ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»
протокол від __ червня 2026 р.
№__

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення лабораторних занять з навчальної дисципліни
«АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ»
для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальностей галузі знань 12 «Інформаційні технолології»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Рекомендовано на засіданні
кафедри комп'ютерної інженерії
та кібербезпеки
11 травня 2026 р., протокол № _

Розробники:
кандидат педагогічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки
Олена Головня
старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Ігор Фальковський

Житомир
2026

УДК 004.45:004.7

Рекомендовано до друку науково-методичною радою
Державного університету “Житомирська політехніка”
(протокол №__ від __ червня 2026 року)

Рецензенти:

Ю. П. Кльоц – кандидат технічних наук, доцент, завідувач кафедри кібербезпеки, Хмельницький національний університет

А. А. Єфіменко – кандидат технічних наук, доцент, завідувач кафедри комп’ютерної інженерії та кібербезпеки, Державний університет «Житомирська політехніка»

Методичні рекомендації для виконання лабораторних робіт з навчальної дисципліни «Адміністрування комп'ютерних систем та мереж» для здобувачів освіти освітнього ступеня «бакалавр» галузі знань 12 «Інформаційні технології / підг. О. С. Головня, І. Г. Фальковський – Житомир : Державний університет “Житомирська політехніка”, 2026. – 153 с.

Методичні рекомендації містять інструкції до виконання лабораторних робіт з навчальної дисципліни “Адміністрування комп’ютерних систем та мереж”. Методичні рекомендації присвячено основам адміністрування мереж на базі Windows Server 2022 та служби каталогів Active Directory (встановлення ОС; розгортання Active Directory; створення структури домену; налаштування групових політик; конфігурування DNS, DHCP і реплікації; використання PowerShell; налаштування служб віддаленого доступу, друку, квотування та веб-сервера IIS; інтеграція з Ubuntu Server і організація обміну файлами за протоколом SMB). Лабораторні роботи супроводжуються прикладами та рекомендаціями щодо використання інструментів адміністрування. Методичні рекомендації адресовано здобувачам освіти спеціальностей галузі знань 12 “Інформаційні технології”.

Підготували: О. С. Головня, І. Г. Фальковський.

УДК 004.45:004.7

ЗМІСТ

Вступ

Дані методичні рекомендації розроблено відповідно до програми навчальної дисципліни “Адміністрування комп’ютерних систем та мереж” для здобувачів освіти галузі знань 12 “Інформаційні технології”. Це видання також може використовуватися для проведення лабораторних робіт з інших подібних дисциплін під час вивчення практичних аспектів адміністрування комп’ютерних мереж із кінцевими вузлами під управлінням ОС Windows.

До методичних рекомендацій увійшли лабораторні роботи, присвячені основам адміністрування комп’ютерних систем і мереж на базі Windows Server 2022 та служби каталогів Active Directory (встановлення операційної системи; розгортання Active Directory; створення структури домену; налаштування групових політик; конфігурування DNS-, DHCP-служб і реплікації; використання PowerShell; налаштування служб віддаленого доступу, друку, квотування та веб-сервера IIS; інтеграція з Ubuntu Server і організація обміну файлами за протоколом SMB).

Ці методичні рекомендації мають наступні особливості.

- ✓ **Використані операційні системи.** Використовуються ОС Windows Server 2022 для налаштувань домену Active Directory, Windows настільних редакцій для робочих станцій а також Ubuntu Server 24.04 LTS.
- ✓ **Засоби віртуалізації комп’ютерних систем та мереж**. Комп’ютерні мережі, які будуються у лабораторних роботах, розраховані на моделювання в емуляторі GNS та гіпервізорі Oracle VirtualBox. У разі обмеженого обсягу ресурсів, можуть бути реалізовані засобами виключно віртуальних мереж Oracle VirtualBox.
- ✓ **Вимоги до вмісту звіту.** Кожне завдання містить вказівки про те, які саме результати мають відображатися у звітах**.**
- ✓ **Приклади.** Теоретичні відомості до лабораторних робіт супроводжуються прикладами оснащень, команд, їх виводів тощо.

Методичні рекомендації адресовано здобувачам освіти, які вивчають адміністрування комп’ютерних систем та мереж, викладачам закладів вищої освіти та всім, хто цікавиться моделюванням Windows-мереж.

Робота № 1.Встановлення ОС Windows Server

Мета: навчитися здійснювати базове встановлення ОС Windows Server 2022 Standard (Desktop Experience) на віртуальну машину.

Інструменти: гіпервізор VirtualBox, інсталяційний образ ОС Windows Server 2022.

Завдання до лабораторної роботи Засобами гіпервізора VirtualBox створіть нову віртуальну машину.

※ Ім'я віртуальної машини має відповідати наступному формату:

Srv -*GG*-*VV*

де *GG* - номер вашої групи, *VV* – ваш варіант. Варіант – значення у першій колонці рейтингової таблиці.

※ Вказуючи дисковий розділ, на якому зберігатимуться файли віртуальної машини, обов'язково переконайтеся, що на обраному вами розділі достатньо вільного місця.

※ Обсяг оперативної пам'яті, виділений віртуальній машині, - принаймні 3 Гб, 1 core CPU.

Підключіть до створеної віртуальної машини інсталяційний образ ОС Windows Server (iso-файл). Підключення виконуйте на місце віртуального оптичного приводу.

Виконайте встановлення ОС Windows Server на створену віртуальну машину.

※ Редакція - Windows Server 2022 Standard (Desktop Experience)

※ Тип інсталяції - *Custom* (не *Update*)

※ Дискові розділи можна поки лишити без змін

※ Пароль для адміністратора - на власний розсуд, але має відповідати базовим вимогам:

- Мінімальна довжина — 8 символів.
- Складність пароля має бути увімкнена:
  - ✓ принаймні одна велика літера (A–Z);
  - ✓ принаймні одна мала літера (a–z);
  - ✓ принаймні одна цифра (0–9);
  - ✓ принаймні один спеціальний символ (напр., !, @, #, $, тощо).

Від'єднайте інсталяційний образ (iso-файл) від віртуального оптичного приводу віртуальної машини.

Після завершення встановлення переконайтеся у працездатності системи.

Звіт має містити: скриншоти основних кроків виконання встановлення ОС Windows Server

Активація та ліцензування Windows Server

Після встановлення Windows Server 2022 операційна система працює у режимі ознайомчого (evaluation) використання. Для редакції Windows Server 2022 Standard (Desktop Experience) за замовчуванням надається пробний період тривалістю 180 днів. У цей період:

- ✓ система повністю функціональна;
- ✓ обмеження продуктивності відсутні;
- ✓ доступні всі базові ролі та можливості сервера;
- ✓ активація продукту не є обов'язковою для виконання лабораторних робіт.

Після завершення пробного періоду система починає регулярно повідомляти про необхідність активації.

У навчальному середовищі дозволяється обмежене подовження evaluation-періоду за допомогою системного скрипта slmgr.vbs (Software Licensing Management Tool). slmgr.vbs — це вбудований у Windows скрипт керування ліцензуванням, який використовується для:

- ✓ перегляду стану активації;
- ✓ введення ключів продукту;
- ✓ керування службою ліцензування;
- ✓ подовження evaluation-періоду.

Для подовження пробного періоду використовується команда (у командному рядку від імені адміністратора):

slmgr.vbs /rearm

Після виконання команди необхідно перезавантажити сервер.

Кожне виконання /rearm подовжує ознайомчий період ще на 180 днів. У редакції Windows Server 2022 Standard зазвичай доступно дві операції rearm, що дозволяє збільшити сумарний термін evaluation до 540 днів (180 + 180 + 180).

Кількість доступних повторних активацій обмежена системою ліцензування. У production-середовищі сервер повинен бути активований відповідно до придбаної ліцензії (Retail, Volume Licensing, KMS тощо).

Корисні посилання

Системні вимоги до Windows Server 2022 Base (Desktop Experience):
https://docs.microsoft.com/en-us/windows-server/get-started/hardware-requirements
Microsoft Evaluation Center
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022

Робота №2. Встановлення служби каталогів Active Directory у Windows Server 2022

Мета: навчитися налаштовувати контролер домену Active Directory на базі Windows Server 2022.

Інструменти: гіпервізор VirtualBox, (за потреби) мережний емулятор GNS3, модель комп'ютерної мережі, що будується у відповідності до варіанту завдання.

Теоретичні відомості

Опишемо основні кроки, потрібні для розгортання контролера домену Active Directory на основі Windows Server 2022.

Створюємо схему адресації, яка відповідає схемі (рис. 2.1) та таблиці 2.2.

Для прикладу використаємо схему адресації для мережі 192.168.40.240/28 , яка подана у таблиці 2.1.

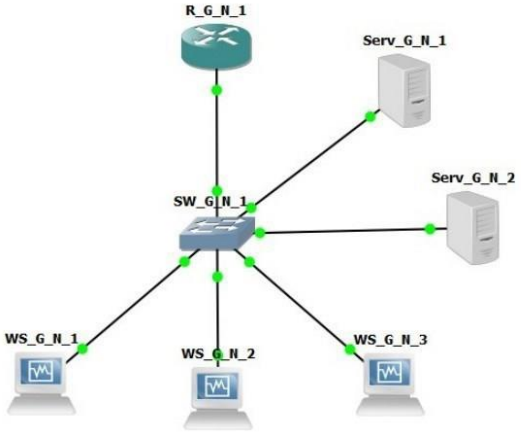


Рис. 2.1. Топологія мережі

Таблиця 2.1

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс / Мережний адаптер / Шлюз	IP-адреса	Маска	Префікс
Мережа A	-	192.168.40.240	255.255.255.240	/28
Маршрутизатор R_19_30_1 або резерв NAT Network VirtualBox	Eth1/0	192.168.40.241	255.255.255.240	/28
Комутатор SW_19_30_1 або резерв NAT Network VirtualBox	Інтерфейс Vlan 1	192.168.40.242	255.255.255.240	/28
Сервер Serv_22_40_1	Мережний адаптер	192.168.40.243	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.40.241	-	-
Сервер Serv_22_40_2	Мережний адаптер	192.168.40.244	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.40.241	-	-
Робочі станції WS_22_40_1 - WS_22_40_3	Мережний адаптер	DHCP	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.40.241	-	-

Створюємо в Oracle VirtualBox дві віртуальні машини Windows Server 2022, як у лабораторній роботі №1. Імена віртуальних машин та серверів (під серверами маються на увазі імена віртуальних

хостів) – відповідно до топології мережі (рис. 2.1. Serv_G_N_1 та Serv_G_N_2). Можливо використати, створену у лабораторній роботі №1 віртуальну машину Windows Server 2022 у якості одного з серверів.

Важливо. Імена серверів та робочих станцій у домені мають відповідати умовам завдання.

Налаштовуємо ip-адреси та підключення серверів відповідно до створеної схеми адресації та реалізації роботи. Дозволяємо на обох серверах вхідний icmp v4 трафік. Для цього обираємо ***[Local Server][Windows Defender Firewall]-[Advanced Settings]-[Inbound Rules]-[File and Printer Sharing (Echo Request ICMP v4 In)]*** (рис. 2.2).

Рис. 2.2. Налаштування правила для вхідного трафіку за ICMP-v4

Якщо ви будуєте модель мережі лише у VirtualBox, **без використання GNS,** то в Oracle VirtualBox налаштовуємо параметри підключення до мережі для обох серверів як NAT Network, Internal Network або Host-Only adapter (рис. 2.3). Використання NAT Network – найбільш універсальний метод.
Якщо ви будуєте модель мережі у GNS та VirtualBox, то для серверів можна лишити віртуальний адаптер за замовчуванням – маршрутизація налаштовується на GNS3.

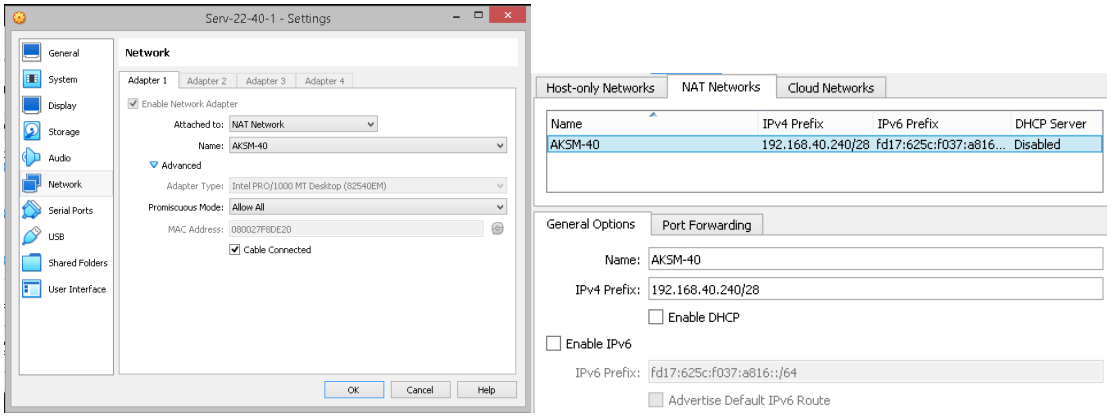


Рис. 2.3. Налаштування віртуального адаптера VirtualBox та мережі NAT Network (для моделі мережі, побудованої у VirtualBox без використання GNS)

Перевіряємо можливість інформаційного обміну між серверами (ping, rpcping, tracert).

На сервері Serv_G_N_1 в налаштуваннях мережі вказуємо у якості DNS адресу loopback 127.0.0.1.

Додаємо ролі AD DS та DC через меню ***[Dashboard][Add roles and features]*** Ім'я домену верхнього рівня - **surname.net**, де *surname* - ваше прізвище транслітом. Основні кроки налаштування цих ролей показано на рис. 2.4-2.13.

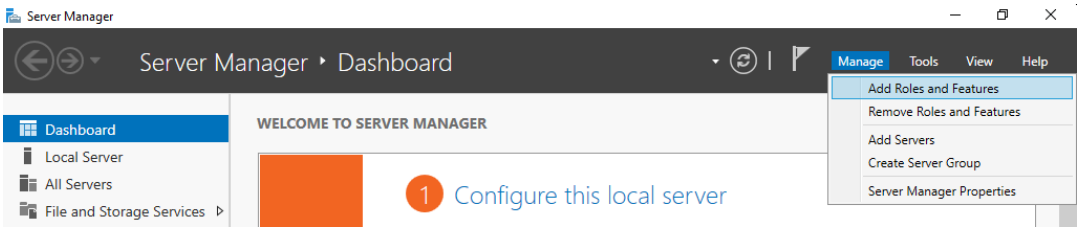


Рис. 2.4. Налаштування ролей на контролері домену (крок 1)

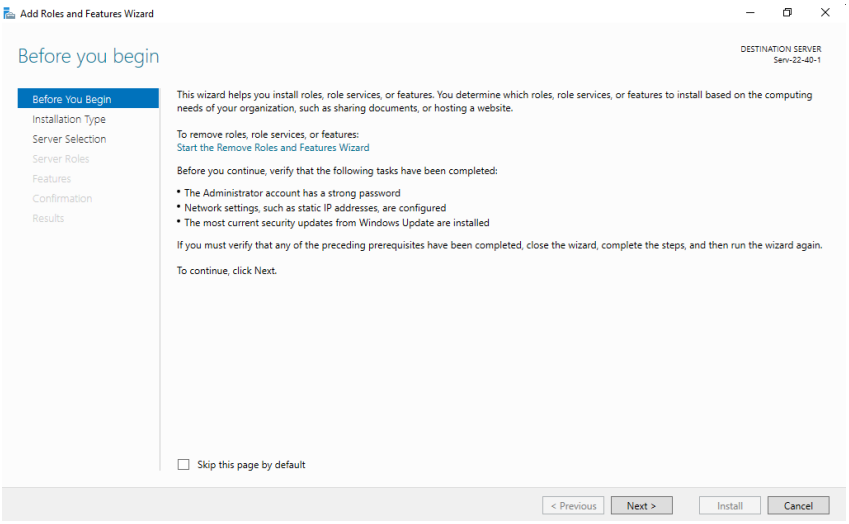


Рис. 2.5. Налаштування ролей на контролері домену (крок 2)

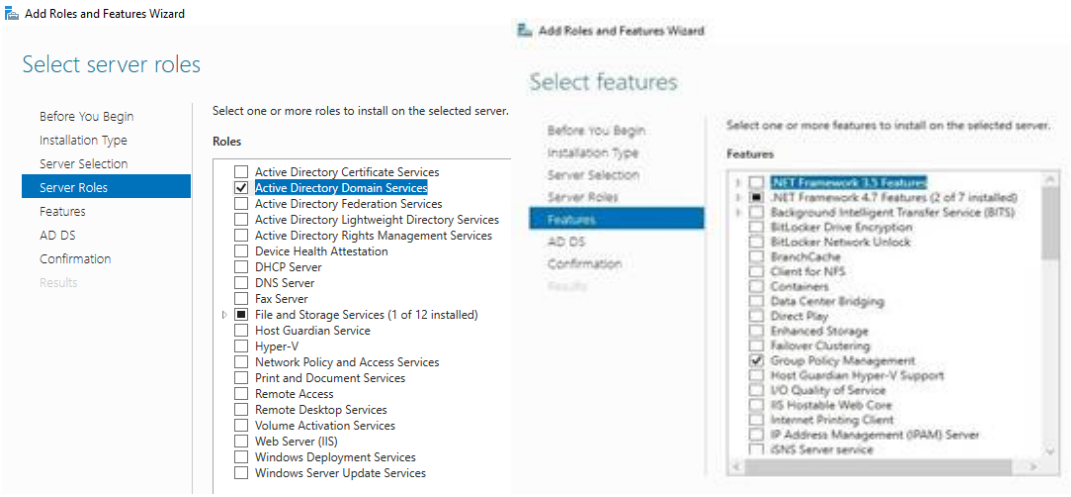


Рис. 2.6. Налаштування ролей на контролері домену (крок 3)

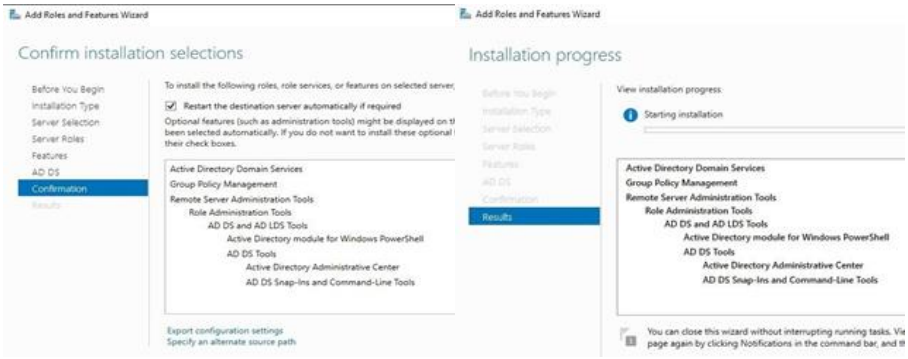


Рис. 2.7. Налаштування ролей на контролері домену (крок 4)

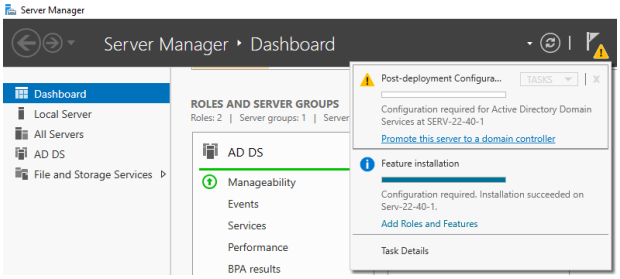


Рис. 2.8. Налаштування ролей на контролері домену (крок 5)

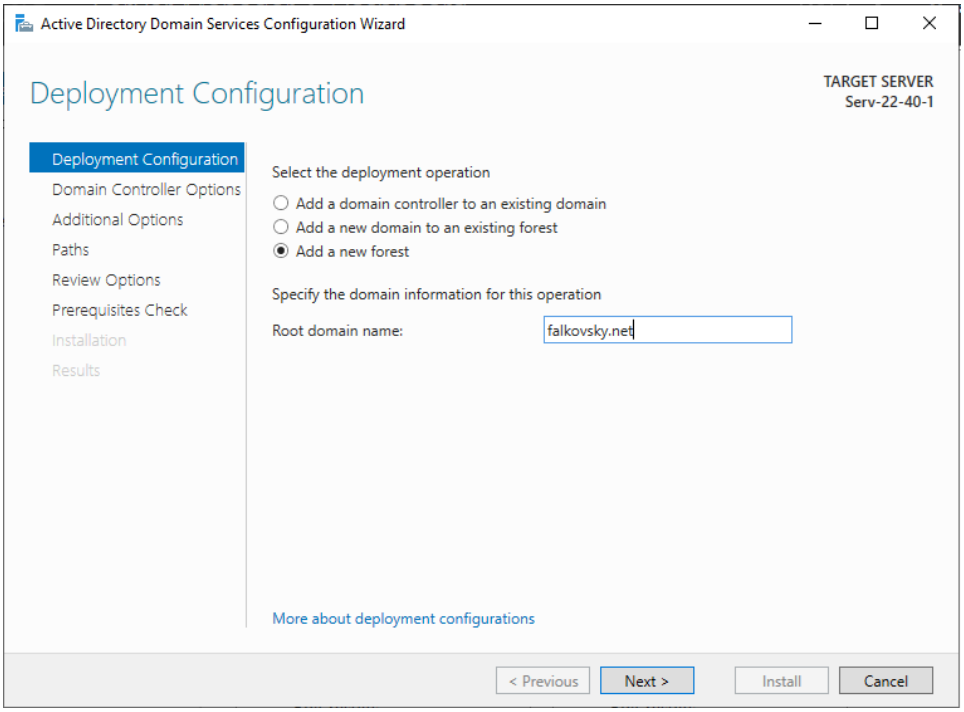


Рис. 2.9. Налаштування ролей на контролері домену (крок 6)

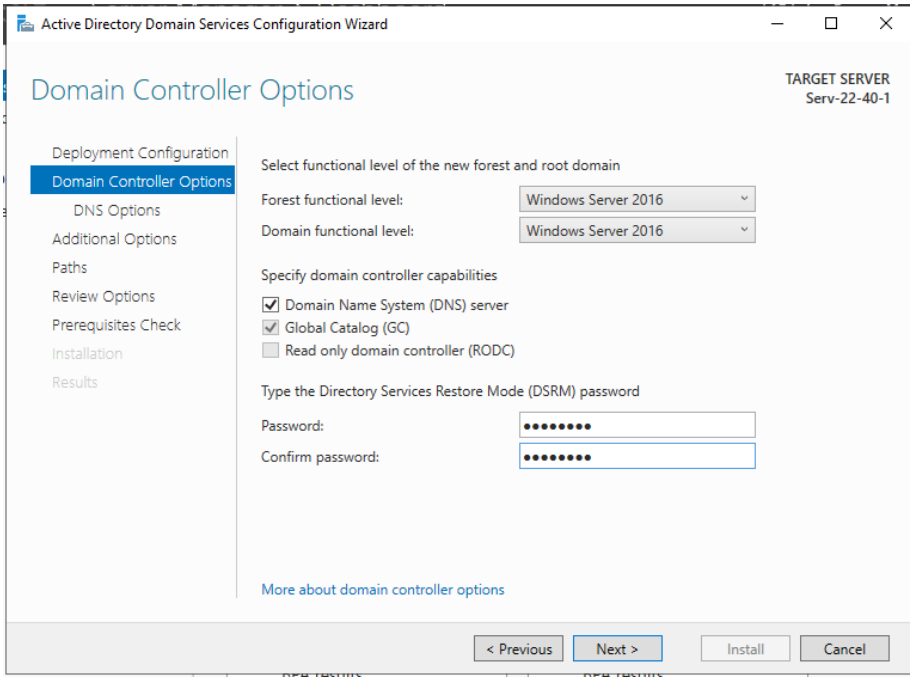


Рис. 2.10. Налаштування ролей на контролері домену (крок 7)

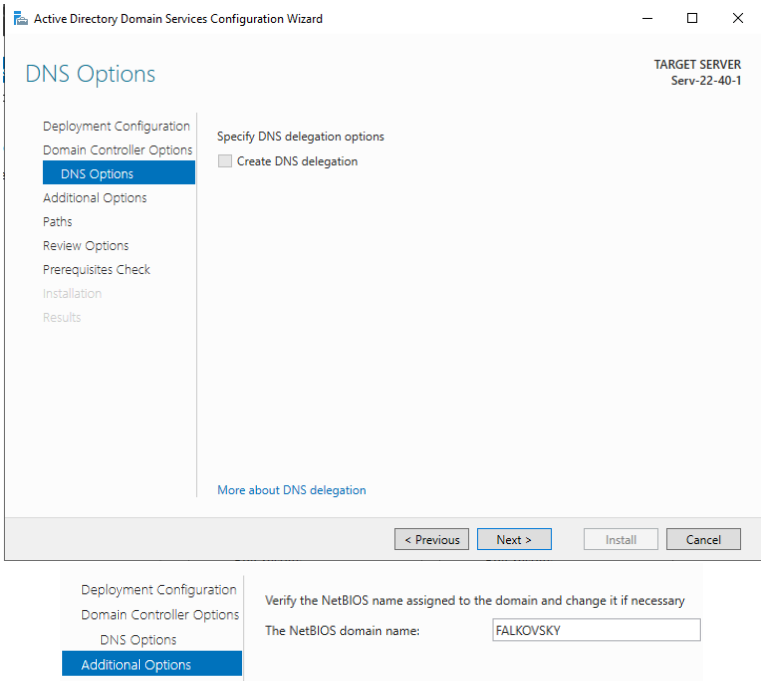


Рис. 2.11. Налаштування ролей на контролері домену (крок 8)

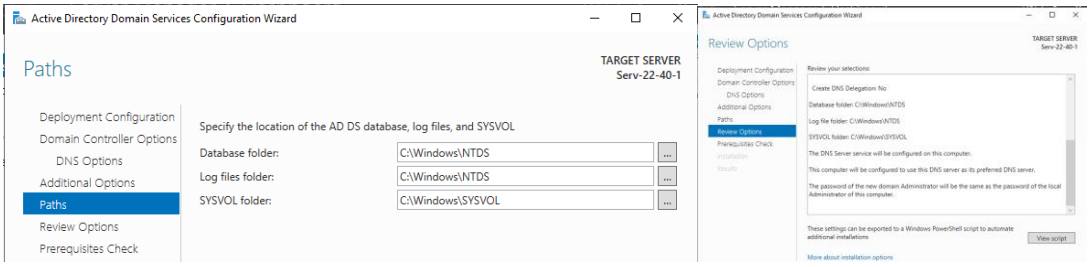


Рис. 2.12. Налаштування ролей на контролері домену (крок 9)

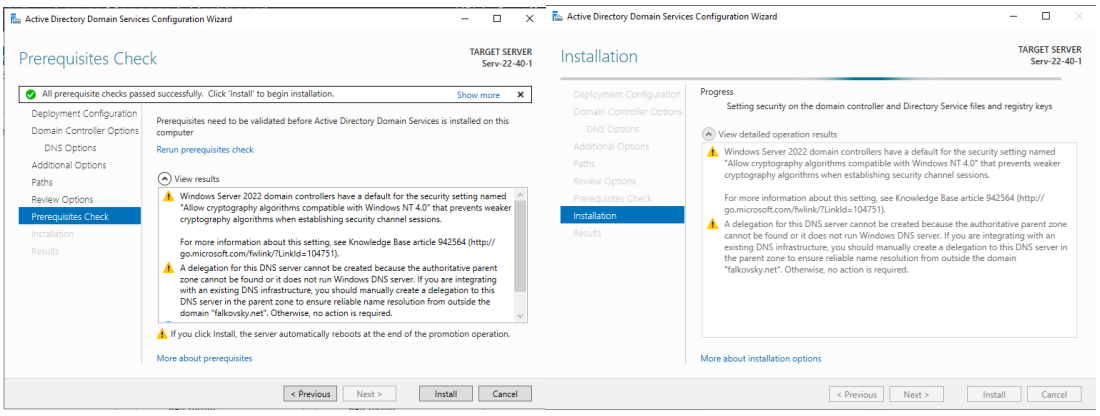


Рис. 2.13. Налаштування ролей на контролері домену (крок 10)

Вказуємо на сервері **Serv_G_N_2** у якості DNS в налаштуваннях мережі IPv4 адресу **Serv_G_N_1**

Перевіряємо зв’язок та дієздатність DC-серверу на обох серверах командою

nslookup surname.net

Додаємо у домен **Serv_G_N_2** та надаємо йому роль додаткового DC. Щоб зробити другий сервер додатковим контролером домену, на ньому також потрібно встановити роль Active Directory

Domain Services, але на етапі вибору конфігурації розгортання (Deployment Configuration) замість *Add to a new forest* (рис.2.9) обрати *Add a domain controller to an existing domain.* У якості облікових даних адміністратора домену ***surname.net*** при включенні серверу чи робочої станції до домену ***surname.net*** можливе використання двох типів рядків:

surname.net\Administrator або ***Administrator@surname.net***

Вказівки

- Імена комп'ютерів на першому і другому сервері мають відрізнятися та відповідати іменам у таблиці адресації,що ви створюєте у відповідності до завдання. (у домені імена комп'ютерів не можуть повторюватися!)
- MAC-адреси віртуальних машин з серверами мають відрізнятися.
- На другому сервері у налаштуваннях IPv4 змінюємо адресу DNS сервера на адресу вашого першого сервера (DC-servers).

