. 7.23).

```
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 7.23 – 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. 7.24).

```
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 7.24 – 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. 7.25).

```
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 7.25 – 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. 7.26).

```
#!/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 7.26 – 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».

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курс мережевої академії Cisco Packet Tracer (Курс-інструкція до симулятору мереж та IoT). Доступний з URL: http://surl.li/mimft (дата звернення: 14.04.2025).
2. Курс Мережевої академії Cisco CCNAv7: Introduction to Networks URL: https://www.netacad.com/courses/networking/ccna-introduction-networks (дата звернення: 20.04.2025).
3. Курс Мережевої академії Cisco CCNAv7: Switching, Routing, and Wireless Essentials URL: https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials (дата звернення: 29.04.2025).
4. Networking101Lite Друга сесія «Другий (канальний) рівень OSI моделі. Ethernet. Комутація. VLAN». URL: http://surl.li/eoiuy (дата звернення: 02.05.2025).
5. Networking101Lite Третя сесія «Третій (мережевий) рівень OSI моделі. IP. Маршрутизація». URL: http://surl.li/eoiuz (дата звернення: 10.05.2025)
6. Networking101Lite Сесія №9 «Динамічна маршрутизація/OSPF URL: http://surl.li/eoivq (дата звернення: 21.05.2025)
1. Windows Server 2019 Beginners Video Tutorials. URL: http://surl.li/mkrxs (дата звернення: 21.05.2025).
2. 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).
3. 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).
4. Огляд Microsoft Windows Server 2025. URL: https://softlist.com.ua/ua/news/oglyad-microsoft-windows-server (дата звернення: 21.05.2025).
5. 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).
6. 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).
7. Windows Server 2025 URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025 (date of access: 29.05.2025).
8. 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).
9. 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).

10. 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).
11. 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).
12. 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).
13. 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).
14. 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).
15. 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: 10.06.2025).
16. Ubuntu Server documentation. Ubuntu Server. URL: https://documentation.ubuntu.com/server/ (date of access: 10.06.2025).
17. 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: 10.06.2025).
18. 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: 10.06.2025).

І-74 Інформаційні мережі та адміністрування: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12(F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2025. 73 с.

Методичне видання до лабораторних робіт з дисципліни «Інформаційні мережі та адміністрування» складене відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 126 (F6) Інформаційні системи та технології освітньої програми «Інформаційні системи та технології охорони і безпеки».

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