Створюємо ВМ **WS_G_N_1** відповідно до завдання. ОС ВМ – Windows 10 (за потреби можна використати одну з попередніх настільних версій Windows).

Включаємо **WS_G_N_1** до домену *surname.net*. Створюємо на першому контролері домену тестову групу користувачів **GR_G_N**, а в ній - нового користувача. Перевіряємо, чи вдається ввійти у систему робочої станції під новоствореним обліковим записом.

Завдання до лабораторної роботи

1. У середовищі програмного емулятора створіть проект комп'ютерної мережі (рис. 2.1).

2. Розробіть схему адресації пристроїв мережі. Для цього скористайтеся даними табл. 2.2. Під час розрахунку враховуйте, що для схеми використовується мережа /28 задана у таблиці 2.2.

Таблиця 2.2

Параметри для розрахунку у завданні №2.2

№ варіанта(N)	IP-адреса мережі	№ варіанта(N)	IP-адреса мережі	№ варіанта(N)	IP-адреса мережі
1	192.168.N.32/28	13	192.168.N.32/28	25	192.168.N.32/28
2	192.168.N.48 /28	14	192.168.N.48 /28	26	192.168.N.48 /28
3	192.168.N.64/28	15	192.168.N.64/28	27	192.168.N.64/28
4	192.168.N.80/28	16	192.168.N.80/28	28	192.168.N.80/28
5	192.168.N.96/28	17	192.168.N.96/28	29	192.168.N.96/28
6	192.168.N.112/28	18	192.168.N.112/28	30	192.168.N.112/28
7	192.168.N.128/28	19	192.168.N.128/28	31	192.168.N.128/28
8	192.168.N.144/28	20	192.168.N.144/28	32	192.168.N.144/28
9	192.168.N.160/28	21	192.168.N.160/28	33	192.168.N.160/28
10	192.168.N.176/28	22	192.168.N.176/28	34	192.168.N.176/28
11	192.168.N.192/28	23	192.168.N.192/28	35	192.168.N.192/28
12	192.168.N.208/28	24	192.168.N.208/28	36	192.168.N.208/28

3. Перевірте можливість інформаційного обміну між хостами мережі. У разі виявлення проблем зв'язку знайдіть та усуньте їх причини.

4. На сервері Serv_G_N_1 проведіть встановлення Active Directory, а сервер Serv_G_N_2 додайте у домен та надайте йому роль додаткового контролеру домену. Ім'я домену верхнього рівня - *surname*.net, де *surname* - ваше прізвище.

Примітка. На сервері Serv_G_N_2 також потрібно встановити роль *Active Directory Domain Services*, але на етапі вибору конфігурації розгортання (Deployment Configuration) замість *Add to a new forest* вибрати *Add a domain controller to an existing domain*.

5. Додайте у домен робочі станції. У разі браку ресурсів рекомендовано під'єднати меншу кількість робочих станцій, ніж у розробленій вами схемі адресації. Однієї робочої станції буде достатньо.

6. На сервері Serv_G_N_1 в Active Directory створіть тестову групу користувачів GR_G_N. В цій групі створіть нового користувача та, використовуючи цей обліковий запис, здійсніть вхід у систему з робочої станції.

Звіт має містити:
- схему адресації мережі;
- скриншоти та короткий опис основних кроків створення структури домену та перевірки можливості входу з-під одного з новостворених облікових записів.

Корисні посилання

Посібник з Active Directory для початківців
https://corewin.ua/blog/active-directory-delegation-tutorial-for-beginners/

Setting up Active Directory in VirtualBox
https://surl.lu/knqabf
https://surl.li/rolpkp

How To Enable Ping In Windows Server 2022 Firewall
https://www.rootusers.com/how-to-enable-ping-in-windows-server-2022-firewall/

Робота №3. Створення структури домену в Active Directory у Windows Server 2022

Мета: навчитися будувати структуру домену з одним деревом в Active Directory на базі Windows Server 2022.
Інструменти: гіпервізор VirtualBox, (за потреби) мережний емулятор GNS3, модель комп'ютерної мережі, побудована у межах лабораторної роботи №2.

Завдання до лабораторної роботи

1. Розробіть структурну діаграму майбутнього домену для організації.

※ Ім'я домену верхнього рівня - *surname*.net, де *surname* - ваше прізвище.

※ Тут і далі під час створення структури домену керуйтеся рекомендаціями з теми 3 "Створення структури домену в Active Directory". Зокрема, у ролі основних структурних компонентів домену використовуйте **організаційні одиниці** (Organizational Units).

※ У домені *surname*.net заплануйте три організаційні одиниці, кожна з яких відповідає окремому філіалу організації. Відповідні організаційні одиниці (OUs) назвіть Branch-*GG*-*NN*-1, Branch-*GG*-*NN*-2 та Branch-*GG*-*NN*-3, де *GG* - номер вашої групи, *NN* - номер варіанту.

※ Всередині кожної організаційної одиниці філіалу заплануйте по 2-4 організаційні одиниці для відділів цього філіалу та по 1 організаційній одиниці для адміністраторів. Організаційні одиниці відділів назвіть Dep-*GGNN*-*Номер_філіалу*-1, Dep-*GG*-*NN*-*Номер_філіалу*-2 і т. д. Організаційні одиниці для адміністраторів назвіть самостійно, забезпечивши унікальність.

※ Всередині кожної *організаційної одиниці відділу* заплануйте щонайменше двох користувачів. Також додайте мінімум одного користувача до кожної *адміністративної організаційної одиниці.* Для іменування всіх користувачів використовуйте єдиний підхід (наприклад, такий, як показано на рис. 4.1). Ім'я кожного користувача має бути унікальним у межах домену. Додаванням користувачів до груп займемося трохи згодом.

※ Побудуйте структурну діаграму. Приклад можливої діаграми подано на рис. 3.1.

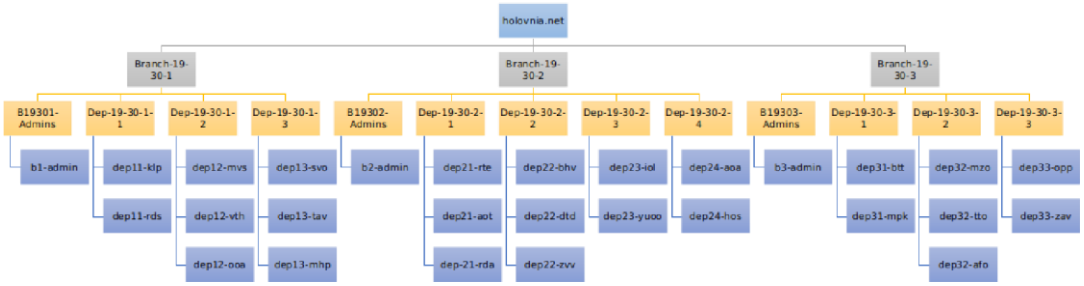


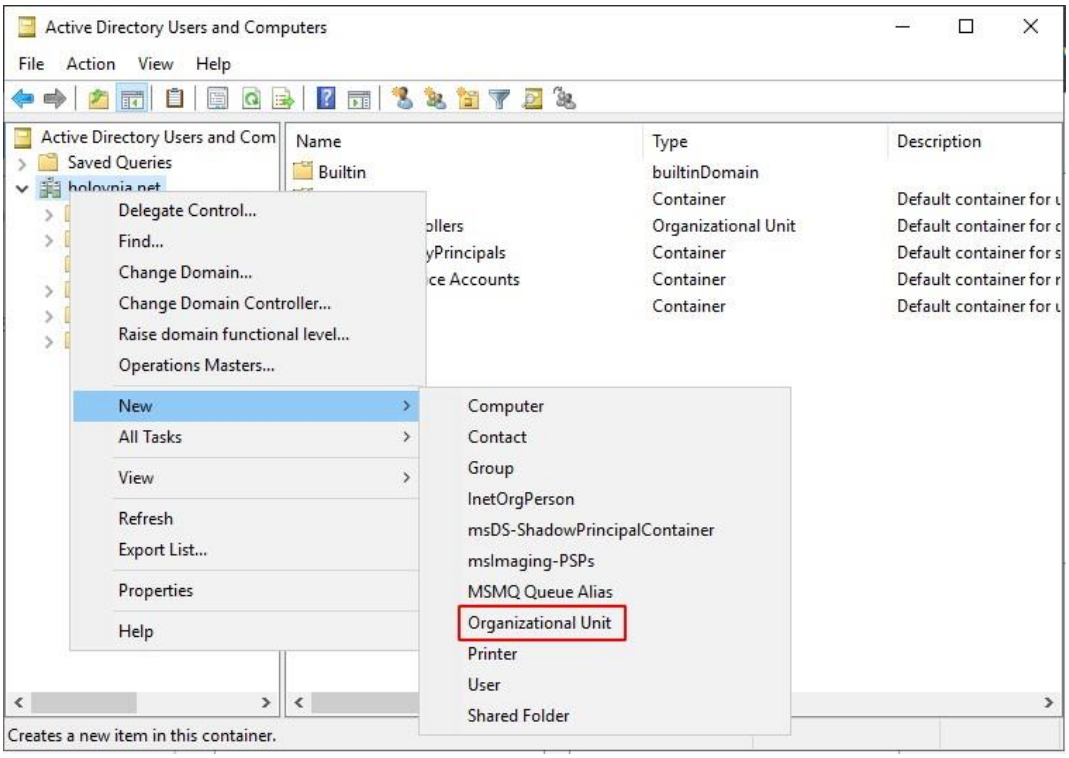
Рис. 3.1.Приклад структурної діаграми домену
(сірим і жовтим позначено організаційні одиниці)

Примітка. У межах даної лабораторної роботи всі організаційні одиниці розміщені у межах єдиного домену. Це пов'язано з обмеженими ресурсами. У разі розростання даної умовної організації можна було б створити окремі дочірні домени для філіалів. Наприклад, з іменами branch19301.holovnia.net, branch19302.holovnia.net, branch19303.holovnia.net чи, імовірно, іншими, змістовнішими іменами.

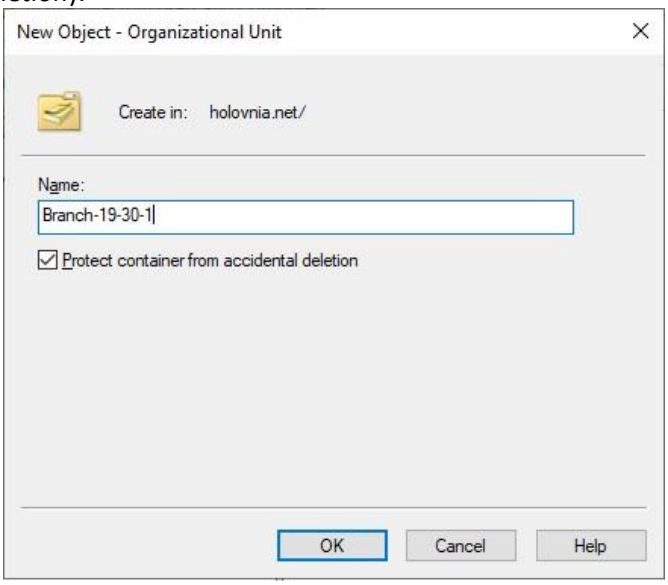
2. На контролері домену запустіть оснащення *Active Directory Users and Computers*. Створіть організаційні одиниці (Organizational Units) та користувачів (Users), які відповідають створеній вами структурній діаграмі домену.

Вказівки

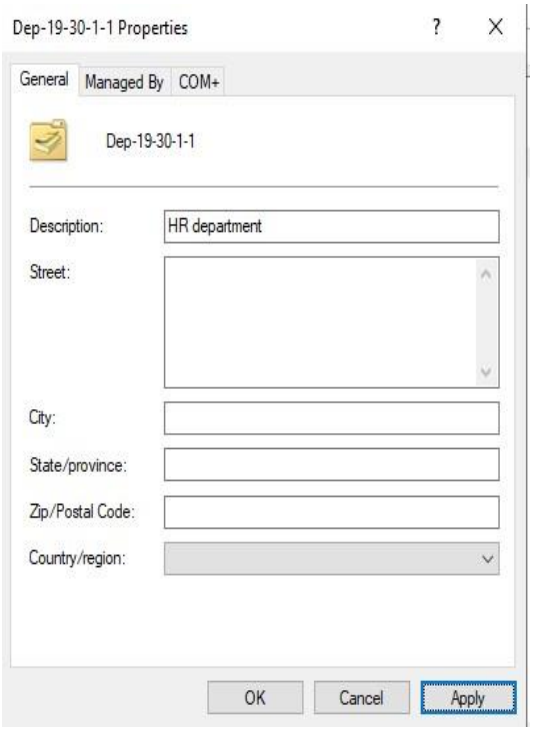
Додавання нової організаційної одиниці в домені верхнього рівня:



Обов'язково переконайтеся, що вибрано опцію захисту від випадкового видалення (*Protect container from accidental deletion*):

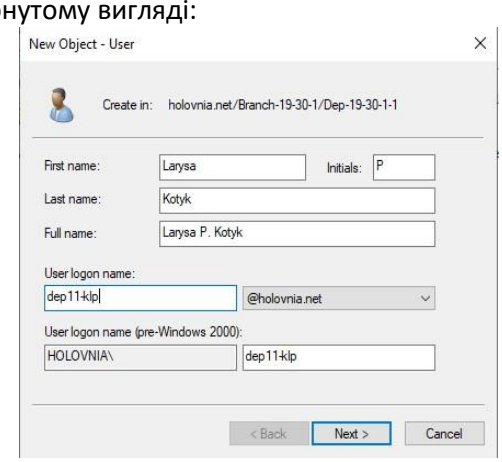


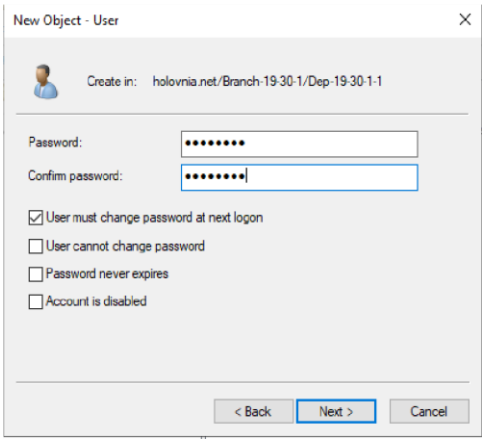
Документування організаційної одиниці для відділу (поле *Description*, порожнє за замовчуванням, заповнене):

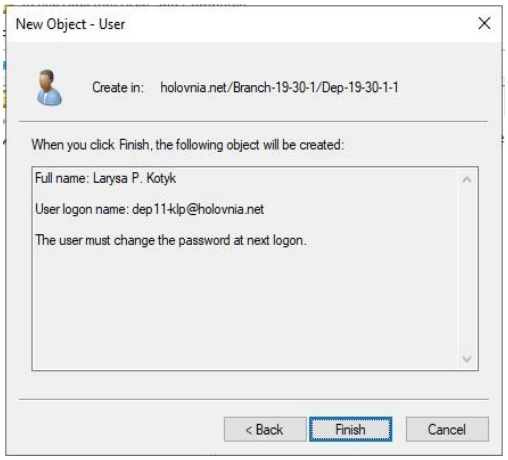


Приклад структури домену. Одну з організаційних одиниць філіалів подано у розгорнутому вигляді:

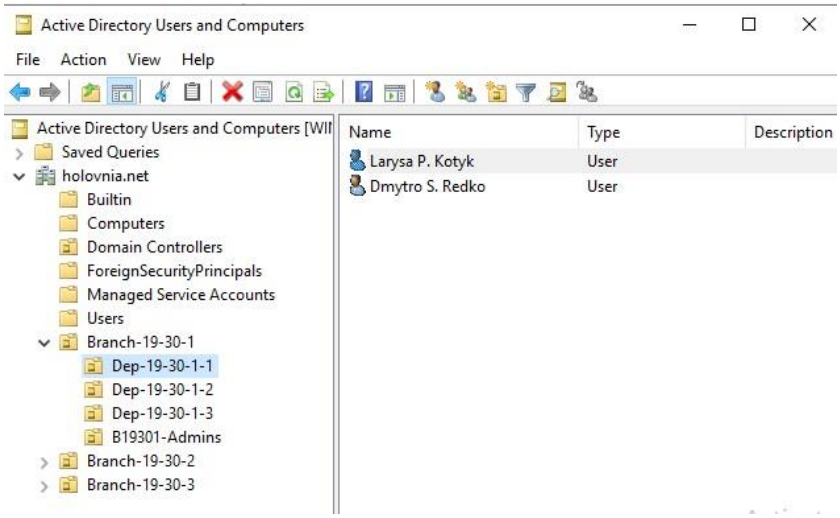
Додавання нового користувача в організаційну одиницю відділу:



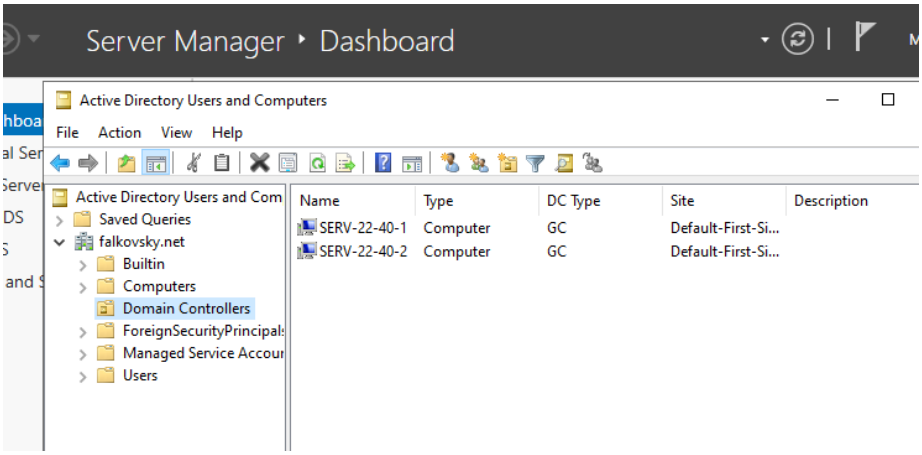




Організаційна одиниця відділу з доданими користувачами:



3. Переконайтеся, що обидва контролери домену містяться в організаційнійодиниці *Domain Controllers*:



4. Аналогічно перевірте, чи всі наявні у вас робочі станції відображаютьсявсередині групи *Computers* (зараз там має бути принаймні одна робоча станція).

5. Запустіть принаймні одну робочу станцію та принаймні один контролердомену. Здійсніть вхід з робочої станції за допомогою одного з облікових записів користувачів, створених у завданні №2.

Звіт має містити:

- структурну діаграму домену;
- скриншоти та короткий опис основних кроків створення структури домену таперевірки можливості входу з-під одного з новостворених облікових записів.

Корисні посилання

Практика:

M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020 (p. 78).

Теорія:

Orin Thomas. Windows Server 2016 Inside Out. Pearson Education, 2017 (p. 170).

Робота №4. Налаштування групових політик в Active Directory

Мета: навчитися основ роботи з груповими політиками в Active Directory (на прикладі Windows Server 2022).

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №2-3.

Теоретичні відомості та завдання до лабораторної роботи

Завдання №4.1. Аналіз групових політик на рівні домену

1. Виконайте вхід на одному з контролерів домену під обліковим записомадміністратора та запустіть оснащення *Group Policy Management* (*Server Manager → Tools → Group Policy Management*).

2. Перегляньте та проаналізуйте вкладку *Scope* об'єкту групової політики *Default Domain Policy* для вашого домену. Дайте відповідь на наступні питання.

- Яких контейнерів (сайти, домени, OU), згідно з налаштуваннями, стосується даний об'єкт групової політики?
- Яких облікових записів, груп стосується даний об'єкт групової політики?
- Які WMI-фільтри наразі діють для даного об'єкту групової політики?

3. Перегляньте та проаналізуйте повний перелік налаштувань на вкладці*Settings* об'єкту групової політики *Default Domain Policy* для вашого домену. Дайте відповідь на наступні питання.

- Скільки останніх паролів користувача зберігаються в історії паролів?
- Якою є мінімальна довжина паролю?
- Чи повинен пароль відповідати вимогам складності?
- Який максимальний термін існування паролю?
- Чи встановлене блокування облікового запису у разі помилкового введення паролю? Якщо так, після скількох невдалих спроб відбувається блокування?

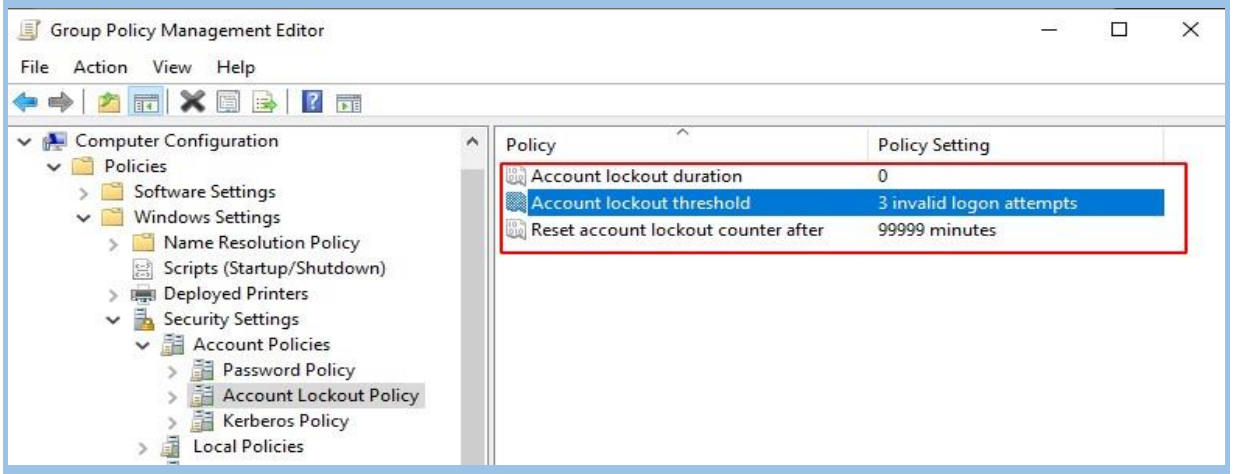
Це допоможе вам виконати наступні завдання. У дужках щодо кожної відповіді на запитання із п. 3 вкажіть вузол налаштувань, до яких належить відповідна групова політика. Наприклад: *Computer Configuration → Policies → Windows Setting → Security Settings → Account Policies/Password Policy → Minimum password length*.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Завдання №4.2

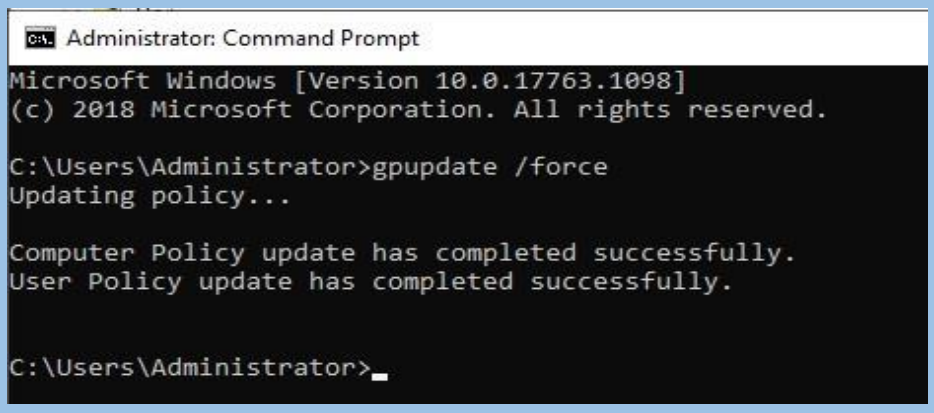
1. Спираючись на відомості, одержані вами під час виконання *завдання №6.1*, відредагуйте об'єкт групової політики *Default Domain Policy* так, щоб у межах вашого домену відбувалося блокування облікового запису після трьох підряд невдалих спроб входу, а розблокування мав робити адміністратор.

Підказка до п. 3:



2. Групові політики час від часу оновлюються автоматично (30-120 хвилин). Щоб не чекати, можна зробити наступне:

- Запустіть командний рядок на контролері домену і введіть команду gpupdate /force



- Коли оновлення групових політик на контролері домену завершиться, запустіть командний рядок на тестовій робочій станції і повторіть таку саму команду там

3. Після оновлення групових політик перевірте зроблені налаштування:

 З довільної робочої станції домену зробіть три поспіль невдалі спроби входу від імені будь-якого облікового запису і переконайтеся, що обліковий запис заблоковано.

 На контролері домену під обліковим записом адміністратора домену знайдіть заблокованого користувача у відповідній OU і розблокуйте його.

 Переконайтеся, що раніше заблокований користувач знову має можливість увійти.

Звіт має містити скриншоти зроблених налаштувань та опис основних дій.

Делегування прав на керування OU локальним адміністраторам

Етап I: Створення групи локальних адміністраторів

1) Відкрийте оснащення *Active Directory Users and Groups*.

2) У межах організаційної одиниці адміністраторів створіть нову групу локальних адміністраторів (рис. 4.1).

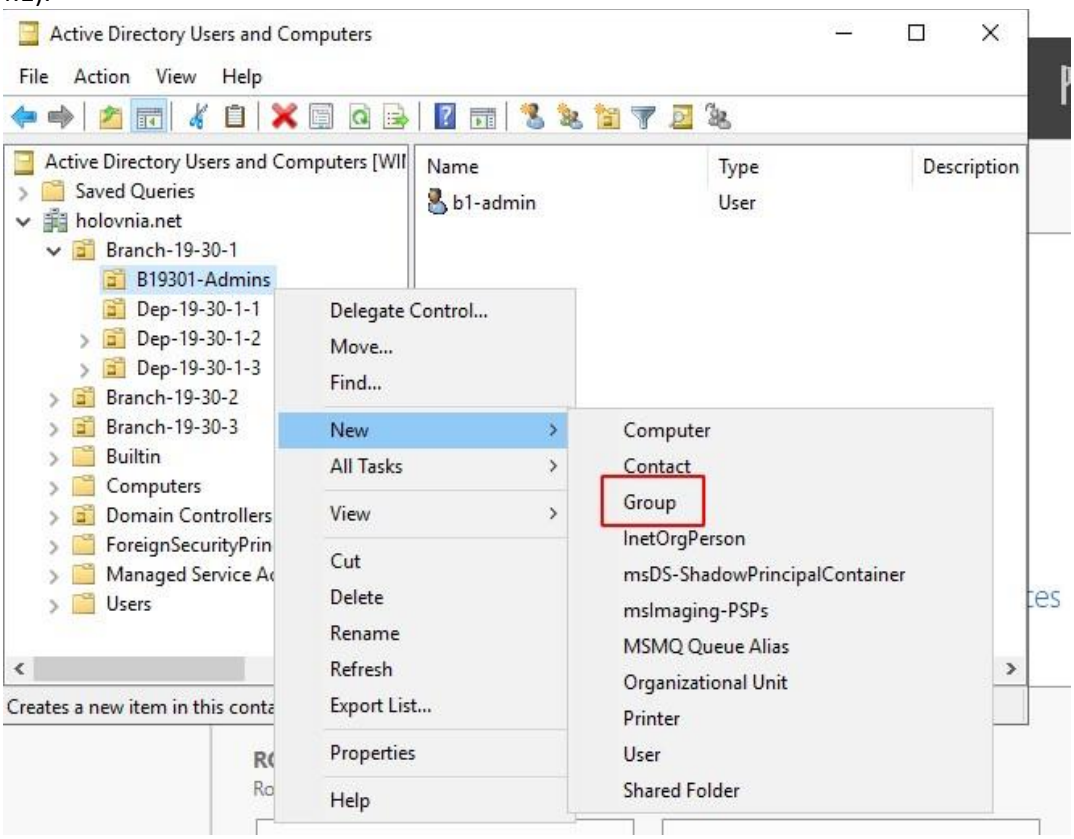


Рис. 4.1

3) Дайте групі ім’я, унікальне у межах домену. Межі дії групи - *Domain local* (рис. 4.2).

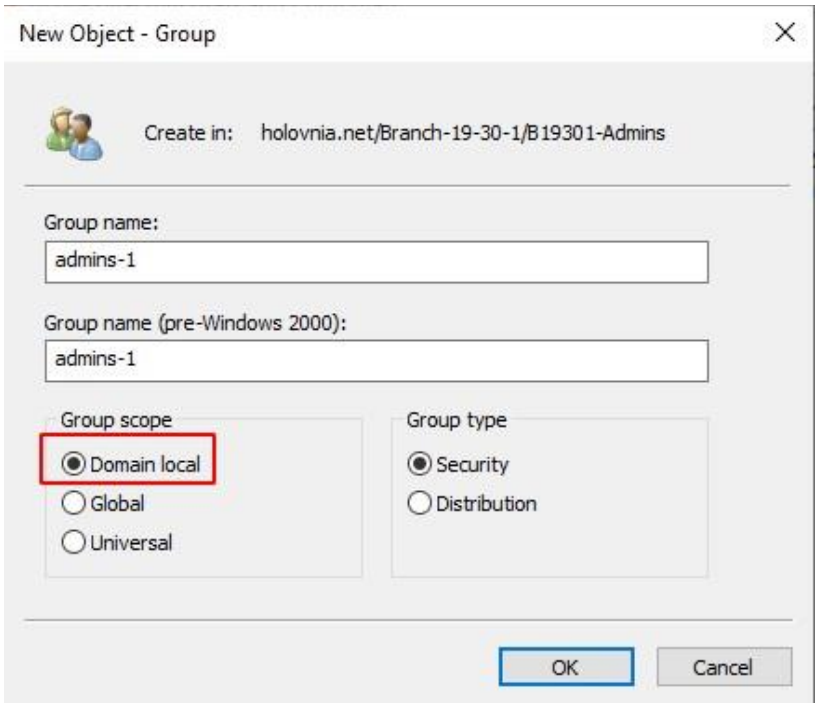


Рис. 4.2

4) Додайте наявні в даній організаційній одиниці облікові записи адміністраторів у новостворену групу (рис. 4.3).

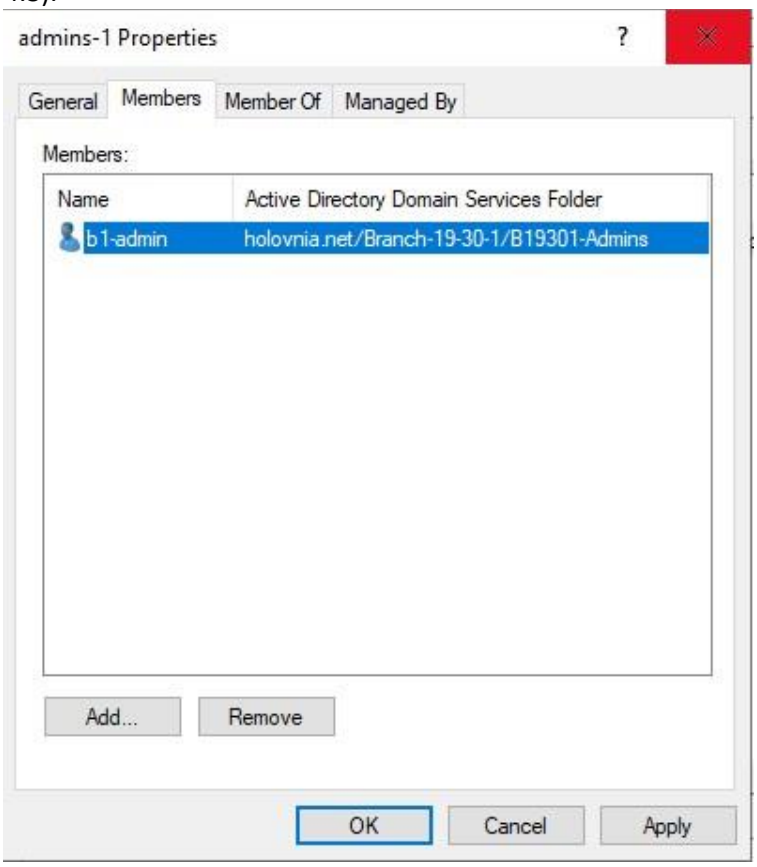


Рис. 4.3

5) Тепер у межах організаційної одиниці для локальних адміністраторів буде адміністративний обліковий запис (записи) і відповідна група (рис. 4.4).

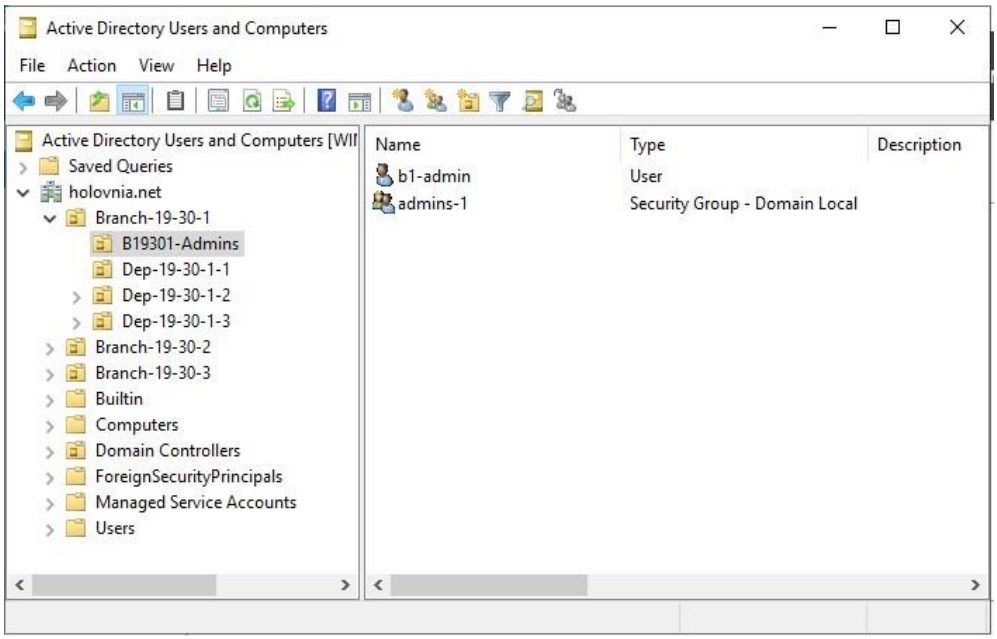


Рис. 4.4.

Етап II: Делегування групі локальних адміністраторів відповідних прав

1) Виберіть організаційну одиницю, яку мають адмініструвати члени новоствореної групи (*Branch-19-30-1* у прикладі). У контекстному меню клацніть по пункту *Delegate Control* (рис. 4.5).

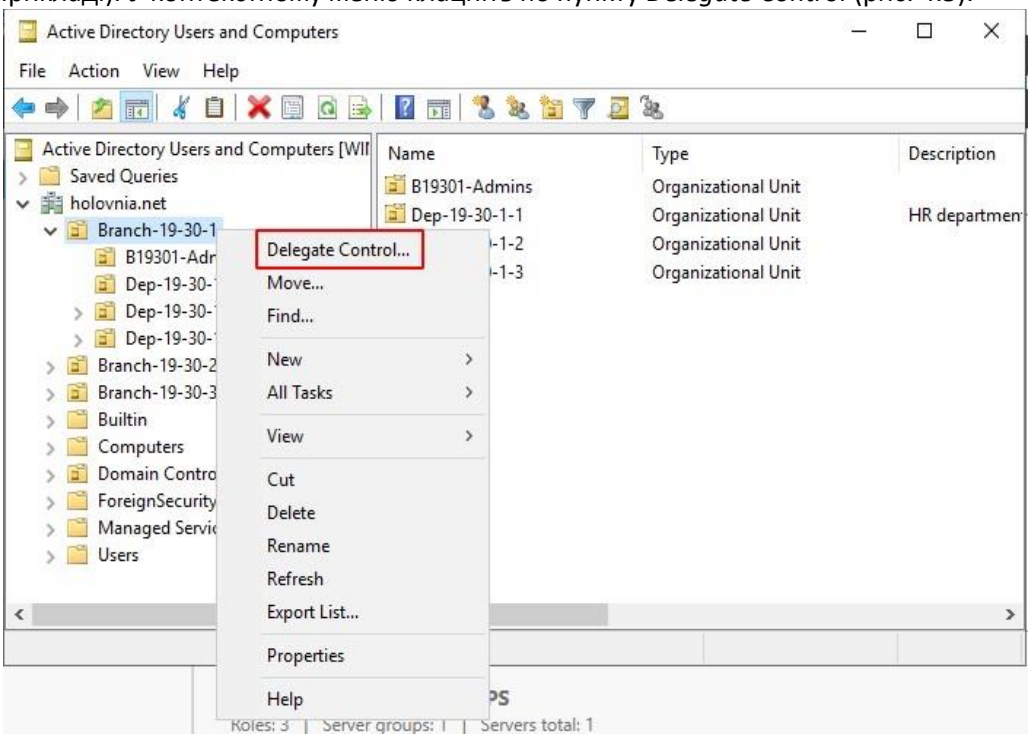


Рис. 4.5

2) Додайте до переліку користувачів та груп, яким треба делегувати контроль над цією організаційною одиницею, новостоворену групу локальних адміністраторів (рис. 4.6).

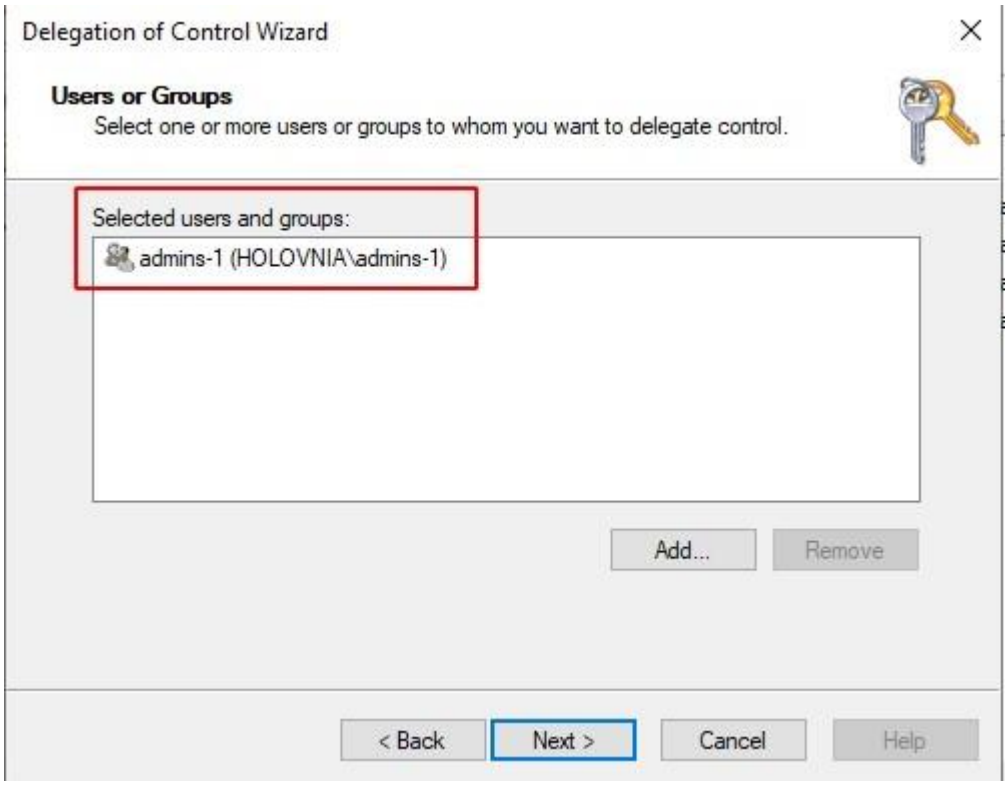


Рис. 4.6

3) Виберіть права, які треба делегувати групі. У прикладі обрано більшість адміністративних прав. Діятимуть вони лише у межах даної організаційної одиниці (рис. 4.7, рис. 4.8).

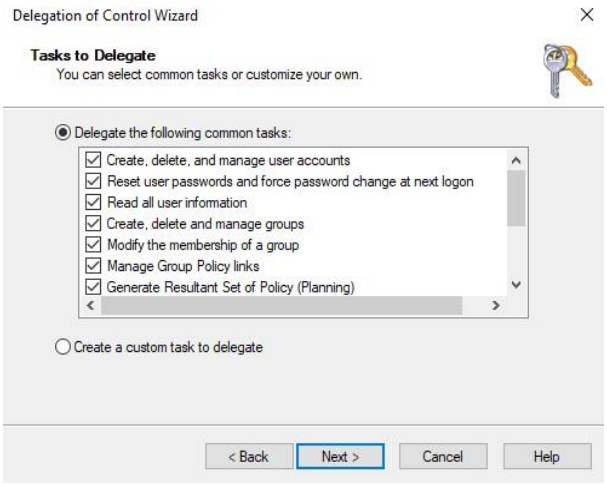


Рис. 4.7

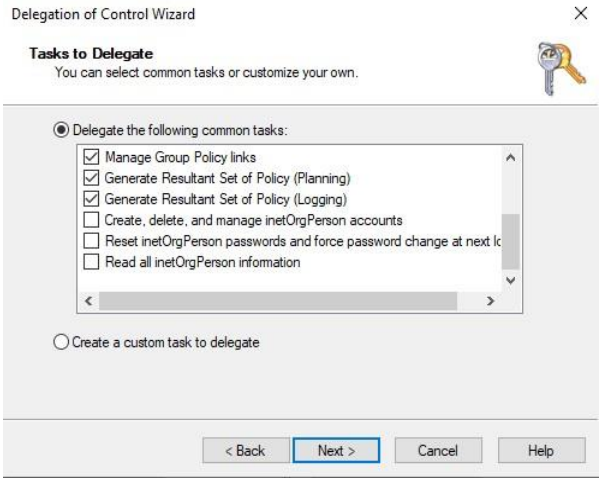


Рис. 4.8

4) Перевірте і підтвердіть зроблені налаштування (рис. 4.9).

Рис. 4.9

Етап III: Надання групі локальних адміністраторів прав на локальний вхід на DC

1) Відкрийте оснащення *Group Policy Management*.
2) Оберіть потрібний ліс, домен та організаційну одиницю. У прикладі це організаційна одиниця *Domain Controllers* всередині домену *holovnia.net* (рис. 4.10). Знайдіть об'єкт групової політики *Default Domain Controller Policy* та у його контекстному меню виберіть *Edit*.

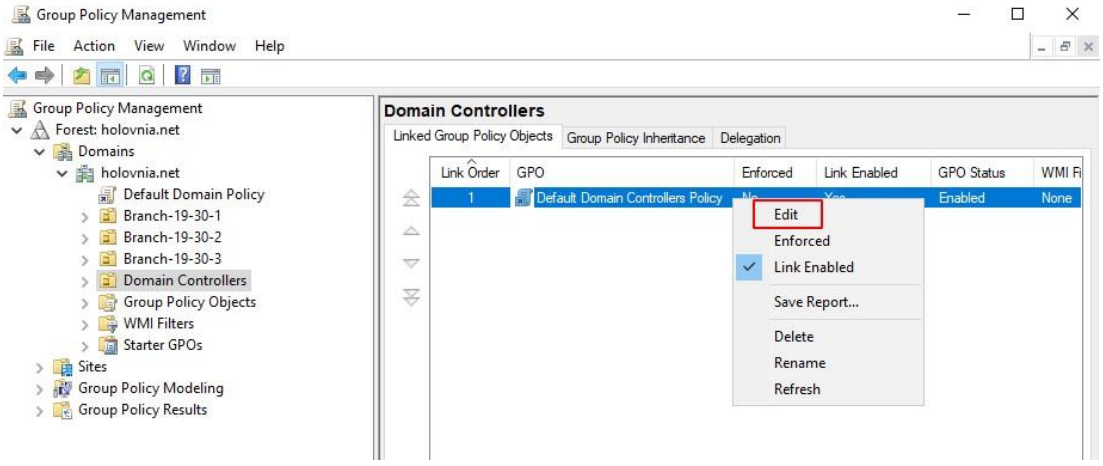


Рис. 4.10

3) Відкриється вікно *Group Policy Management Editor*. Оберіть *Computer Configuration* → *Policies* → Windows Settings → Security Settings → Local Policies → User Right Assingment та двічі клацніть по політиці Allow log on locally (рис. 4.11).

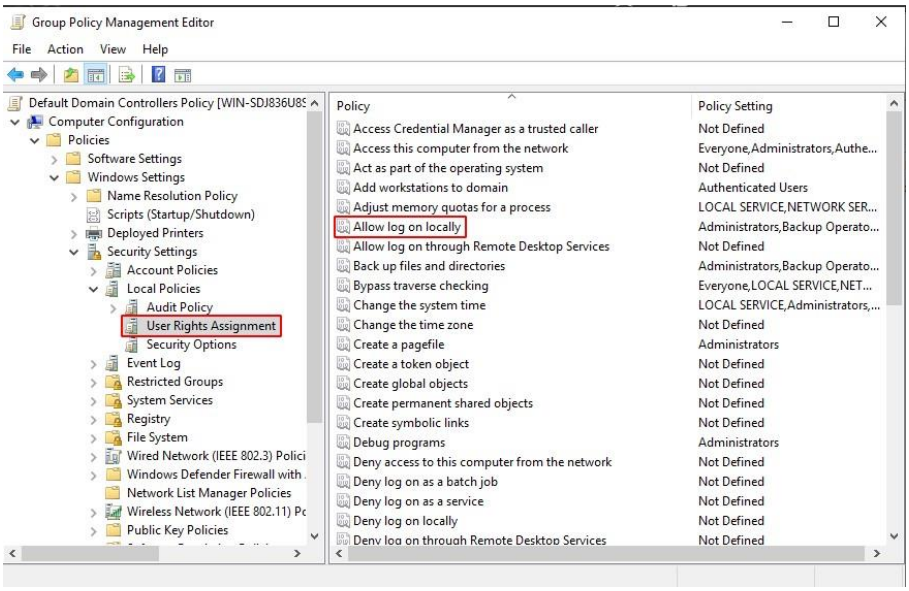


Рис. 4.11

4) Додайте до переліку користувачів та груп, яким дозволено локальний вхід на контролери домену, групу локальних адміністраторів (рис. 4.12).

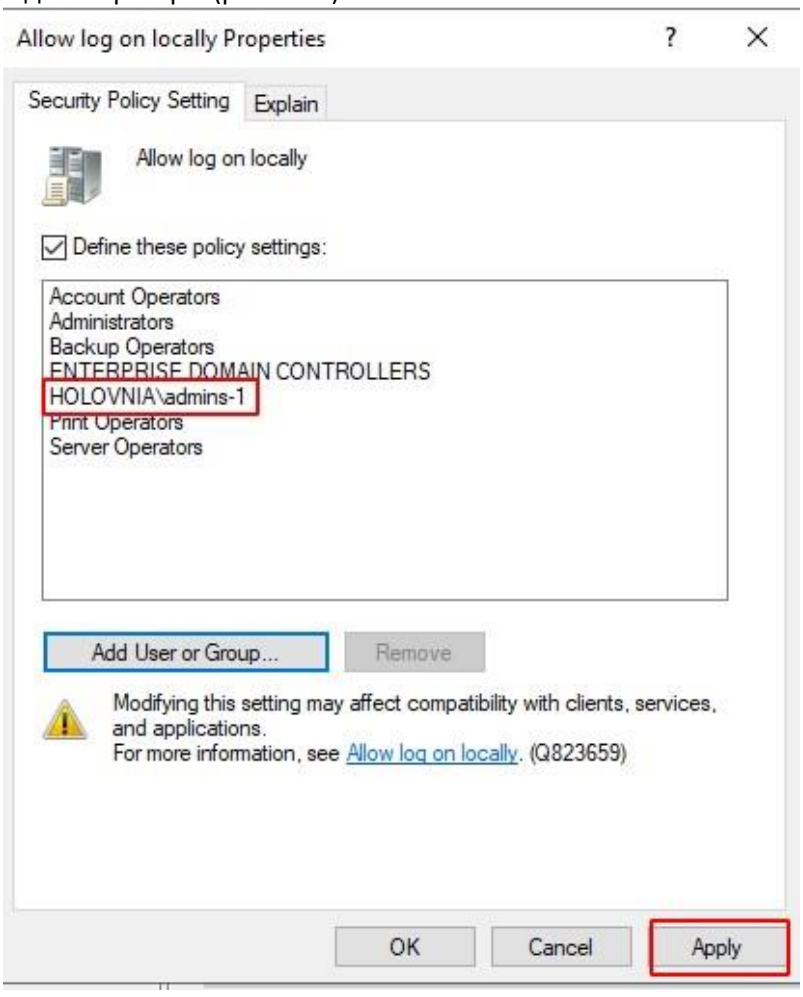


Рис. 4.12

5) Виконайте оновлення групової політики для контейнера *Domain Controllers*.

Завдання №4.3. Налаштування повноважень для локальних адміністраторів

1. Спираючись на подані вище теоретичні відомості, створіть в OU *Branch-GGNN-1* групу локальних адміністраторів та делегуйте їх адміністративні повноваження на рівні цієї організаційної одиниці.

2. Дозвольте членам новоствореної групи локальних адміністраторів локальний вхід на контролерах домену.

3. Перевірте зроблені налаштування, ввійшовши на контролері домену від імені одного з членів групи локальних адміністраторів OU *Branch-GG-NN-1* і спробувавши створити нового користувача у межах цієї організаційної одиниці. Чи вдається це зробити? Чи вдається створити користувача у межах іншої організаційної одиниці? Чому?

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені питання.

Завдання №4.4. Налаштування традиційних політик для користувачів та комп'ютерів

1. У лабораторній роботі №3 ми не створювали організаційні одиниці для комп'ютерів - через обмежену кількість робочих віртуальних машин. Однак для виконання наступного завдання нам знадобиться принаймні одна така організаційна одиниця.

За допомогою оснащення Active Directory Users and Groups створіть у вашому домені організаційну одиницю Computers-GG-NN, а в ній - дочірню організаційну одиницю Comp-Branch-GG-NN-1. Перемістіть одну з робочих станцій із контейнера Computers в організаційну одиницю Comp-Branch-GG-NN1.

2. Самостійно з'ясуйте, як в оснащенні Group Policy Management за допомогою вузла Policies (традиційні групові політики) для комп'ютерів зробити так, щоб:

⌘ у межах OU Comp-Branch-GG-NN-1 звичайні користувачі були зобов'язані встановлювати собі паролі довжиною принаймні 10 символів.

Виконайте описані вище налаштування.

3. Самостійно з'ясуйте, як в оснащенні Group Policy Management за допомогою вузла Policies (традиційні групові політики) для користувачів зробити так, щоб:

⌘ у межах OU Branch-GG-NN-1 звичайним користувачам не було дозволено запускати Панель керування (Control Panel);

⌘ у межах OU Branch-GG-NN-1 вимкнулося відображення значка Смітника / Корзини на робочому столі.

Виконайте описані вище налаштування.

Підказки. Для окремих налаштувань вам може знадобитися вузол Administrative Templates. Для встановлення заборони на запуск Панелі керування існує більше одного шаблону. Оберіть той, що працюватиме.

4. Переконайтеся, що налаштування успішно застосовані.

Звіт має містити скриншоти зроблених налаштувань та опис основних дій.

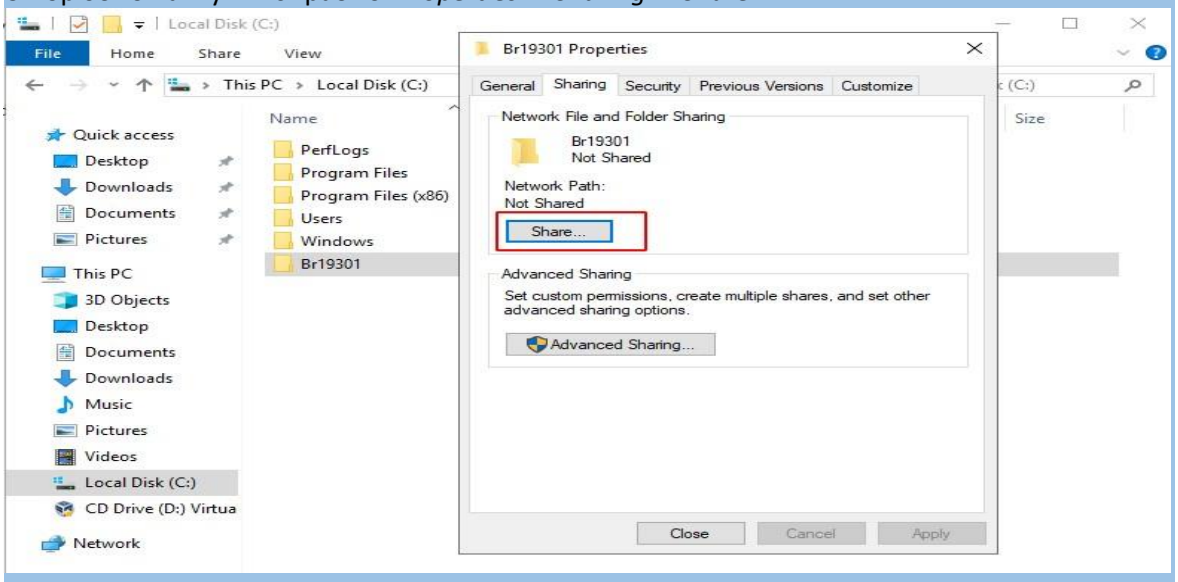
Завдання №4.5. Налаштування *Preferences* для комп'ютерів

1. Спираючись на матеріали лекції, самостійно з'ясуйте, як за допомогою вузла *Preferences* налаштувати для користувачів OU *Branch-GG-NN-1*:

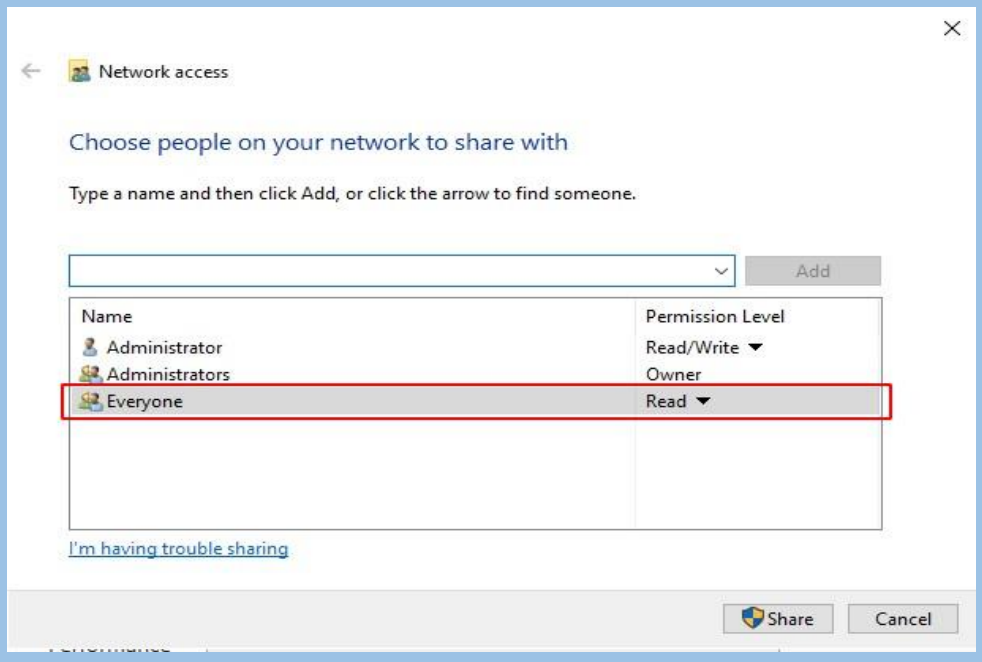
⌘ підключення мережного диску з міткою *BrGGNN1*.

Підказка. Відповідну папку можна створити на контролері домену. Наприклад, так.

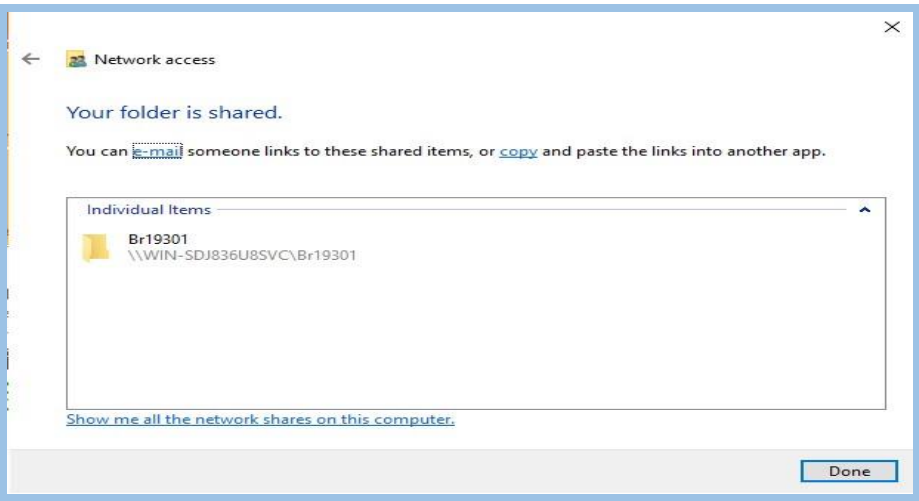
Створюємо папку і вибираємо: *Properties -> Sharing -> Share*



Дозволяємо групі *Everyone* (всім суб'єктам, які пройшли автентифікацію) читання вмісту цієї папки.



З'ясовуємо мережне ім'я спільної папки:



Дії, необхідні для підключення цієї папки як мережного диску, описані у лекції.

Звіт має містити: скриншоти зроблених налаштувань та опис основних дій.

Завдання №4.6

1. За допомогою вузла *Group Policy Results* дослідіть права, які має один з локальних адміністраторів OU *Branch-GG-NN-1* у межах домену.

2. За допомогою вузла *Group Policy Modeling* змоделюйте ситуацію, що матиме місце, якщо того самого локального адміністратора OU *Branch-GG-NN-1* додати до групи *Domain Admins*.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені питання.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 4.1-4.6.

Робота №5. Налаштування DNS-сервера на основному контролері домену Active Directory

Мета: навчитися інтерпретувати та змінювати основні налаштування DNS-сервера на основному контролері домену в Active Directory (на прикладі Windows Server 2022).

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №2-3, а також лабораторної роботи №4.

Теоретичні відомості та завдання до лабораторної роботи

DNS: основні поняття

DNS (*Domain Name System*, доменна система імен) - це ієрархічна децентралізована система імен для комп'ютерів, служб та інших мережних ресурсів.
На DNS-сервері зберігається перелік записів, які ставлять у відповідність доменним іменам конкретні IP-адреси. Використовуються записи різних типів (зокрема A, AAA, CNAME, MX, NS, PTR, SOA, SRV тощо). Деякі з цих типів буде розглянуто далі у цій роботі.
Зона DNS - частина простору імен, для якого DNS-сервер може виконувати операції з перетворення імен (*name resolution*).
Важливо. Зона не є тотожною домену. У межах одного домену зон DNS може бути декілька. Але якщо домен невеликий, то він може мати й одну зону.

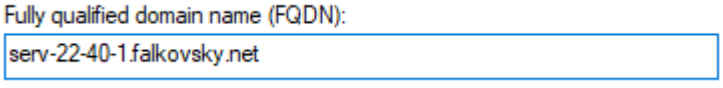
Розрізняють зону прямого перегляду і зону зворотного перегляду.

Зона прямого перегляду (*forward lookup zone*) використовується для перетворення доменного імені в IP-адресу (є доменне ім'я - за ним треба одержати IP-адресу). Це пряме перетворення імені.
Зона зворотного перегляду (*reverse lookup zone*) використовується для перетворення IP-адреси у доменне ім'я (є IP-адреса - за нею треба одержати доменне ім'я). Це зворотне перетворення імені.
Сервер імен (*name server*, *NS*) - сервер, на якому зберігаються DNSзаписи. Серверів імен може бути декілька.
У налаштуваннях Active Directory абревіатурою NS позначаються *авторитетні сервери імен*.
Авторитетний сервер імен (*authorative name server*) - сервер імен, записи якого вважаються найбільш достовірними у домені на противагу записам інших серверів імена, котрі можуть бути кешованою версією записів авторитетного сервера. Тільки такі сервери можуть повертати авторизовані відповіді.

Абсолютні доменні імена записуються у форматі FQDN.

FQDN (*Fully Qualified Domain Name*) - повне доменне ім'я, яке визначає точне розташування ресурсу в ієрархічній структурі DNS.

Наприклад:



Деякі типи DNS-записів

Запис A (*A host address*) ставить у відповідність текстовому імені ресурсу IP-адресу цього ресурсу за протоколом IPv4.
Запис AAAA (*AAAA host address*) ставить у відповідність текстовому імені ресурсу IP-адресу цього ресурсу за протоколом IPv6.
Запис CNAME є псевдонімом, що перескеровує з одного імені (псевдоніму) на інше.

Прикладом використання запису *CNAME* є присвоєння псевдоніму спільному мережному ресурсу (наприклад, вебсерверу, файловому серверу тощо), який би дозволив звертатися до цього ресурсу за коротшим і зручнішим ім'ям, ніж його доменне ім'я.

Запис NS (*Name Server*) містить ім'я авторитетного сервера імен (таких записів може бути декілька - для кожного авторитетного сервера окремий).

Запис SOA (*Start of Authority*) містить адміністративну інформацію про дану зону.

До такої адміністративної інформації, зокрема, належать наступні відомості:

первинний сервер (*primary server*, головний авторитетний сервер, на якому може відбуватися зміна DNS-записів, після чого решта серверів імен також оновлюють свої записи відповідним чином);

інтервал оновлення (*refresh interval*, часовий проміжок, через який вторинні сервери імен повинні надіслати первинному серверу імен запит на виявлення можливих змін у зоні DNS);

інтервал повторення (*retry interval*, часовий проміжок, через який вторинні сервери імена мають повторити запит на виявлення можливих змін у зоні DNS, якщо первинний сервер не відповідає; цей інтервал має бути меншим за інтервал оновлення);

дійсний до (*expires after*, часовий проміжок, через який вторинні сервери повинні припинити відповідати на запити, пов'язані з даною зоною DNS, якщо первинний сервер не відповідає; цей інтервал має бути більшим за суму інтервалу оновлення та інтервалу повторення).

Запис PTR (скорочення від *pointer* - вказівник) автоматично створюється в зоні зворотного перегляду для кожного запису A чи AAAA із зони прямого перегляду.

Встановлення ролі DNS-сервера в Active Directory

Часто роль DNS-сервера в Active Directory вже встановлено. Якщо ж її потрібно встановити, виконайте наступну послідовність кроків.

1. У вікні *Server Manager* на панелі Dashboard виберіть опцію *2 Add roles and features*. (рис. 5.1).

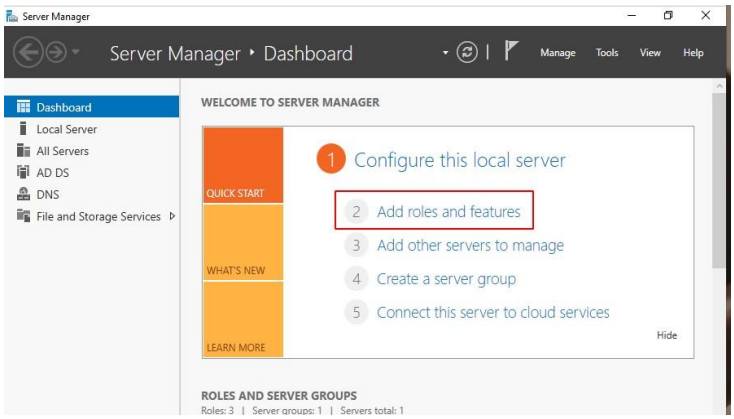


Рис. 5.1

2. Оберіть опцію *Role-based or feature-based installation* (рис. 5.2).

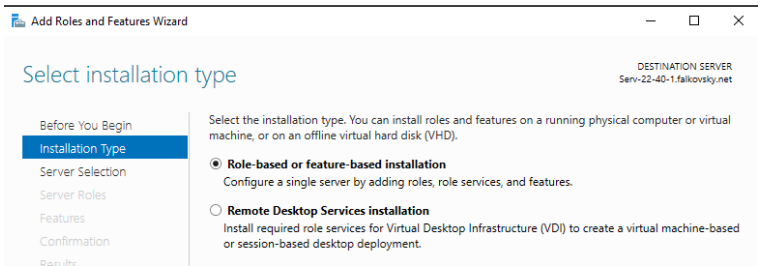


Рис. 5.2

3. Вкажіть сервер домену, на якому необхідно встановити роль DNScервера. На рис. 5.3 це основний контролер домену.

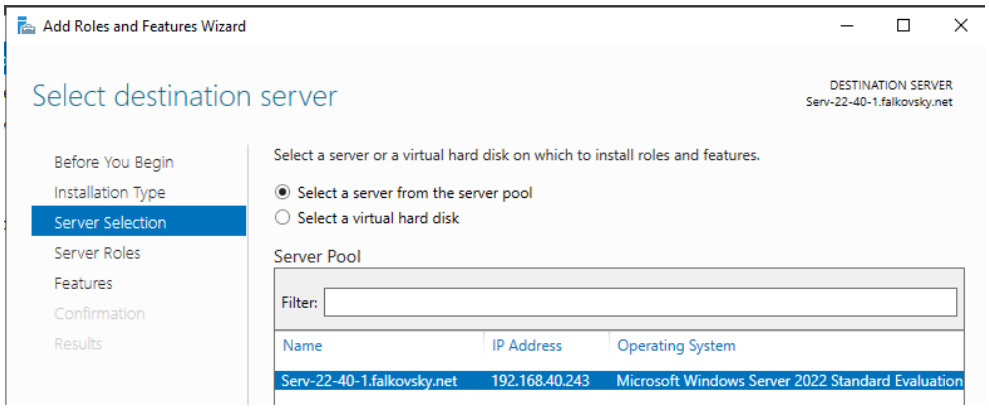


Рис. 5.3

4. Оберіть роль, яку необхідно довстановити - у даному випадку це роль *DNS Server*. Якщо роль вже встановлено, опцію буде обраною і неактивною, як на рис. 5.4. В іншому разі встановіть прапорець навпроти опції.

Рис. 5.4

5. Якщо роль DNS Server встановлена, але відповідні меню на сервері відсутні, виконайте у PowerShell з правами адміністратора домену команду

Install-WindowsFeature -Name RSAT-DNS-Server

```
PS C:\Users\Administrator> Get-WindowsFeature -Name DNS

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] DNS Server                                          DNS                         Installed


PS C:\Users\Administrator>
PS C:\Users\Administrator> Install-WindowsFeature -Name RSAT-DNS-Server

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {DNS Server Tools}
```

Рис. 5.5

<u>Завдання №5.1</u>. Довстановлення ролі DNS-сервера (за потреби)

1. Запустіть основний контролер вашого домену і перевірте, чи встановлено на ньому роль DNS-сервера. Якщо ні - встановіть.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Оснащення DNS Manager

Основний функціонал, пов'язаний з налаштуваннями DNS-сервера у Windows Server, міститься в оснащенні *DNS Manager* (меню *Tools* -> *DNS*, рис. 5.5).

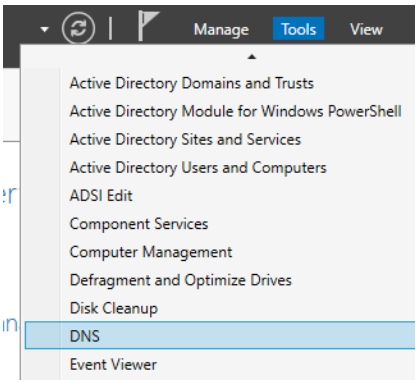


Рис. 5.6

Вікно оснащення *DNS Manager* має вигляд, подібний до зображеного на рис. 5.7.

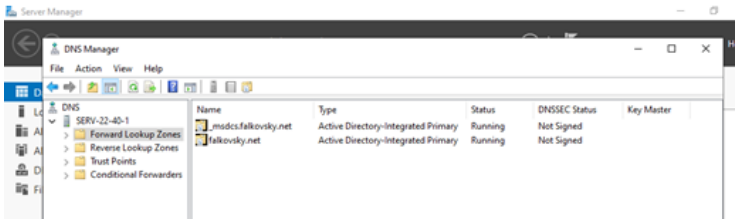


Рис. 5.7

Завдання №5.2. Дослідження наявних налаштувань DNS-сервера

1. Запустіть оснащення *DNS Manager*.
2. Дослідіть наявні налаштування DNS у вашому домені. Перегляньте основні записи в домені (для перегляду подробиць двічі клацніть по відповідному запису). Дайте відповіді на наступні запитання (можуть бути наявні не всі типи записів):

- Чи створено в домені зону прямого перегляду? зону зворотного перегляду?
- Чи є у домені записи типу A? Які повні доменні імена та IP-адреси вказані у цих записах.
- Чи є у домені записи типу AAAA? Які повні доменні імена та IP-адреси вказані у цих записах.
- Чи є у домені записи типу NS? Які доменні імена та IP-адреси відповідають серверам із цих записів?
- Чи є у домені записи типу SOA? Який із серверів домену є первинним? Які значення задано для інтервалів оновлення, повторення та поля *дійсний до*?
- Чи є у домені записи типу PTR? Яким записам типу A (AAAA) вони відповідають?

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Створення DNS-запису для маршрутизатора

Зазвичай DNS-запис для маршрутизатора початково відсутній і за замовчуванням не створюється. Створення такого запису для порту маршрутизатора, що виконує роль шлюзу за замовчуванням, допоможе на практиці побачити, як створюється новий DNS-запис.

1) З'ясуйте адресу порту маршрутизатора, що виконує роль шлюзу за замовчуванням у вашій мережі. У прикладі це буде адреса 192.168.40.241 за протоколом IPv4 (рис. 5.8). Тобто створювати будемо DNS-запис типу A.

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

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.40.243
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.40.241
PS C:\Users\Administrator>
```

Рис. 5.8

2) Зараз шлюз за замовчуванням може пінгуватися безпосередньо за IPадресою (все одно не пінгуватиметься, якщо ви використовуєте внутрішню мережу VirtualBox). Але пінгування за ім'ям *router* буде завершуватися помилкою, так і не розпочавшись. Наприклад, так:

```
PS C:\Users\Administrator> ping router
Ping request could not find host router. Please check the name and try again.
```

3) Додамо DNS-запис для порту маршрутизатора, що є шлюзом за замовчуванням для даної мережі. У контекстному меню домену виберіть пункт *New Host (A or AAAA)...* (рис. 5.9).

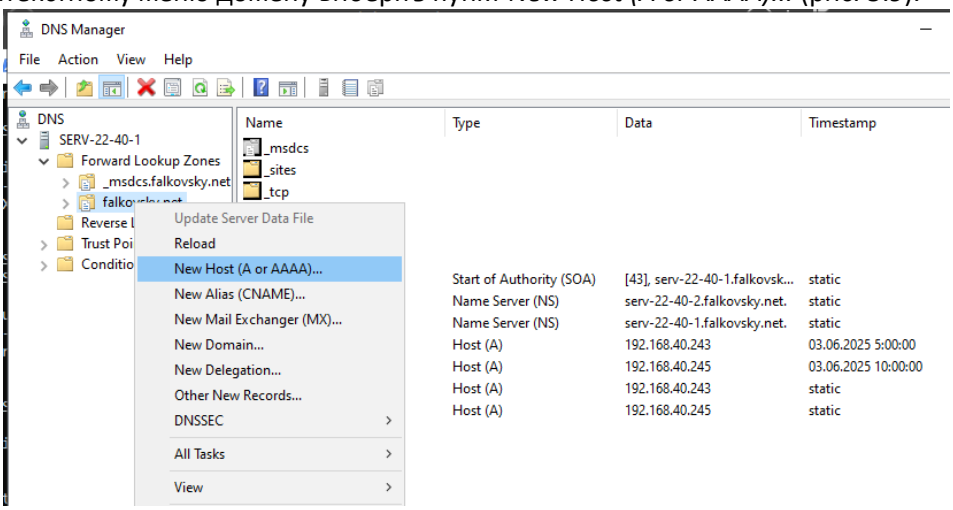


Рис. 5.9

4) У вікні *New Host* (рис. 5.10) вкажіть відносне доменне ім'я для маршрутизатора, зазначте IP-адресу шлюзу за замовчуванням та натисніть *Add Host*.

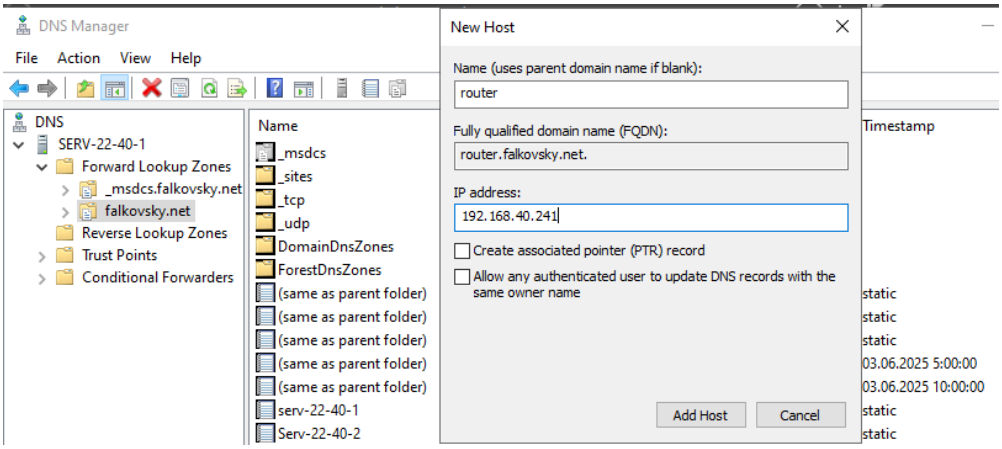


Рис. 5.10

5) Відповідний DNS-запис з’явиться у переліку DNS-записів домену.
6) Здійсніть повторне пінгування шлюзу за замовчуванням через доменне ім’я:

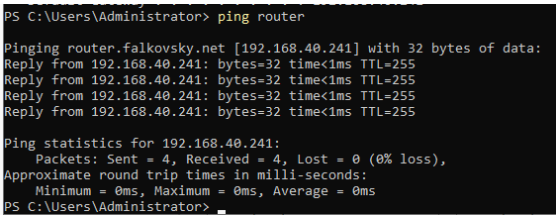


Рис. 5.11

Пінг по імені router працює, оскільки в DNS-сервері був створений A-запис (типу Host), який зв'язує ім'я router з IP-адресою 192.168.40.241.

Коли комп’ютер виконує команду ping router, він спочатку надсилає DNS-запит для визначення IP-адреси, що відповідає імені router.

DNS-сервер відповідає згідно з наявним A-записом, вказуючи на IP-адресу 192.168.40.241. Після цього вже здійснюється ICMP (ping) запит до цієї IP-адреси.

- Ім’я router → DNS-запит → DNS-сервер повертає 192.168.40.241 (завдяки A-запису).
- Потім: ping 192.168.40.241 → якщо IP активний і не блокує ICMP — отримуємо відповідь.

Без запису в DNS або відсутності альтернативних джерел (файл hosts, NetBIOS) ім’я router не могло б бути резольвованим, і пінг завершився б помилкою "Ping request could not find host".

Завдання №5.3. Створення DNS-запису для маршрутизатора

1) Перевірте, чи успішним є пінгування з контролера домену маршрутизатора за доменним ім’ям *router*.

2) Створіть у вашому DNS-запис для порту маршрутизатора, що відповідає шлюзу за замовчування у вашій моделі мережі.

3) Повторіть п. 3 і переконайтеся, що перетворення доменного імені *router* у відповідну IP-адресу було коректним.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Створення зони зворотного перегляду

Наявність зони зворотного перегляду може знадобитися для коректної роботи окремих служб. Розглянемо приклад створення зони зворотного перегляду у домені *holovnia.net*.

1) У вікні оснащення *DNS Manager* виберіть *Action* → *New Zone* (рис. 5.12).

2) Запуститься майстер створення нової зони (рис. 5.13).

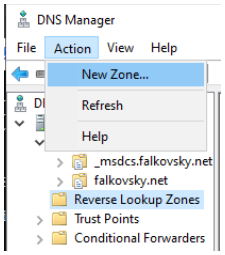


Рис. 5.12

Рис. 5.13

3) Оберіть первинну зону (*primary zone*), щоб майбутню зону зворотного перегляду було створено на поточному сервері (рис. 5.14).

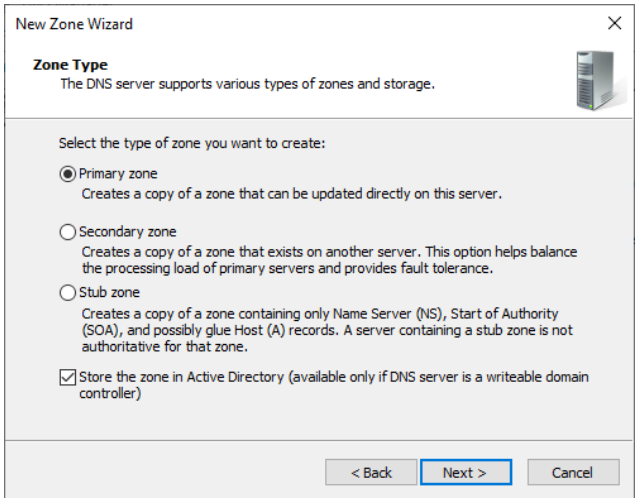


Рис. 5.14

4) Оберіть зону реплікації для створюваної зони DNS - у даному випадку це опція *To all DNS domain controllers in this domain...*, тобто буде відбуватися реплікація даних з цієї зони DNS на всіх DNS-серверах, організованих на контролерах домену (рис. 5.15). У створюваній нами моделі мережі таких контролерів і, відповідно, DNS-серверів буде два.

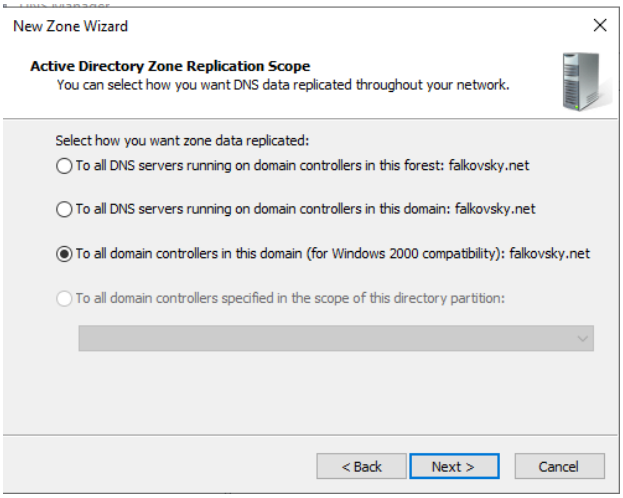


Рис. 5.15

5) Вкажіть, яка версія протоколу IP буде використовуватися у створюваній зоні зворотного перегляду. У даній мережі застосовується протокол IPv4 (рис. 5.16).

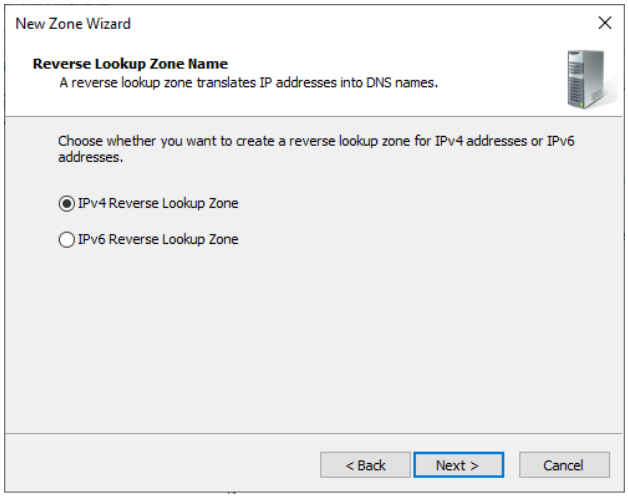


Рис. 5.16

6) Дайте ім'я створюваній зоні зворотного перегляду. Це можна зробити, вказавши адресу мережі або безпосередньо задавши ім'я зони зворотного перегляду. На рис. 5.17 введено адресу мережі. Тоді ім'я зони зворотного перегляду згенерується автоматично і буде таким, як прописано в неактивному полі в нижній частині вікна (рис. 5.17): 40.168..in-addr.arpa.

Зверніть увагу, як утворюється ім'я зони зворотного перегляду. Октети адреси мережі пишуться у зворотній послідовності, а далі записується *in-addr.arpa*.

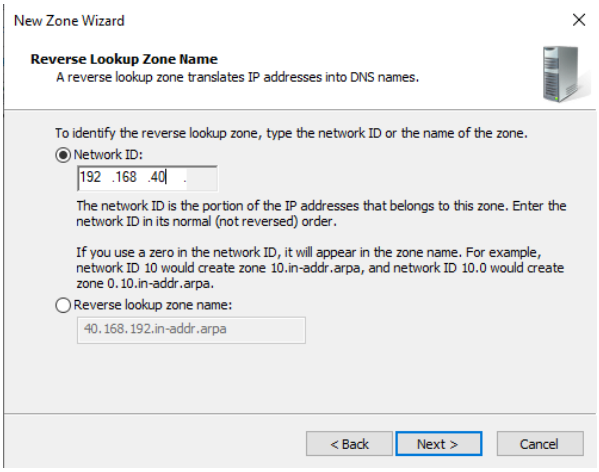


Рис. 5.17

7) Налаштуйте динамічне оновлення створюваної зони DNS. Оберіть *Allow only secure dynamic updates*, щоб здійснювалися лише безпечні динамічні оновлення (рис. 5.18). Тоді такі оновлення будуть відбуватися лише з довірених джерел (рекомендоване налаштування).

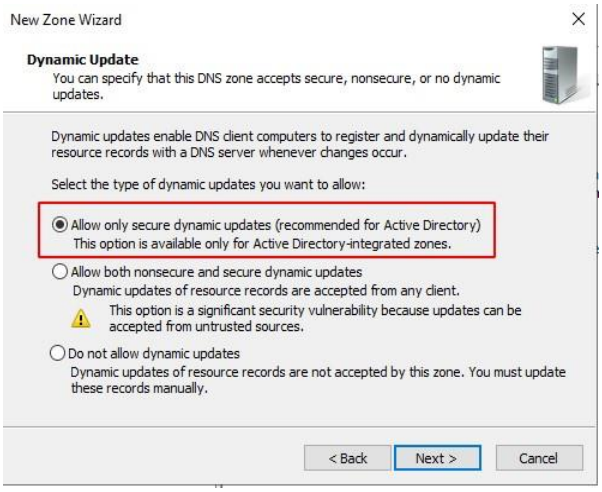


Рис. 5.18

8) Створення зони зворотного перегляду завершене (рис. 5.19).

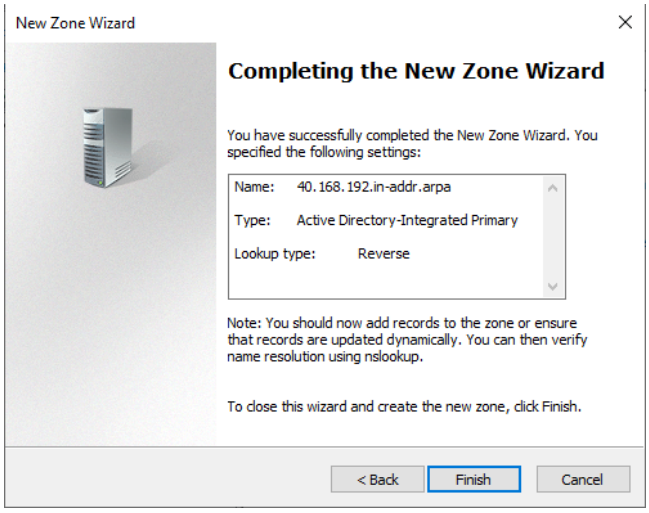


Рис. 5.19

9) Ініціюємо реєстрацію DNS-записів основних ресурсів. У нашому випадку це стосується реєстрації DNS-серверів у зоні зворотного перегляду. Для цього на контролері домену введемо команду ipconfig /registerdns. У разі успішного виконання одержимо вивід, подібний до зображеного на рис. 5.20.

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

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be report
ed in the Event Viewer in 15 minutes.
PS C:\Users\Administrator>
```

Рис. 5.20

10) Перевіримо ефективність виконаних налаштувань. Для цього ввійдемо в систему на одній з робочих станцій домену і введемо команду nslookup, у ролі аргументу вказавши IP-адресу контролера домену, на якому налаштовували DNS-сервер.

Якщо налаштування успішні, то результат роботи команди nslookup буде подібний на той, що зображений на рис. 5.21.

```
*** UnKnown can't find 192.168.40.243: Non-existent domain
PS C:\Users\Administrator.FALKOVSKY> ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be report
ed in the Event Viewer in 15 minutes.
PS C:\Users\Administrator.FALKOVSKY> nslookup 192.168.40.243
Server:  Serv-22-40-1.falkovsky.net
Address:  192.168.40.243

Name:    Serv-22-40-1.falkovsky.net
Address:  192.168.40.243

PS C:\Users\Administrator.FALKOVSKY>
```

Рис. 5.21

Перші два рядки показують ім’я сервера, з якого одержано дані, а останні два рядки - відомості про ресурс, який міститься за заданою адресою. На рис. 5.21 DNS-сервер надав відомості сам про себе.

Завдання №5.4. Створення зони зворотного перегляду

1. За допомогою оснащення *DNS Manager* переконайтеся, що зону зворотного перегляду ще не створено.

2. Створіть зону зворотного перегляду на DNS-сервері, що працює на основному контролері домену. Поки що не виконуйте команду ipconfig /registerdns.

3. За допомогою оснащення *DNS Manager* перегляньте новостворену зону зворотного перегляду. Чи відображаються у ній DNS-записи для серверів?

4. З командного рядка запустіть реєстрацію DNS-записів основних ресурсів. Чи відображаються DNS-записи для серверів у зоні зворотного перегляду тепер?

5. За допомогою команди nslookup перевірте, що зона зворотного перегляду налаштована успішно.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 5.1-5.4.

Рекомендовані джерела

1. M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020 (p. 82).
2. Gilbert Held. Windows Networking Tools: The Complete Guide to Management, Troubleshooting, and Security. CRC Press, 2013 (команда *nslookup*).

Робота №6. Налаштування реплікації між двома контролерами домену Active Directore

Мета: навчитися інтерпретувати та змінювати основні налаштування реплікації між двома контролерами домену в Active Directory (на прикладі Windows Server 2022).

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-5.

Теоретичні відомості та завдання до лабораторної роботи

Реплікація в Active Directory

Внутрішньосайтова реплікація (intrasite replication)

Є здебільшого автоматичною. Задля надійності внутрішньосайтова реплікація організована надлишковим чином: якщо контролерів домену більше двох, то з'єднання для реплікації автоматично створюються таким чином, аби кожний контролер домену був сполучений принаймні з двома іншими контролерами.

Зазвичай реплікація автоматично розпочинається через певний час після того, як на контролері домену відбулися зміни, однак її можна запустити примусово.

Важливо враховувати, що мережний трафік між контролерами домену може бути досить інтенсивним. Саме тому й існує рекомендація щодо максимально стабільного та швидкого з'єднання всередині сайту Active Directory.

Для передавання даних внутрішньосайтова реплікація використовує протокол IP.

Міжсайтова реплікація (intersite replication)

З'єднання між різними сайтами не створюються автоматично - їх вручну задає адміністратор.

Сервер-плацдарм (*bridgehead server*) - сервер, через яких відбувається реплікація між цим сайтом та іншими сайтами.

Сервер-плацдарм обирається автоматично, однак адміністратор може задати сервер-плацдарм, якому треба надавати перевагу під час вибору (***preffered bridgehead server***). Втім, якщо такий сервер виявиться недоступний, міжсайтова реплікація не відбудеться.

Для міжсайтової реплікації можна задавати розклад (наприклад, такий, аби реплікація відбувалася не в період найбільш інтенсивних операцій скажімо, у неробочі години). Також можна обирати протокол (у більшості випадків - RPC over IP, іноді, для старих мереж - SMTP).

Більшість операцій з реплікації всередині сайту та частину операцій з міжсайтової реплікації виконує компонент ***KCC (Knowledge Consistency Checker)*** - див. лекція №3.

Робота з оснащенням Active Directory Sites and Services

Оснащення Acive Directory Sites and Services дозволяє переглядати та змінювати налаштування, пов'язані з сайтами Active Directory та службами, які працюють у межах ций сайтів, зокрема реплікацією.

Для запуску оснащення Active Directory Sites and Services у вікні Sever Manager оберіть Tools -> Active Directory Sites and Services (рис. 6.1).

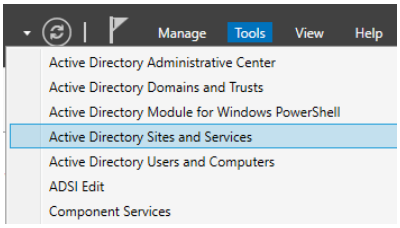


Рис. 6.1

Щоб переглянути з'єднання для конкретного сервера, виберіть *Sites* -> *ім'я сайту* -> *Servers* -> *ім'я сервера* -> *NTDS Settings* (рис. 6.2).

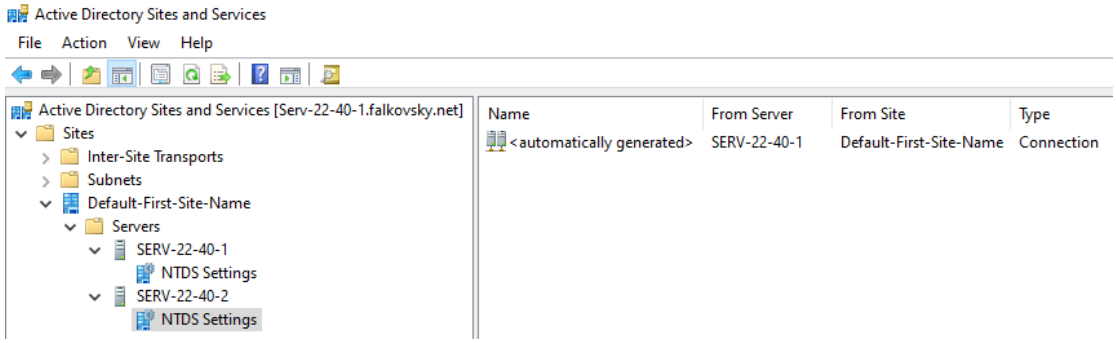


Рис. 6.2

Зверніть увагу. Всі з'єднання, які ви побачите у вікні *Active Directory Sites and Services*, є вхідними з'єднаннями (тобто до цього сервера від інших серверів). Вихідні з'єднання не відображаються. Однак це не має значення для реплікації, оскільки вона відбувається в обох напрямках після того, як з'єднання встановлене.

Для того, щоб змусити KCC перегенерувати топологію реплікації, оберіть *Sites* -> *ім'я сайту* -> *Servers* -> *ім'я сервера* -> *NTDS Settings* -> *All tasks* -> *Check Replication Topology* (рис. 6.3). Щоб побачити результати, **оновіть** вміст вікна *Active Directory Sites and Servers*.

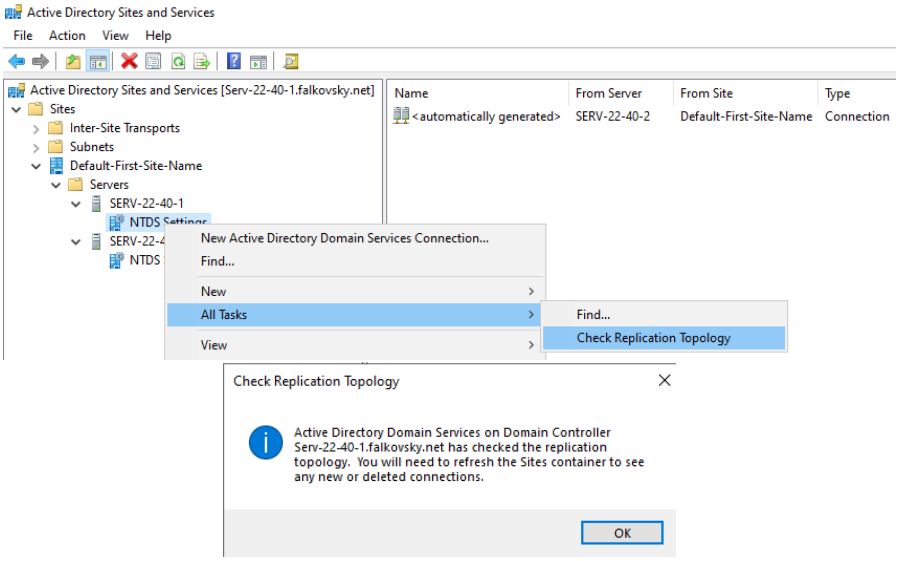


Рис. 6.3

Щоб розпочати примусову реплікацію, зробіть активним вузол *NTDS Settings* відповідного сервера, знайдіть з'єднання, через яке має відбутися реплікація і у контекстному меню цього з'єднання оберіть *Replicate Now* (рис. 6.4). У вашому випадку серверів два, і таку операцію треба повторити на обох.

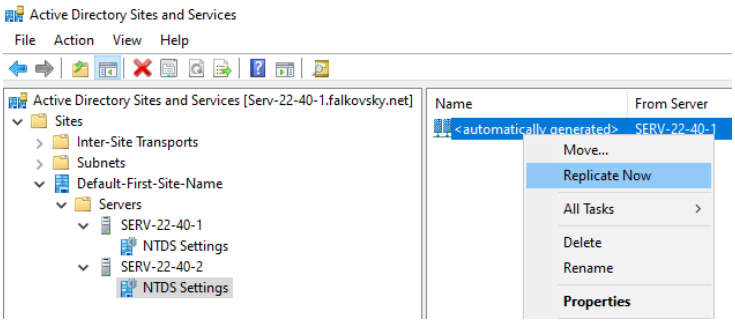


Рис. 6.4

Якщо реплікація успішна, відобразиться повідомлення, подібне до зображеного на рис. 6.5. **Ви маєте одержати таке повідомлення для кожного сервера (у вас їх два).**

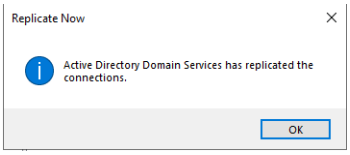


Рис. 6.5

Також примусову реплікацію можна запустити з командного рядка:

```
repadmin /SyncAll
```

Наочно побачити, чи успішна реплікація, можна, наприклад, переглянувши структуру домену в оснащенні *Active Directory Users and Computers* (рис. 6.6). Зокрема, якщо ви внесете зміни на першому контролері, то після успішної реплікації структура має співпадати на обох контролерах (рис. 6.6).

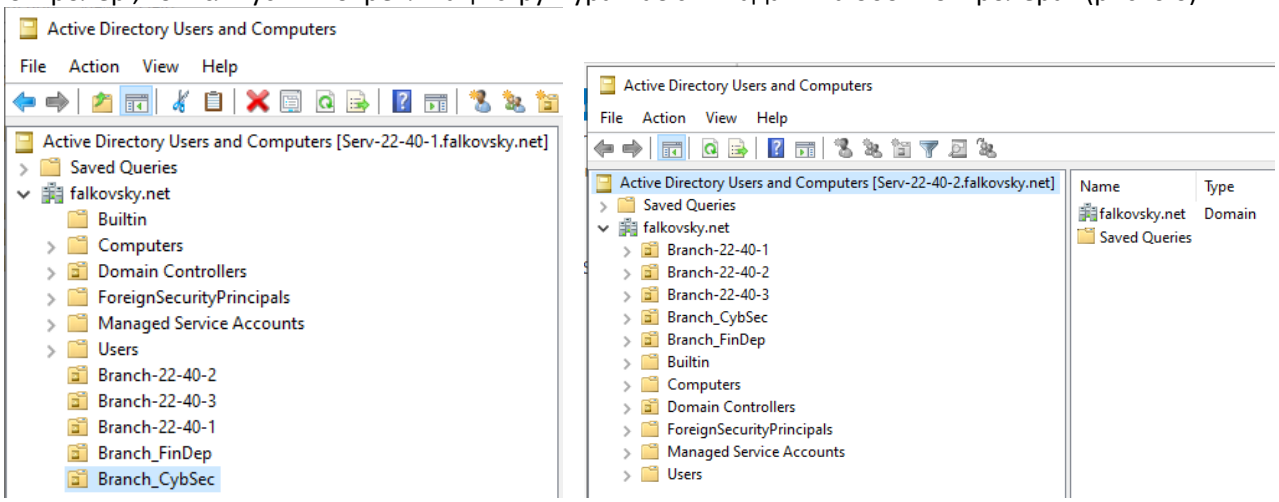


Рис. 6.6

<u>Завдання №6.1</u>. *Дослідження сайтів та наявної топології реплікації*

1. На першому контролері домену ввійдіть у *Active Directory Sites and Services*. Дослідіть вміст вікна цього оснащення і дайте відповіді на наступні питання

- Скільки сайтів наявно у вашому середовищі Active Directory?
- До якого сайту належать наявні контролери домену?
- Які зв'язки (*Connections*) відображаються в оснащенні *Acive Directory Sites and Services* для кожного з серверів? З яким саме сервером сполучає даний сервер кожне з'єднання?

Ці з’єднання вхідні чи вихідні? (див. теоретичні відомості)

<u>Звіт має містити</u> скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Завдання №6.2. ***Дослідження роботи KCC***

1. Видаліть автоматично створені з'єднання для кожного з серверів.

2. Запустіть примусову перевірку топології реплікації.

3. Оновіть вміст вікна *Active Directory Sites and Servers*. Які з'єднання згенерував *KCC*? Чи відрізняються вони від тих, які ви досліджували у **завданні №6.1**.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Завдання №6.3. ***Дослідження та налаштування реплікації AD***

1. Запустіть другий контролер домену (перший лишіть ввімкненим також).
2. На другому контролері домену відкрийте оснащення *Active Directory Users and Groups*. Чи відповідає структура домену, що відображається у цьому оснащенні, від тієї, яку ви створювали на першому контролері домену у межах *лабораторних робіт №3* і *№4*? Зробіть висновки про те, чи коректно функціонує реплікація.
3. З першого контролера домену ініціюйте примусову реплікацію на обох серверах. Після одержання двох повідомлень про успішну реплікацію повторіть п. 2.
4. Якщо реплікація не працює так, як очікувалося, з'ясуйте та усуньте причини. Якщо усе гаразд, пропустіть цей пункт.
5. На першому контролері домену додайте до однієї з організаційних одиниць нового користувача.
6. Переконайтеся, що реплікація виконалася успішно і цього разу:

- цей користувач має відображатися і на другому контролері домену
- коли перший контролер домену недоступний (відповідна віртуальна машина неактивна), то вхід від імені новоствореного користувача з однієї з робочих станцій домену все одно має вдаватися

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Завдання 6.4. Дослідження міжсайтової реплікації

1) В оснащеннні Active Directory Sites and Services оберіть вузол Inter-Site Transports (рис.6.7.)

2) З'ясуйте, який протокол має використовуватися для міжсайтової реплікації. Обґрунтуйте, чому налаштування за замовчуванням зроблено саме таким чином (див. теоретичні відомості).

3) Чи відбувається міжсайтова реплікація зараз? Чому?

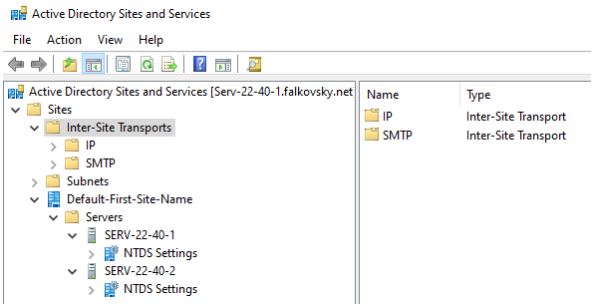


Рис. 6.7

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Деякі можливі причини того, що реплікація не працює як належне:

1) Порушено мережне з'єднання між контролерами домену (перевірте шляхом пінгування, виправте мережні налаштування - у ролі DNSсервера вкажіть адресу першого контролера домену, інші адреси DNSсерверів приберіть).

2) Відключено потрібні служби (відповідні повідомлення, імовірно, будуть відображатися у вікні *Server Manager* у розділах *Events* та *Services*).

3) Проблеми з DNS-сервером (може допомогти оновлення зони DNS на DNS-сервері, що на першому контролері домену, та наступне перезавантаження першого контролера домену).

4) Комплексна проблема, передусім у налаштуваннях другого контролера домену (у деяких випадках найефективнішим рішенням може бути повне перевстановлення ролі AD DS на другому контролері домену - у такому разі варто поки зняти прапорець *Domain Name System (DNS) Server* і лишити тільки прапорець *Global Catalog (GC)*, а також явно вказати, що реплікація буде відбуватися з першого контролера домену - у полі *Replicate from* задайте ім'я першого контролера).

***Де шукати підказки*.** У вікні *Server Manager* для даного контролера та кожного зі встановлених сервісів виводяться повідомлення аудиту, серед яких можуть бути і повідомлення про помилки. Аналізуйте такі повідомлення на обох контролерах. Особливу увагу зверніть та ті повідомлення, які стосуються *AD DS* та *DNS*.

Будь ласка, врахуйте, що **повідомлення про відключення служби NtFrs (File Replication) є цілком нормальним**, оскільки у сучасних версія AD здебільшого використовується служба DFSR (DFS Replication).

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 6.1-6.4.

Робота №7. Налаштування DHCP-сервера на базі домену Active Directory засобами Windows Server 2022

Мета: навчитися основ налаштування протоколу динамічного конфігурування вузлів DHCP для домену Active Directory та основ моніторингу його роботи (у Windows Server 2022).

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-6.

Теоретичні відомості та завдання до лабораторної роботи

НАЛАШТУВАННЯ ПРОТОКОЛУ ДИНАМІЧНОГО КОНФІГУРУВАННЯ ВУЗЛІВ DHCP

Додавання ролі DHCP-сервера

DHCP-сервер організуємо на першому контролері домену. Для цього спершу потрібно додати відповідну роль.

У вікні *Server Manager* оберіть *Manage* → *Add Roles and Features* (рис. 7.1).

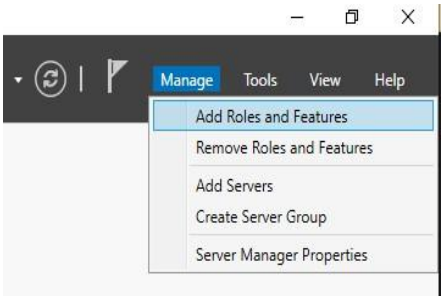


Рис. 7.1

Встановіть прапорець навпроти ролі *DHCP server* (рис. 7.2).

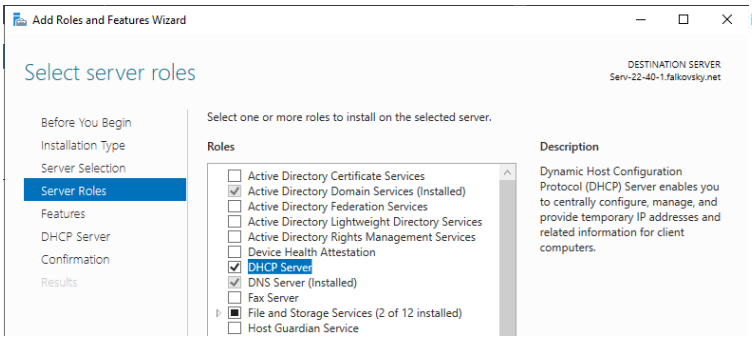


Рис. 7.2

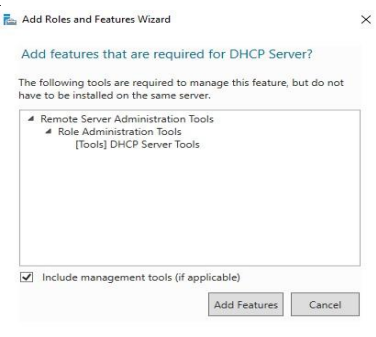


Рис. 7.3

Підтвердіть зроблені налаштування. Прапорець *Include management tools (if applicable)* лишіть (рис. 7.3).

Нових компонентів встановлювати не потрібно (рис. 7.4).

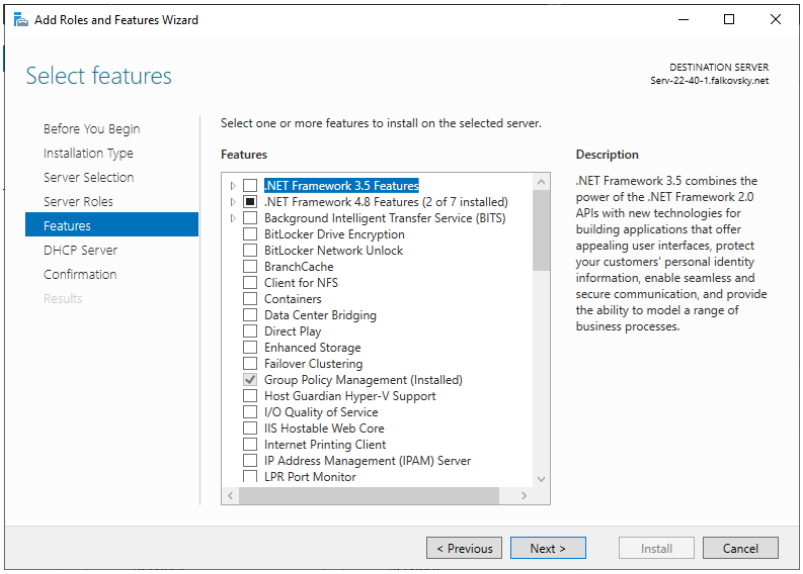


Рис. 7.4

Зверніть увагу на попередження, які виводить система (рис. 7.5). На даному етапі потрібно мати щонайменше одну статичну IP-адресу на цього комп'ютері (у нашому випадку це так), а також спланувати розподіл адрес у мережі. У даній лабораторній роботі статичні адреси лишаться у маршрутизатора, комутатора та обох серверів AD, натомість робочим станціям адреси присвоюватимуться динамічно.

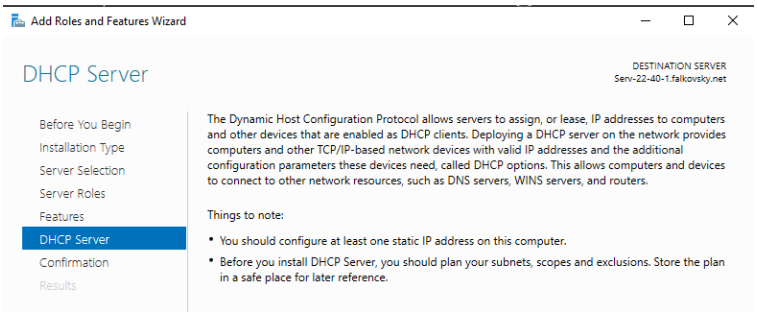


Рис. 7.5

Перегляньте вибрані налаштування та натисніть Install (рис. 7.6).

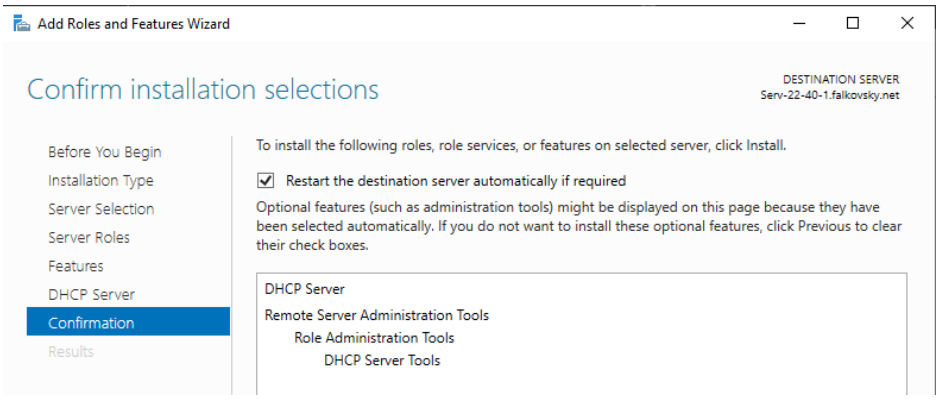


Рис. 7.6

Розпочнеться встановлення DHCP-сервера (рис. 7.7). На віртуальній машині воно може зайняти деякий час.

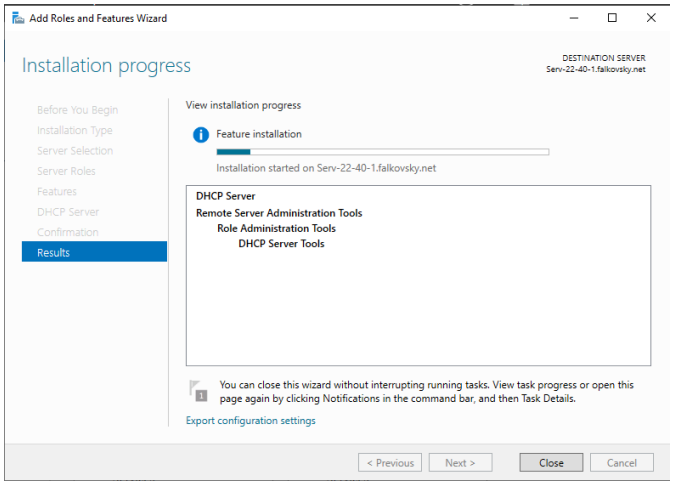


Рис. 7.7

Після завершення інсталювання DHCP-сервера у вікні Server Manager з’явиться відповідна панель (рис. 7.8). Звідси можна буде здійснювати моніторинг подій, пов’язаний з роботою DHCP-сервера.

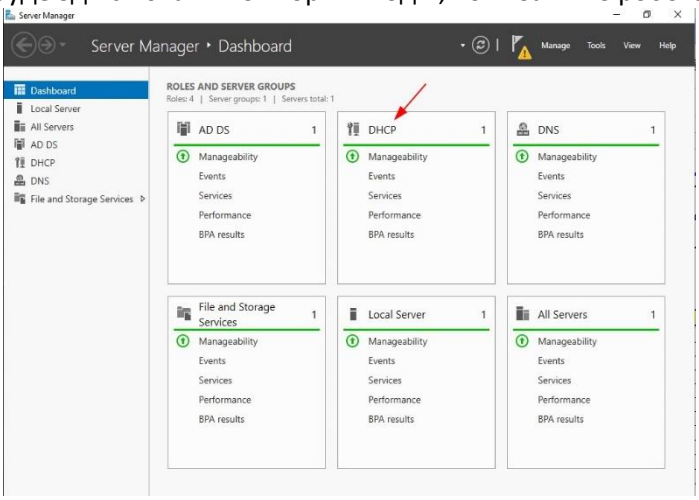


Рис. 7.8

Далі потрібно здійснити конфігурування DHCP-сервера.

<u>Налаштування DHCP-сервера</u>

Після встановлення ролі *DHCP Server* у правій верхній частині вікна Server Manager, біля піктограми у вигляді прапорця, має з’явитися знак оклику (рис. 7.9). Щоб налаштувати щойно встановлений DHCP-сервер оберіть опцію *Complete DHCP comfiguration*.

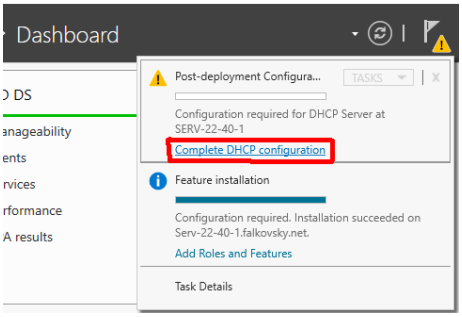


Рис. 7.9

Ознайомтеся з повідомлення про створення стандартних груп *DHCP Administrators* та *DHCP Users* (рис. 7.10).

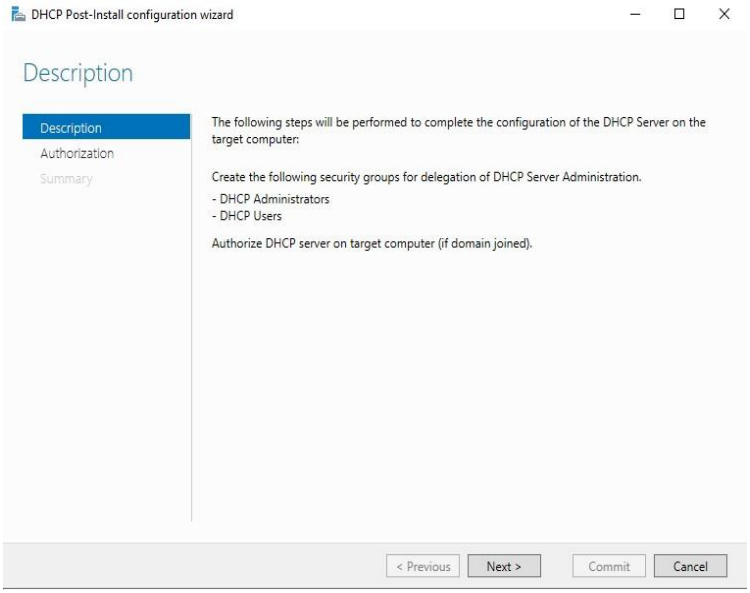


Рис. 7.10

Далі введіть дані для авторизації цього DHCP-сервера в AD DS. Це може бути, наприклад, адміністратор вашого домену (рис. 7.11).

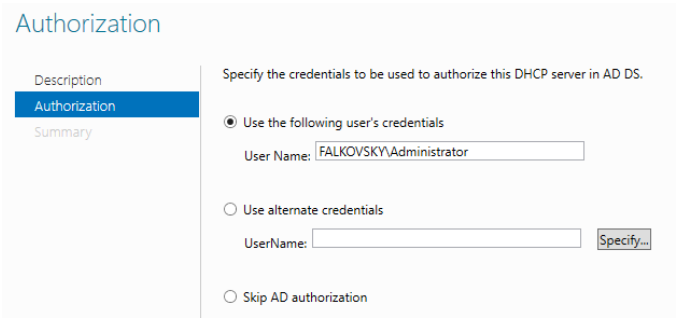


Рис. 7.11

Прогляньте основні налаштування. DHCP-сервер авторизований і майже готовий до роботи (рис. 7.12).

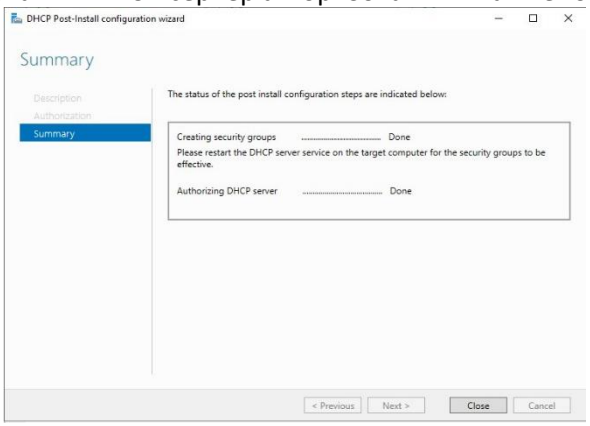


Рис. 7.12

Далі задамо область DHCP, у якій буде здійснюватися автоматичне присвоєння адрес. Працюватимемо через оснащення DHCP (рис. 7.13).

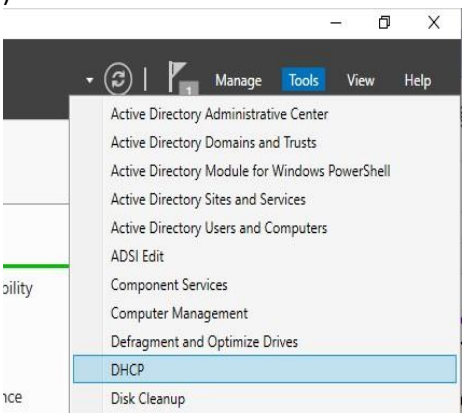


Рис. 7.13

У даній мережі здійснюється за протоколом IPv4, тому відшукайте відповідний вузол, і у його контекстному меню виберіть *New scope...* (рис. 7.14).

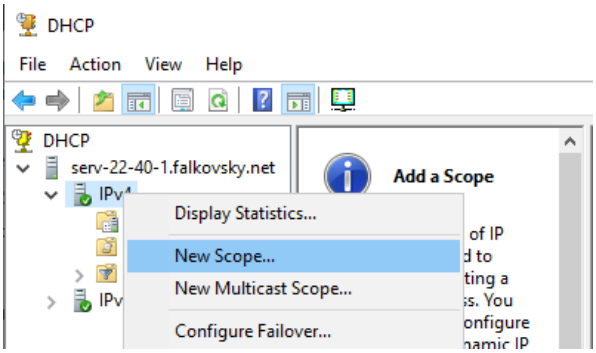


Рис. 7.14

Запуститься *Майстер створення нової області* (рис. 7.15).

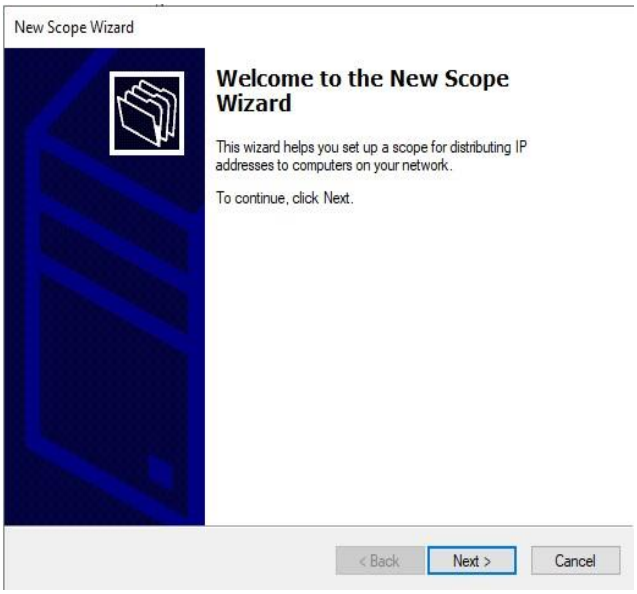


Рис. 7.15

Задайте ім’я області, а також введіть її короткий опис (рис. 7.16).

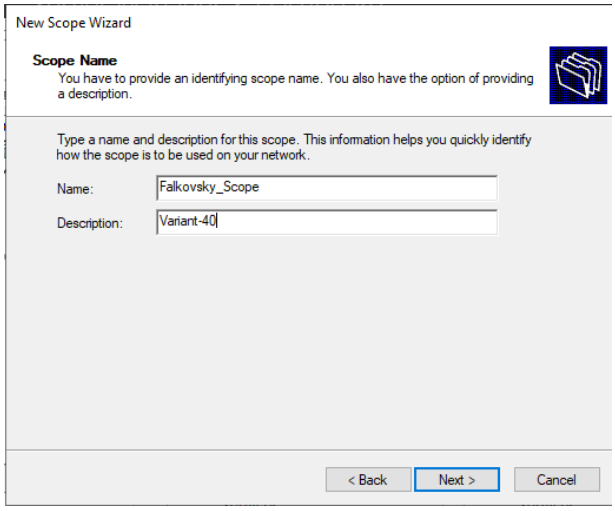


Рис. 7.16

Задайте діапазон адрес, які належатимуть до області. У прикладі як першу та останню адреси діапазону вказано, відповідно, першу та останню доступні адреси вузлів мережі (рис. 7.17). Також вкажіть маску підмережі або префікс (*Lenght*). Статичні адреси ми виключимо на наступному кроці.

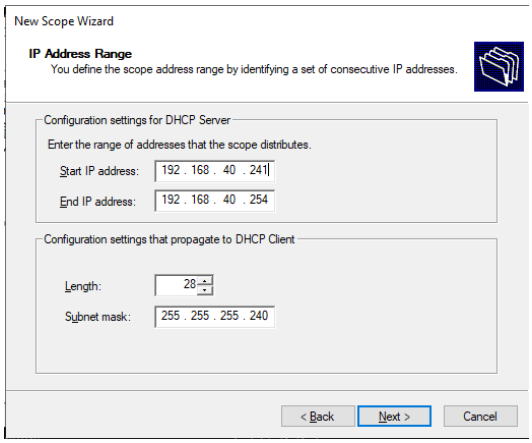


Рис. 7.17

Далі виключимо адреси, які присвоюватимуться статично. У прикладі на рис. 7.17-7.18 це адреси маршрутизатора (192.168.40.241), комутатора (192.168.40.242) та обох контролерів домену (192.168.40.243, 192.168.40.245), тобто діапазон від 192.168.40.241 до 192.168.40.245.

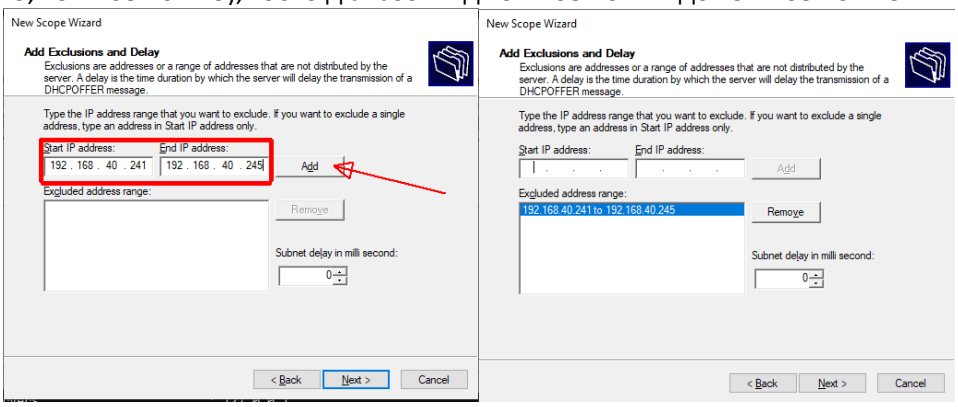


Рис. 7.18

На наступному кроці задайте тривалість оренди адреси (рис. 7.19).

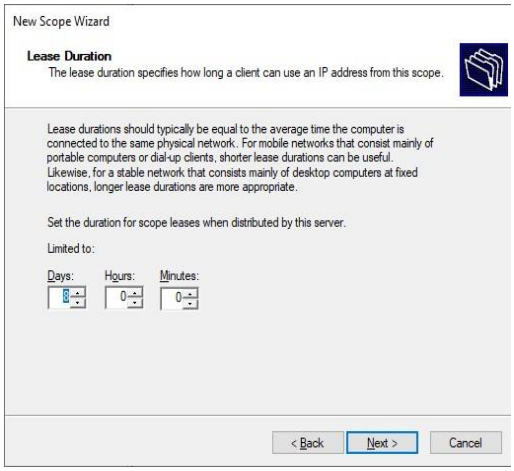


Рис. 7.19

Ми також сконфігуруємо роздачу за протоколом DHCP адреси шлюзу за замовчуванням та адреси DNS-сервера. Для цього на наступному кроці на запитання про додаткові налаштування відповідаємо *Yes, I want to configure these options now* (рис. 7.20).

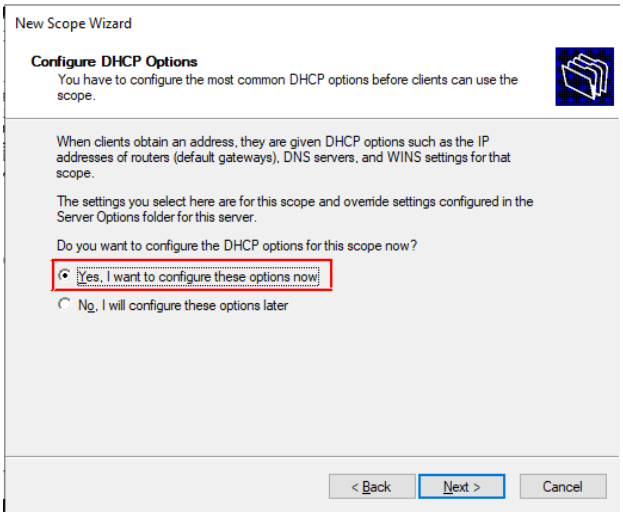


Рис. 7.20

У полі для адреси шлюзу за замовчуванням вкажемо адресу маршрутизатора (рис. 7.21).

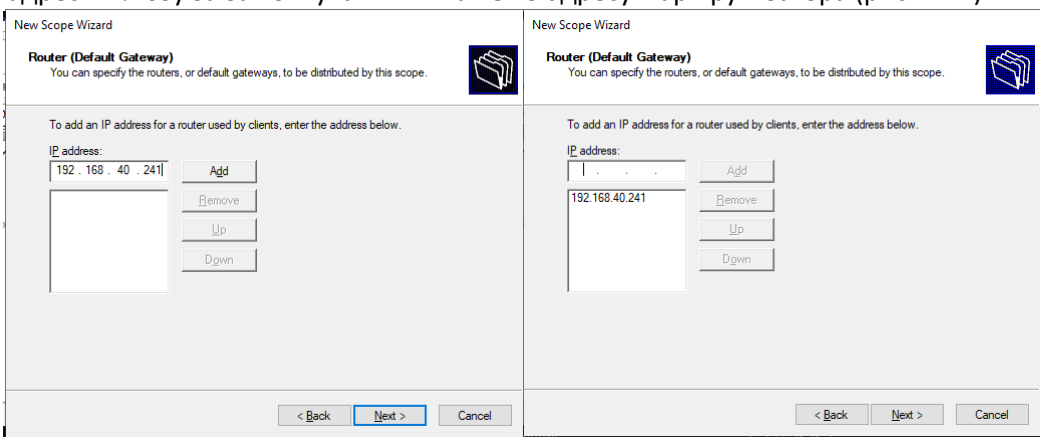


Рис. 7.21

Батьківський домен і DNS-сервер, імовірно, вже обрано автоматично підтверджуємо ці налаштування (рис. 7.22). Налаштування WINS пропускаємо.

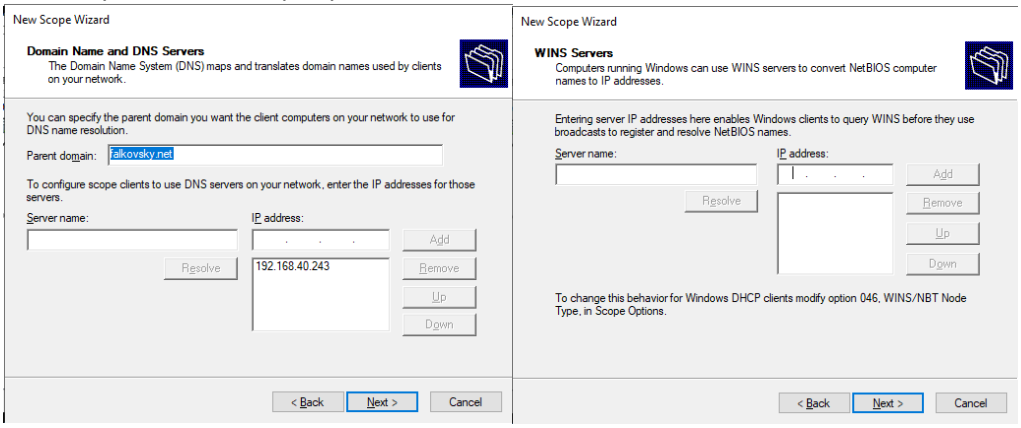


Рис. 7.22

Активовувати область DHCP будемо одразу (рис. 7.23). Майстер створення нової області завершив роботу. Натисніть Finish

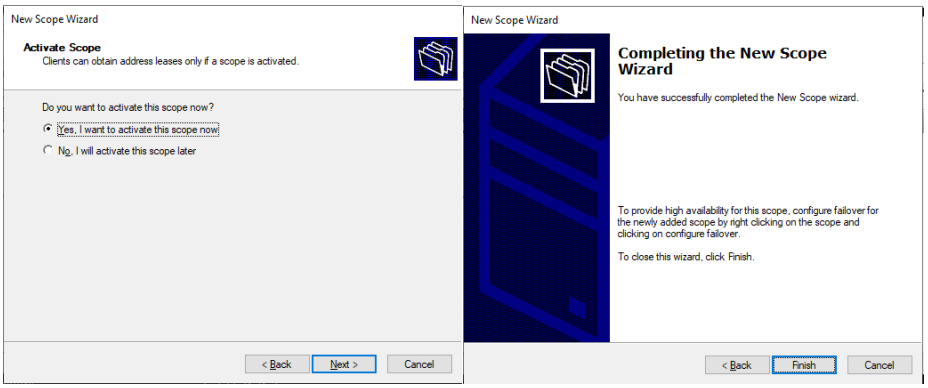


Рис. 7.23

Перевірка роботи DHCP-сервера

Щоб наочно побачити, як працює DHCP-сервер, на принаймні одній робочій станції відредагуйте налаштування мережі таким чином, щоб отримання IP-адреси та адреси DNS-сервера відбувалося автоматично. Після цього робоча станція має одержати дані адресації автоматично наприклад, подібно до даних (рис. 7.24).

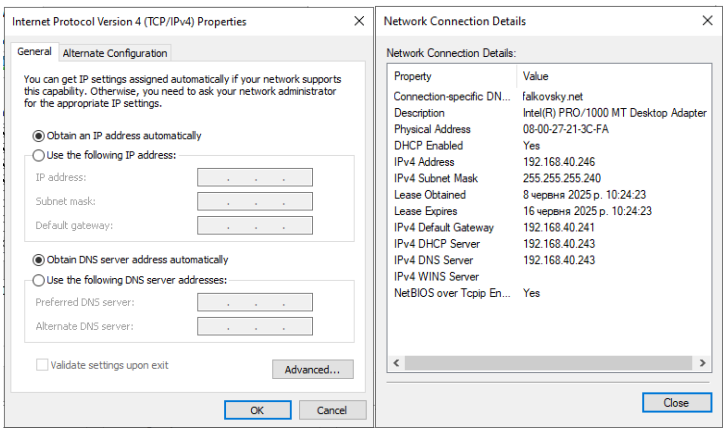


Рис. 7.24

Відомості про оренду адреси, виділеної цій робочій станції, мають відображатися на DHCP-сервері в оснащенні *DHCP*, вузол *Address Leases* (рис. 7.25).

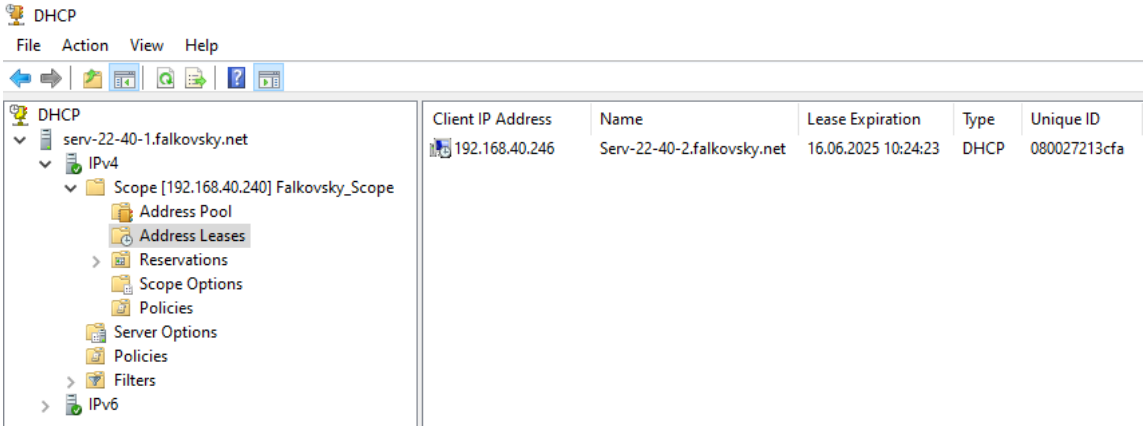


Рис. 7.25

Примітка. Якщо раніше ви налаштували один з об'єктів групових політик таким чином, щоб з даної робочої станції звичайним користувачам не дозволялося запускати налаштування, які належать до панелі завдань, то зараз для зміни мережних налаштувань вам знадобиться:

- або ввійти на робочій станції під обліковкою адміністратора домену (краще так);
- або скасувати відповідну групову політику.

Завдання №7.1

1. Відкорегуйте розроблену вами під час виконання лабораторної роботи №2 схему адресації таким чином, аби статичні адреси присвоювалися портам маршрутизатора, комутатора, а тако обом контролерам домену. Адреси робочих станцій мають конфігуруватися динамічно за DHCP.
2. На першому контролері домену здійсніть налаштування DHCP-сервера.

Вказівки

- Ім'я нової області (*new scope*) - *Surname_scope*, де *Surname* - ваше прізвище.
- Опис нової області (new scope description) - *Variant N*, де *N* - номер варіанту.
- Час оренди адреси встановіть *DD.HH.MM*, де *DD* - номер вашої групи, *HH* - номер вашого варіанту, *MM* - дата (день), коли виконувалася лабораторна робота.

3. Здійсніть перевірку зроблених налаштувань, задавши для довільної робочої станції автоматичне одержання її IP-адреси, адреси шлюзу за замовчуванням та адреси DNS-сервера і переконавшись, що робочій станції справді передається вся ця адресна інформація.
4. За допомогою оснащення *DHCP* на DHCP-сервері перегляньте відомості про оренду адресу, одержаної робочою станцією.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, **а також змінену схему адресації мережі**.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдання 7.1.

Робота №8. Основи використання PowerShell для адміністрування домену Active Directory

Мета: навчитися основних прийомів застосування командної оболонки PowerShell для роботи з Active Directory.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-7.

Теоретичні відомості та завдання до лабораторної роботи

ОКРЕМІ КОМАНДИ POWERSHELL ДЛЯ РОБОТИ З ACTIVE DIRECTORY

Командна оболонка PowerShell у Windows Server доступна з головною меню. Звідси можна викликати і саму оболонку PowerShell, і середовище для написання скриптів PowerShell ISE (рис. 8.1). Починати легше з Windows PowerShell, а скрипти доцільно писати і перевіряти у Windows PowerShell ISE.

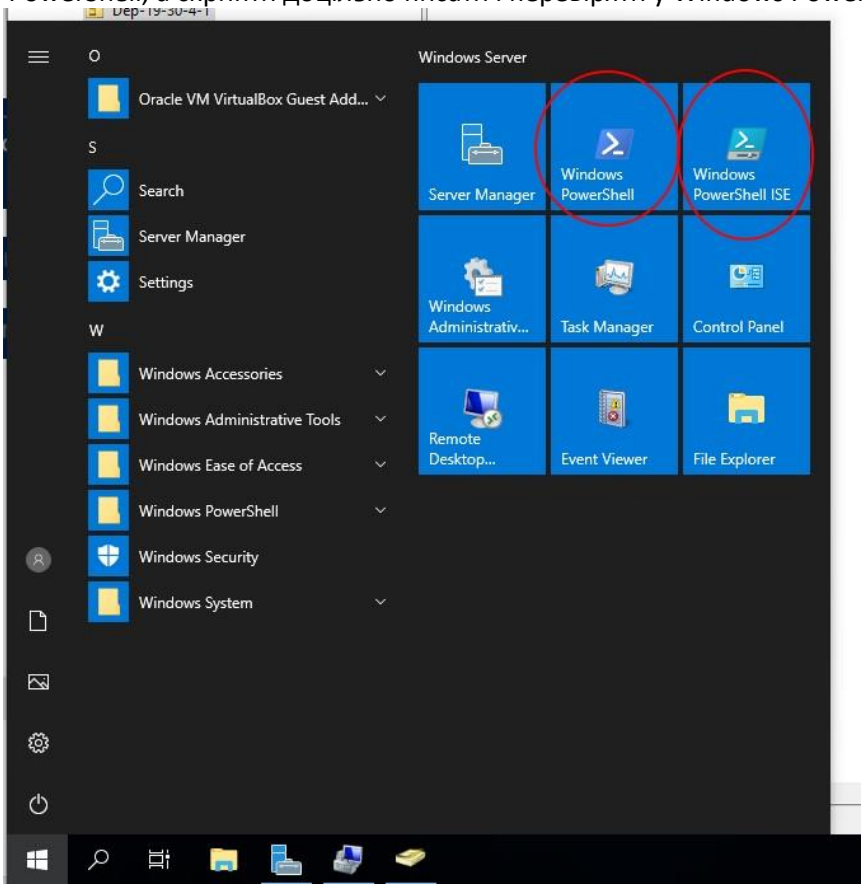


Рис. 8.1

Одержання відомостей про домен

Загальні відомості про домен виводить командлет Get-ADDomain. Введений без параметрів, цей командлет дає вивід, подібний до наступного:

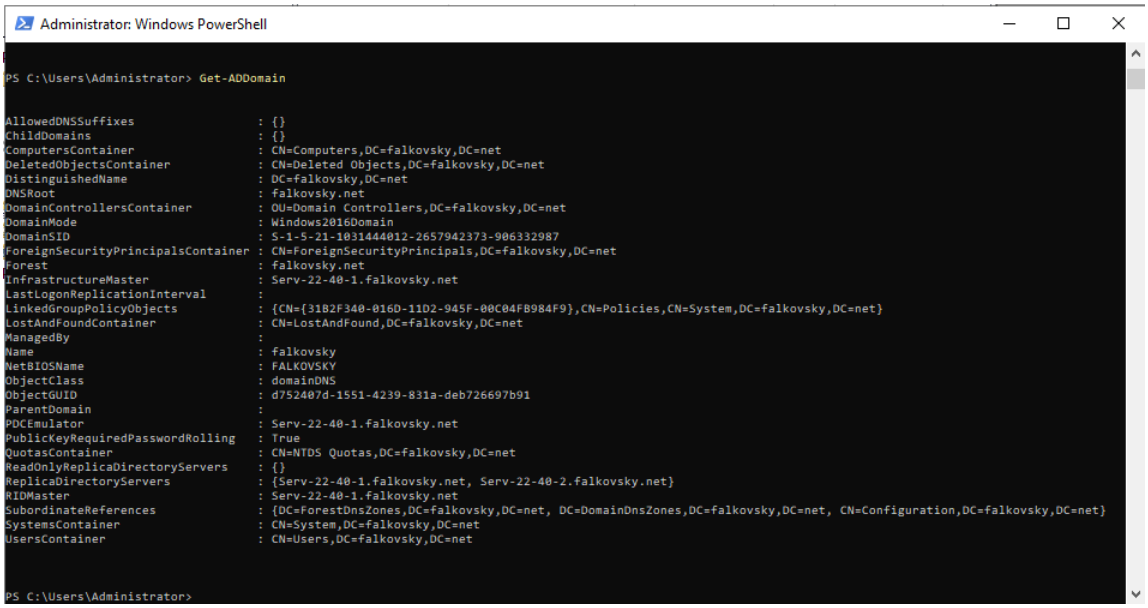


Рис. 8.2

Зверніть увагу на формат імен. Кожна складова доменного імені вказується окремо і супроводжується відомостями про структурний рівень.

Наприклад, поле DomainControllerContainer має вигляд:

```
DomainControllersContainer          : OU=Domain Controllers,DC=falkovsky,DC=net
```

Тобто *Domain Controllers* міститься на рівні організаційних одиниць (OU), що належить до домену *holovnia.net* (DC).

А ось поле DomainControllerContainer:

```
ComputersContainer                  : CN=Computers,DC=falkovsky,DC=net
```

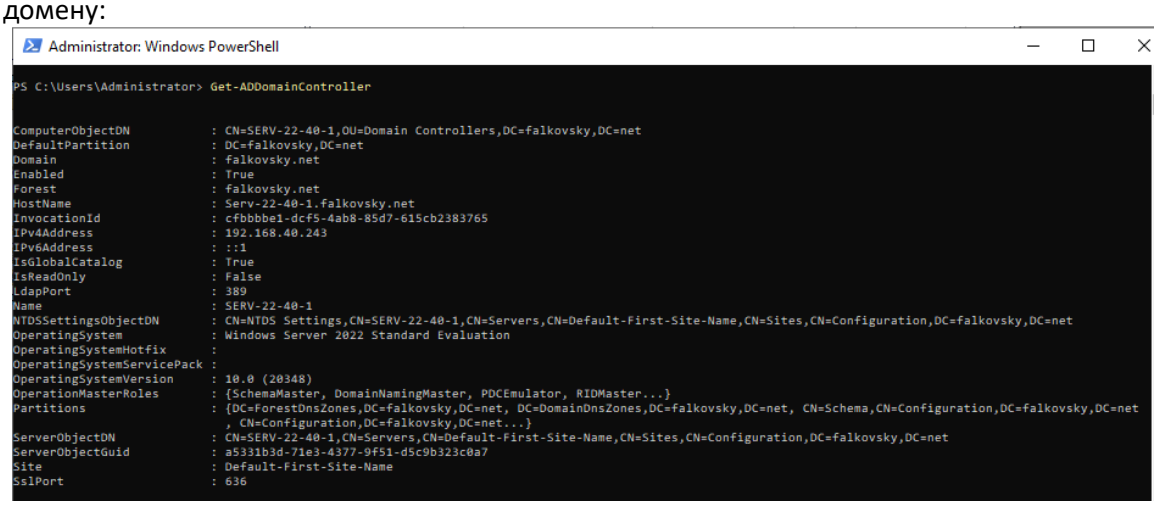
Тут *Computers* позначається як CN (*Common Name*), що у випадку Active Directory відповідає за контейнер.

Пояснення до деяких полів

- ChildDomains - дочірні домени (якщо є)
- ComputersContainer - контейнер для комп'ютерів домену, які не є контролерами домену (наприклад, робочих станцій)
- DeletedObjectsContainer - контейнер для видалених об'єктів
- DestinguishedName - унікальне ім'я домену
- DNSRoot - домен верхнього рівня
- DomainControllerContainer - контейнер для контролерів домену
- DomainSID - SID домену (зазвичай утворюється на основі SID першого контролеру домену)
- Forest - ім'я лісу (у невеликих мережах на основі AD - часто тотожне імені домену)
- LinkedGroupPolicyObjects - об'єкти групової політики рівня домену
- Name - скорочене ім'я домену (те, яке використовується під час входу користувачів, наприклад)
- ParentDomain - ім'я батьківського домену (якщо є)
- ReplicaDirectoryServers - сервери, які беруть участь у реплікації
- SystemContainer - системний контейнер домену

- UsersContainer - контейнер для користувачів домену

Для виведення відомостей про контролер домену, можна скористатися командлетом Get-ADDomainController. За замовчуванням, буде показано інформацію про найближчий контролер домену:

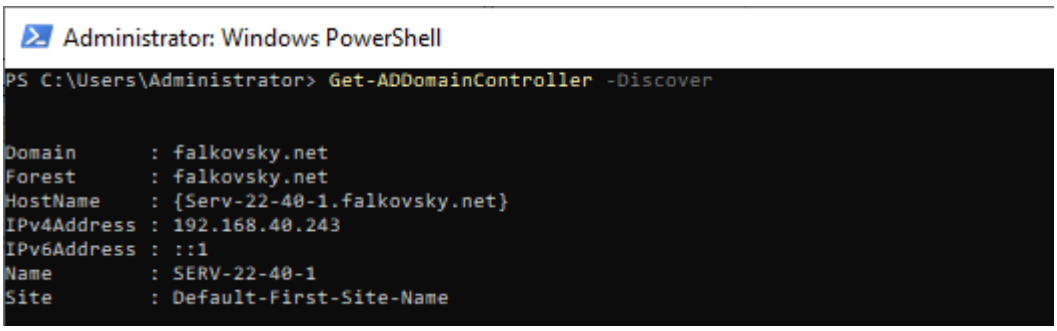


Якщо контролерів домену декілька, переглянути відомості про всі зручно за допомогою параметра -Filter та підстановочних символів. Наприклад, всі контролери домену:

Get-ADDomainController -Filter *

Якщо вжити параметр -Discover, командлет виведе інформацію про найближчий доступний контролер домену:

Get-ADDomainController -Discover Наприклад:



Найближчий доступний у межах того самого сайту контролер у даному випадку визначає процес *DC locator*.

Якщо ви вводите командлет Get-ADDomainController на одному з контролерів домену, то можна дати вказівку обрати як найближчий інший контролер домену, а не той, з якого було запущено команду. Для цього треба додати параметр -AvoidSelf:

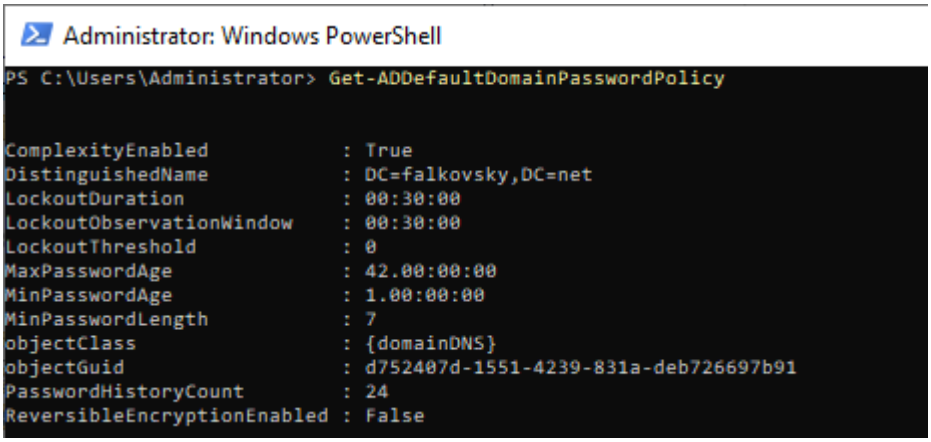
Get-ADDomainController -Discover -AvoidSelf

Вивести інформацію про конкретний контролер домену можна також вказавши його ім'я:

PS C:\> Get-ADDomainController -Identity *DCName*

де *DCName* - ім'я контролера домену.

Групові політики, які стосуються паролів, у багатьох випадках встановлюються на рівні домену. Тому для їх перегляду можна скористатися окремим командлетом Get-ADDefaultDomainPasswordPolicy. Наприклад:



Завдання №8.1

1. Запустіть командну оболонку PowerShell на одному з контролерів вашого домену. Засобами оболонки PowerShell організуйте виведення на екран наступних відомостей:

- Інформація про поточний домен
- Відомості про поточний контролер домену
- Відомості про найближчий контролер домену (але не той, з якого ви вводите команду)
- Відомості про всі контролери, доступні в межах даного домену (одним командлетом)
- Інформація про будь-який із наявних у вас контролерів домену за його ім'ям
- Наявні налаштування групових політик щодо паролів у домені

2. Спираючись на інформацію, одержану під час виконання п. 1, **дайте відповіді на наступні запитання. Поряд вкажіть команди, на основі яких ви одержали ці відповіді.**

- Яке ім'я поточного домену?
- Який SID присвоєно цьому домену?
- Чи є у цього домену дочірні домени?
- Яке ім'я поточного лісу?
- Які імена в контролерів домену? Які IP-адреси цих контролерів?
- Яка операційна система працює на контролерах домену (редакція, версія)? **Не плутати з полем *DomainMode*! (там може фігурувати ім'я іншої версії)**
- Які контролери домену беруть участь у реплікації?
- У межах якого сайту працюють контролери домену?
- Чи є у домені контролери ReadOnly (лише для читання)? Яка мінімальна довжина паролю встановлена груповими політиками для даного домену?
- Яка максимальна кількість спроб дається на введення паролю?

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Робота зі структурою домену

Далі в методичних матеріалах усі приклади та скріншоти наведено на основі Windows Server 2019. Однак методика повністю застосовна і до Server 2022, оскільки обидві версії використовують однакову версію PowerShell за замовчуванням — Windows PowerShell 5.1. Усі команди, сценарії та модулі, що використовуються в цій методиці, підтримуються без змін у Server 2022.

Загальну інформацію про структуру домену (ім'я, батьківський та дочірні домени, SID домену, окремі контейнери та організаційні одиниці тощо) можна почерпнути з виводу командлета Get-ADDomain, описаного вище у цій лабораторній роботі.

Однак для більш ґрунтовної роботи зі структурою домену потрібно мати детальніше уявлення про неї. Переглянути інформацію всі організаційні одиниці домену можна за допомогою командлета Get-ADOrganizationalUnit. Командлет дає доступ до багатьох відомостей про організаційні одиниці (детальніше - у *Microsoft Docs*), і у багатьох випадках є сенс ці відомості відформатувати та відфільтрувати. Так, у прикладі нижче виведено інформацію про всі організаційні одиниці домену, однак із доступних полів обрано тільки скорочені та повні імена цих одиниць:

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter 'Name -like "*"' | Format-Table Name, DistinguishedName -A

Name               DistinguishedName
----               -----------------
Domain Controllers OU=Domain Controllers,DC=holovnia,DC=net
Branch-19-30-1     OU=Branch-19-30-1,DC=holovnia,DC=net
Branch-19-30-2     OU=Branch-19-30-2,DC=holovnia,DC=net
Branch-19-30-3     OU=Branch-19-30-3,DC=holovnia,DC=net
Dep-19-30-1-1      OU=Dep-19-30-1-1,OU=Branch-19-30-1,DC=holovnia,DC=net
Dep-19-30-1-2      OU=Dep-19-30-1-2,OU=Branch-19-30-1,DC=holovnia,DC=net
Dep-19-30-1-3      OU=Dep-19-30-1-3,OU=Branch-19-30-1,DC=holovnia,DC=net
B19301-Admins      OU=B19301-Admins,OU=Branch-19-30-1,DC=holovnia,DC=net
Dep-19-30-2-1      OU=Dep-19-30-2-1,OU=Branch-19-30-2,DC=holovnia,DC=net
Dep-19-30-3-1      OU=Dep-19-30-3-1,OU=Branch-19-30-3,DC=holovnia,DC=net
B19302-Admins      OU=B19302-Admins,OU=Branch-19-30-2,DC=holovnia,DC=net
Computers-19-30    OU=Computers-19-30,DC=holovnia,DC=net
Comp-Branch-19-30-1 OU=Comp-Branch-19-30-1,OU=Computers-19-30,DC=holovnia,DC=net
```

За повними іменами видно, що окремі організаційні одиниці містяться всередині інших організаційних одиниць. Наприклад, OU Dep-19-30-1-1 міститься всередині OU Branch-19-30-1:

```
Dep-19-30-1-1       OU=Dep-19-30-1-1,OU=Branch-19-30-1,DC=holovnia,DC=net
```

У наступному прикладі додано маску для імен організаційних одиниць - буде виведено лише ті з них, імена яких містять буквосполучення Br:

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter 'Name -like "Br*"' | Format-Table Name, DistinguishedName -A

Name           DistinguishedName
----           -----------------
Branch-19-30-1 OU=Branch-19-30-1,DC=holovnia,DC=net
Branch-19-30-2 OU=Branch-19-30-2,DC=holovnia,DC=net
Branch-19-30-3 OU=Branch-19-30-3,DC=holovnia,DC=net
```

З виводу можна бачити, що всі ці організаційні одиниці містяться безпосередньо в домені *holovnia.net*:

```
Name           DistinguishedName
----           -----------------
Branch-19-30-1 OU=Branch-19-30-1,DC=holovnia,DC=net
Branch-19-30-2 OU=Branch-19-30-2,DC=holovnia,DC=net
Branch-19-30-3 OU=Branch-19-30-3,DC=holovnia,DC=net
```

Командлет New-ADOrganizationalUnit дає змогу створювати нові організаційні одиниці.

Для створення нової організаційної одиниці безпосередньо на рівні домену вкажіть ім'я цієї організаційної одиниці:

New-ADOrganizationalUnit -Name *OUName* Наприклад:

```
PS C:\Users\Administrator> New-ADOrganizationalUnit -Name Branch-19-30-4
```

Переконаймося, що нову організаційну одиницю справді створено:

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter 'Name -like "Br*"' | Format-Table Name, DistinguishedName -A

Name           DistinguishedName
----           -----------------
Branch-19-30-1 OU=Branch-19-30-1,DC=holovnia,DC=net
Branch-19-30-2 OU=Branch-19-30-2,DC=holovnia,DC=net
Branch-19-30-3 OU=Branch-19-30-3,DC=holovnia,DC=net
Branch-19-30-4 OU=Branch-19-30-4,DC=holovnia,DC=net
```

Якщо треба створити нову організаційну одиницю всередині іншої організаційної одиниці, треба вказати шлях.

Наприклад, щоб всередині OU *Branch-19-30-4* створити OU *Dep-19-30-4-1*, скористаємося командою:

```
PS C:\Users\Administrator> New-ADOrganizationalUnit -Name Dep-19-30-4-1 -Path 'OU=Branch-19-30-4,DC=holovnia,DC=net'
```

З'явилася нова організаційна одиниця *Dep-19-30-4-1*, і вона справді є дочірньою для OU *Branch-19-30-4*:

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter 'Name -like "Dep*"' | Format-Table Name, DistinguishedName -A

Name           DistinguishedName
----           -----------------
Dep-19-30-1-1 OU=Dep-19-30-1-1,OU=Branch-19-30-1,DC=holovnia,DC=net
Dep-19-30-1-2 OU=Dep-19-30-1-2,OU=Branch-19-30-1,DC=holovnia,DC=net
Dep-19-30-1-3 OU=Dep-19-30-1-3,OU=Branch-19-30-1,DC=holovnia,DC=net
Dep-19-30-2-1 OU=Dep-19-30-2-1,OU=Branch-19-30-2,DC=holovnia,DC=net
Dep-19-30-3-1 OU=Dep-19-30-3-1,OU=Branch-19-30-3,DC=holovnia,DC=net
Dep-19-30-4-1 OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net
```

Вивести всі організаційні одиниці, які містяться всередині даної, можна за допомогою параметра -SearchBase:

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -LDAPFilter '(name=*)' -SearchBase 'OU=Branch-19-30-4,DC=holovnia,DC=net' -SearchScope OneLevel | Format-Table Name

Name
----
Dep-19-30-4-1
```

Створити нового користувача домену можна за допомогою командлета New-ADUser. У цього командлета дуже багато параметрів (детальніше - у *Microsoft Docs*). Скористаймося деякими з них:

New-ADUser -Name *Логін* -UserPrincipalName *Логін@доменне.ім_я*

-GivenName *Ім_я* -Initials *Ініціали* -Surname *Прізвище*

-Path *Повний_шлях_до_організаційної_одиниці* Наприклад:

```
PS C:\Users\Administrator> New-ADUser -Name "dep41-poa" -UserPrincipalName "dep41-poa@holovnia.net" -GivenName
 "Oleh" -Initials "A." -Surname "Pinchuk" -Path "OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net"
```

Вивести відомості про користувача можна командлетом Get-ADUser. Наприклад, так:

```
PS C:\Users\Administrator> Get-ADUser -Identity dep41-poa -Properties *
```

Оскільки для параметра -Properties задано маску *, то буде показано всі властивості облікового запису, і вивід стане доволі довгим. Проте в ньому можна помітити, що наразі обліковий запис відключений:

```
DistinguishedName                 : CN=dep41-poa,OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net
Division                          :
DoesNotRequirePreAuth             : False
dSCorePropagationData             : {01.01.1601 2:00:00}
EmailAddress                      :
EmployeeID                        :
EmployeeNumber                    :
Enabled                           : False
Fax                               :
GivenName                         : Oleh
HomeDirectory                     :
HomedirRequired                   : False
HomeDrive                         :
HomePage                          :
```

Також для обліковки не задано пароль. На рівні властивостей це виглядає так: пароль ніколи не було встановлено, але термін його дії скінчився:

```
PasswordExpired                   : True
PasswordLastSet                   :
PasswordNeverExpires              : False
PasswordNotRequired               : False
POBox                             :
```

Так відбувається тому, що пароль є обов'язковим (окрім тих випадків, коли властивість *PasswordNotRequired* має значення *True*). Задамо новоствореному користувачу тимчасовий пароль:

```
PS C:\Users\Administrator> Set-ADAccountPassword -Identity dep41-poa -Reset
Please enter the desired password for 'CN=dep41-poa,OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net'
Password: ********
Repeat Password: ********
```

Параметр -Reset потрібний для того, аби перед новим паролем не вводити старий пароль, котрого поки не було задано.

Увімкнемо обліковий запис та, оскільки пароль тимчасовий, додамо вимогу обов'язкової зміни паролю під час наступного входу цього користувача:

```
PS C:\Users\Administrator> Set-ADUser -Identity dep41-poa -Enabled $true -ChangePasswordAtLOgon $true
```

Тепер обліковий запис увімкнено:

```
PS C:\Users\Administrator> Get-ADUser -Identity dep41-poa -Properties Enabled


DistinguishedName : CN=dep41-poa,OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net
Enabled           : True
GivenName         : Oleh
Name              : dep41-poa
ObjectClass       : user
ObjectGUID        : 9413fa0a-bd49-4a2f-a463-f21ed849fcff
SamAccountName    : dep41-poa
SID               : S-1-5-21-3806899930-2341899199-3056094349-1123
Surname           : Pinchuk
UserPrincipalName : dep41-poa@holovnia.net
```

За замовчуванням облікові записи додаються до групи *Domain Users*, і нас це влаштовує.

Якщо потрібно додати обліковий запис до іншої групи, можна скористатися командлетами New-AddGroup (створення нової групи) та AddADGroupMember (додавання нових членів групи). Більше про ці командлети є в *Microsoft Docs*.

Командлет Search-ADAccount також надає можливості для пошуку облікових записів користувачів, комп'ютерів та служб за певною ознакою.

Наприклад, якщо треба відшукати облікові записи, котрі було заблоковано, введемо наступну команду:

```
PS C:\Users\Administrator> Search-ADAccount -LockedOut | Format-Table Name,ObjectClass -A

Name            ObjectClass
----            -----------
Larysa P. Kotyk user
```

Командлет Search-ADAccount має ще багато корисних параметрів. Більше про доступні параметри та приклади їх використання на практиці - у *Microsoft Docs*.

Щоб розблокувати користувача, нам знадобиться його логін (поле *SamAccountName*). Вивести потрібну інформацію можна, наприклад, так:

```
PS C:\Users\Administrator> Get-ADUser -Filter 'Name -like "*Kotyk"' | Format-Table Name,SamAccountName -A

Name            SamAccountName
----            --------------
Larysa P. Kotyk dep11-klp
```

Тепер розблокуємо користувача за допомогою командлета UnlockADAccount, вказавши логін користувача як значення параметра *-Identity*:

```
PS C:\Users\Administrator> Unlock-ADAccount -Identity dep11-klp
```

Переконаймося, що такого заблокованого облікового запису більше немає:

```
PS C:\Users\Administrator> Search-ADAccount -LockedOut | Format-Table Name,ObjectClass -A
```

Після цього може знадобитися змінити користувачу пароль та зобов'язати його змінити пароль під час наступного входу.

Видалення облікового запису користувача робиться командлетом Remove-ADUser. Це сама та ситуація, коли незайве застосувати режим прототипування (параметр -*WhatIf*). Так зменшується ризик помилково вилучити не той обліковий запис:

```
PS C:\Users\Administrator> Remove-ADUser -Identity dep41-poa -WhatIf
What if: Performing the operation "Remove" on target "CN=dep41-poa,OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net".
```

Якщо все правильно, повторюємо команду без параметра -*WhatIf*:

```
PS C:\Users\Administrator> Remove-ADUser -Identity dep41-poa

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove" on target "CN=dep41-poa,OU=Dep-19-30-4-1,OU=Branch-19-30-4,DC=holovnia,DC=net".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
```

Зверніть увагу, що комнадлет Remove-ADUser за замовчуванням працює в режимі підтвердження, хоча параметра -*Confirm* і не вказано.

Переконаймося, що користувача справді видалено за допомогою командлета Get-ADUser. Уважно читайте повідомлення, які у даному випадку виводить вам команда. Якщо команду введено правильно, але такого користувача не знайдено, вгорі виводу буде відповідна інформація:

```
PS C:\Users\Administrator> Get-ADUser -Identity dep41-poa -Properties *
Get-ADUser : Cannot find an object with identity: 'dep41-poa' under: 'DC=holovnia,DC=net'.
At line:1 char:1
+ Get-ADUser -Identity dep41-poa -Properties *
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (dep41-poa:ADUser) [Get-ADUser], ADIdentityNotFoundException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundExceptio
   n,Microsoft.ActiveDirectory.Management.Commands.GetADUser
```

Завдання №8.2

1. Засобами PowerShell створіть у корені домену організаційну одиницю *BranchGG-NN-4*.
2. Усередині OU *Branch-GG-NN-4* через PowerShell створіть дві дочірні OU: *DepGG-NN-4-1* та *Dep-GG-NN-4-2*.
3. Засобами PowerShell створіть в OU *Dep-GG-NN-4-1* та *Dep-GG-NN-4-2* по одному користувачу. Під час іменування користувачів дотримуйтеся тих самих правил, які ви обрали для імен користувачів у лабораторній роботі №4, коли створювали структуру домену.

Наступні дії також виконайте засобами PowerShell (окрім спроб входу користувачів).

4. Організуйте виведення відомостей про новостворених користувачів - окремо про першого, окремо про другого.
5. Забезпечте двом новостворениим користувачам можливість входу в систему та переконайтеся, що обидва вони можуть увійти з довільної побочої станції домену.
6. Заблокуйте обліковий запис першого користувача шляхом кількаразового введення ним неправильного паролю.
7. Здійсніть пошук облікових записів домену, котрі зараз заблоковано.
8. Розблокуйте обліковий запис першого користувача. Задайте йому новий тимчасовий пароль та у примусовому порядку зобов’яжіть змінити пароль під час наступного входу.
9. Видаліть облікові записи першого та другого користувачів у режимі прототипування.
10. Видаліть обліокві записи першого та другого користувачів насправді. Переконайтеся, що облікові записи справді видалено.

Звіт має містити скриншоти зроблених налаштувань та опис основних дій.

Дослідження налаштувань DNS

Наведемо також окремі команди для дослідження налаштувань DNS.

Щоб вивести всі DNS-записи типу A, введіть командлет GetDnsServerResourseRecord з параметром -RRType “A”:

```
PS C:\Users\Administrator> Get-DnsServerResourceRecord -ZoneName "holovnia.net" -RRType "A"

HostName                  RecordType Type       Timestamp           TimeToLive      RecordData
--------                  ---------- ----       ---------           ----------      ----------
@                         A          1          22.11.2021 17:00:00 00:10:00        220.19.30.4
@                         A          1          22.11.2021 17:00:00 00:10:00        220.19.30.3
DomainDnsZones            A          1          22.11.2021 17:00:00 00:10:00        220.19.30.3
ForestDnsZones            A          1          22.11.2021 17:00:00 00:10:00        220.19.30.3
router                    A          1          0                   01:00:00        220.19.30.1
WIN-8T2CASENUDU           A          1          22.11.2021 17:00:00 00:20:00        220.19.30.4
win-sdj836u8svc           A          1          0                   01:00:00        220.19.30.3
WS-19-30-5                A          1          15.11.2021 16:00:00 00:20:00        220.19.30.5
```

Аналогічно можна переглянути записи інших типів - наприклад, записи про сервери імен (тип *NS*):

```
PS C:\Users\Administrator> Get-DnsServerResourceRecord -ZoneName "holovnia.net" -RRType "NS"

HostName                  RecordType Type       Timestamp           TimeToLive      RecordData
--------                  ---------- ----       ---------           ----------      ----------
@                         NS         2          0                   01:00:00        win-sdj836u8svc.holovnia.net.
_msdcs                    NS         2          0                   01:00:00        win-sdj836u8svc.holovnia.net.
```

Перевірити доступність DNS-сервера можна командлетом TestDnsServer за IP-адресою:

```
PS C:\Users\Administrator> Test-DnsServer -IPAddress 220.19.30.3

IPAddress    Result  RoundTripTime TcpTried UdpTried
---------    ------  ------------- -------- --------
220.19.30.3 Success 00:00:11      True     True
```

Завдання №8.3

1. Засобами PowerShell організуйте виведення відомостей про DNS-записи типів A, AAAA, та NS у зоні прямого перегляду.

2. За допомогою PowerShell перевірте наявність доступних DNS-серверів за IPадресами першого та другого контролерів домену. Поясніть одержані результати.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

СТВОРЕННЯ ПРОСТИХ СКРИПТІВ POWERSHELL

Налаштування політики виконання скриптів

На робочих станціях та в локальних Windows-системах, які не входять до складу домену, запуск скриптів у системі за замовчуванням не дозволено. Водночас, у Windows Server, навпаки, стандартною є політика виконання *RemoteSigned* для області *LocalMachine*.
Перевірити, якими є поточні налаштування політик виконання для скриптів у вашій системі, можна за допомогою командлета Get-ExecutionPolicy -List:

```
PS C:\Users\Administrator> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser       Undefined
 LocalMachine    RemoteSigned
```

Детальніше про створення та запуск скриптів - у матеріалах лекції на відповідну тему.

Завдання №8.4

1. На контролері домену створіть та протестуйте скрипт, який виводить на екран повідомлення *“Hello world!”*.

2. Використовуючи команди, які ви виконували у межах завдань Напишіть скрипт lab8-*GG-NN*.ps1, який виконує наступні дії:

- виводить відомості про домен загалом, про найближчий контролер домену, а також про найближчий контролер домену, але не той, з якого запущено скрипт;
- виводить інформацію про наявність доступних DNS-серверів за IPадресами першого та другого контролерів домену;
- створює у корені домену організаційну одиницю *Branch-GG-NN-5;*
- всередині OU *Branch-GG-NN-5* створює дочірню OU *Dep-GG-NN-5-1;*
- в OU *Dep-GG-NN-5-1* створює обліковий запис користувача, задає йому тимчасовий пароль, забезпечує можливість входу і зобов’язує користувача змінити тимчасовий пароль під час першого входу.

Під час іменування користувачів дотримуйтеся тих самих правил, які ви обрали для імен користувачів, коли створювали структуру домену.

3. Перевірте роботу скрипта, запустивши його на контролері домену і переглянувши результати його роботи.

Звіт має містити скриншоти використаних команд, скриншот скрипта та одержаних виводів, **а також програмний код скрипта** lab8- *GG-NN* **(окремим файлом, прикріпленим до листа - розширення приберіть для уникнення проблем з вкладанням)**.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 8.1-8.4.

Рекомендовані джерела

1) ActiveDirectory Module - Microsoft Docs. URL: https://docs.microsoft.com/en-us/powershell/module/activedirectory/?
view=windowsserver2019-ps
2) E. Wilson. Windows PowerShell 3.0 Step by Step. - Microsoft, 2013.
3) M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020 (p. 82).

Робота №9. Налаштування служб віддаленого робочого столу на базі Windows Server 2022 та Active Directory

Мета: навчитися налаштовувати основні служби віддаленого робочого столу для домену Active Directory на базі Windows Server 2022.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-8.

Теоретичні відомості та завдання до лабораторної роботи

Встановлення служб віддаленого робочого столу у Windows Server

Для встановлення служб віддаленого робочого столу (Remote Desktop Services) у Windows Server 2022 у вікні Server Manager оберіть *Manage → Add Roles and Features* (рис. 9.1).

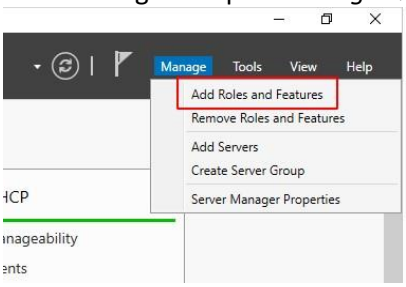


Рис. 9.1

Цього разу знадобиться вибрати другий пункт - *Remote Desktop Services Installation* (рис. 9.2). Надалі він дозволяє налаштувати служби віддаленого робочого столу як на основі сесій віддаленого робочого столу, так і на основі віртуальних машин.

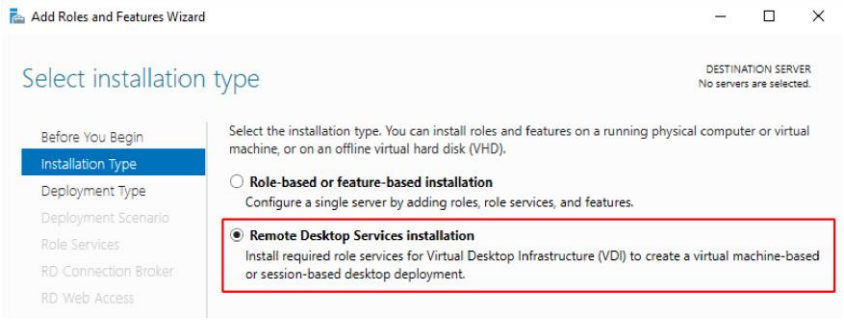


Рис. 9.2

Далі обираємо опцію стандартного розгортання (рис. 9.3).

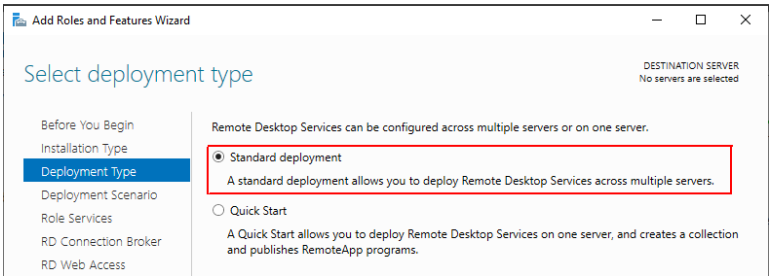


Рис. 9.3

На наступному етапі пропонується обрати сценарій розгортання. Обираємо служби віддаленого столу на основі віддалених сесій / *session-based desktop deployment* (рис. 9.4). Цей сценарій потребує значно менше ресурсів для роботи, що є визначальним фактором для нашої навчальної моделі мережі.

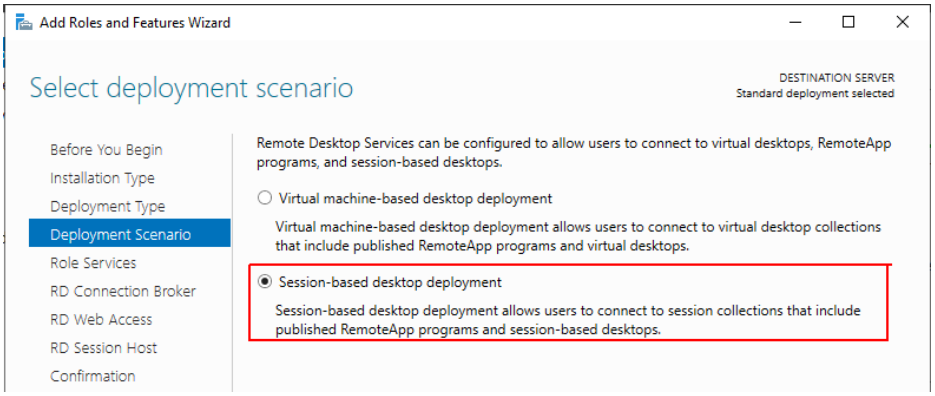


Рис. 9.4

Далі у вікні майстра виводиться перелік служб, які буде встановлено на наступних кроках (рис. 9.5). Ознайомтеся з переліком і натисніть *Next*.

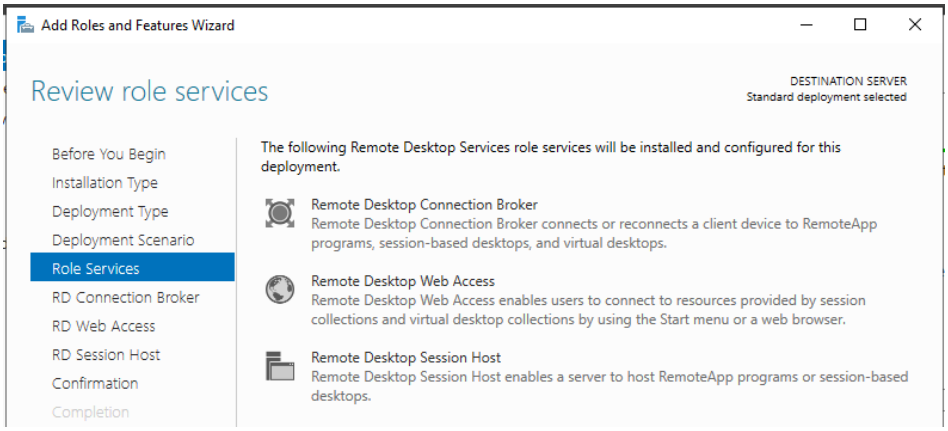


Рис. 9.5

Далі пропонується обрати із наявного пулу серверів ті з них, на які треба встановити обрані служби. У нашому випадку щоразу обираємо перший контролер домену. На рис. 9.6 цей сервер обрано для встановлення RD Connection Broker (рис. 9.6).

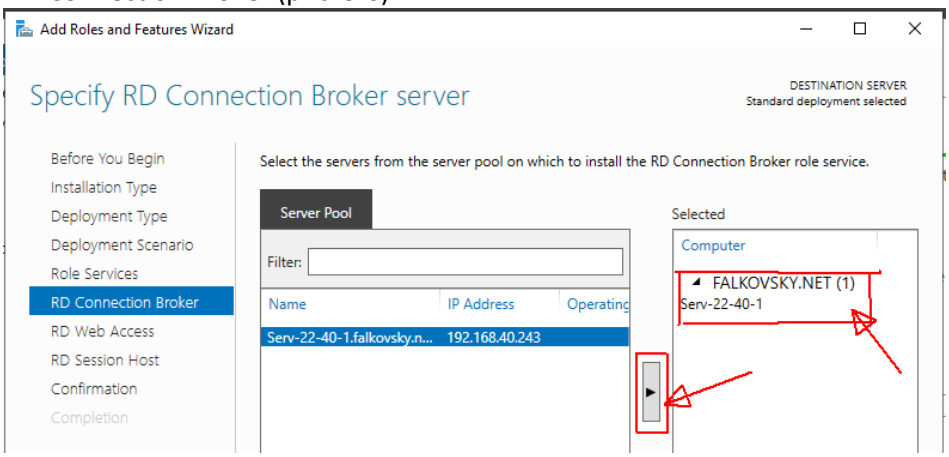


Рис. 9.6

На рис. 9.7 показано, що той самий сервер обрано для компонента RD Web Access.

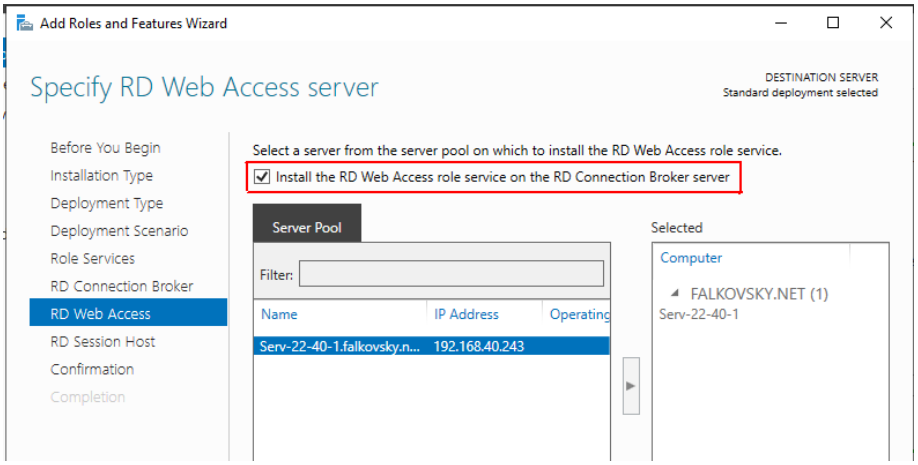


Рис. 9.7

І нарешті, той самий сервер обрано для RD Session Host (рис. 9.8).

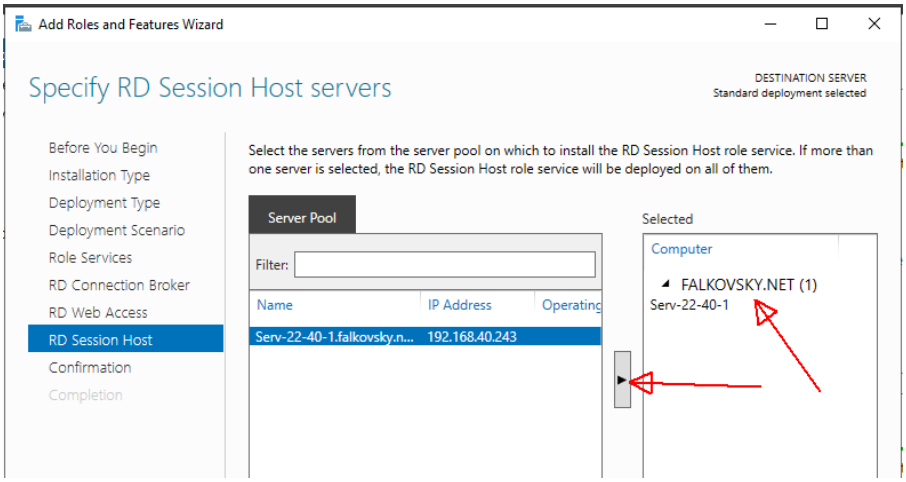


Рис. 9.8

Підготовку завершено - можна розпочинати встановлення. Варто встановити прапорець про перезавантаження системи. Процес встановлення може зайняти деякий час. Після успішного завершення вікно майстра виглядатиме подібно до зображеного (рис. 9.9).

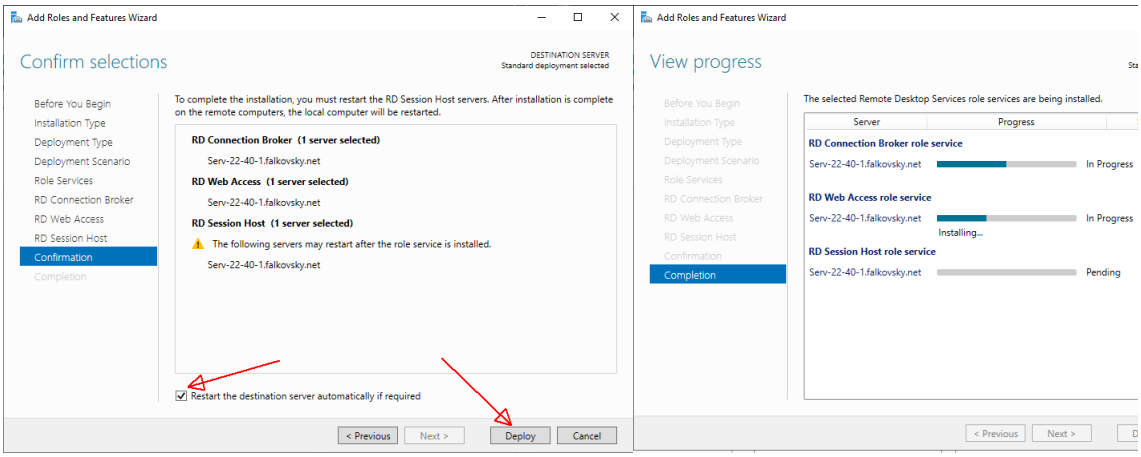


Рис. 9.9

Встановлення необхідних компонентів завершено, а відповідна група опцій з’явилися у вікні Server Manager (рис. 9.10). Тепер треба налаштувати встановлені служби.

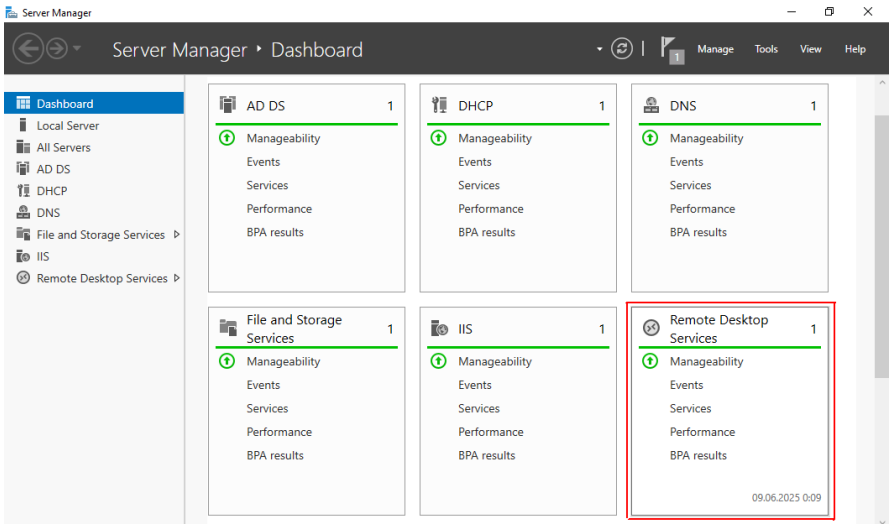


Рис. 9.10

Завдання №9.1

- Користуючись інструкціями, поданими вище, здійсніть встановлення служб віддаленого робочого столу на першому контролері домену з ОС Windows Server.
- Переконайтеся, що служби віддаленого робочого столу (Remote Desktop Services) було успішно встановлено.

Звіт має містити скриншоти одержаних відомостей та опис основних дій.

Налаштування служб віддаленого робочого столу у Windows Server

Далі потрібно виконати налаштування встановлених компонентів RDS. У вікні *Server Manager* перейдіть до групи *Remote Desktop Services*. У нижній частині області Overview відображатиметься діаграма відповідних служб (рис. 9.11). Деякі з них уже мають базові необхідні налаштування, а деякі ще треба доналаштувати - їх позначено зеленими плюсами. У цій роботі ми не будемо налаштовувати службу RD Gateway, оскільки наша модель мережі наразі не має виходу у зовнішню мережу. Натомість сконфігуруємо RD Licensing (рис. 9.11).

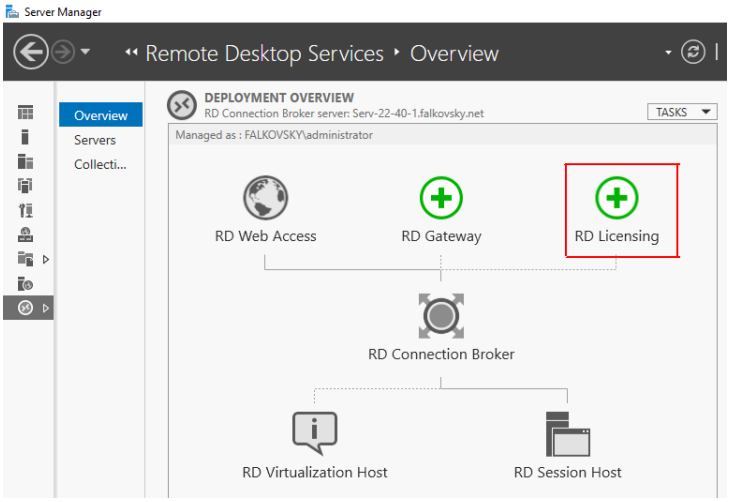


Рис. 9.11

Оберемо у ролі серверу ліцензій перший контролер домену (рис. 9.12).

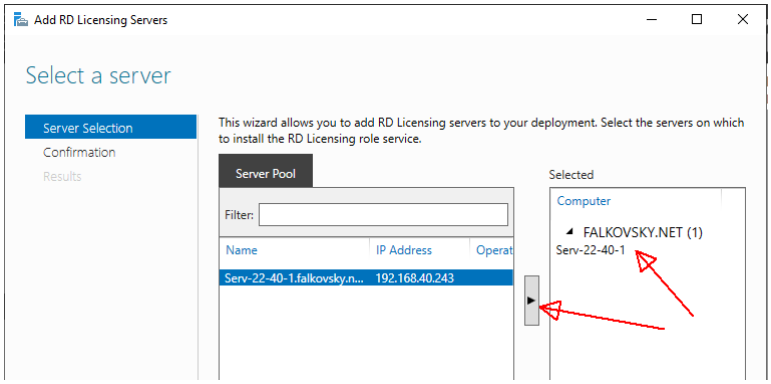


Рис. 9.12

Переконайтеся, що потрібний сервер обрано (рис. 9.13) на натисніть *Add*.

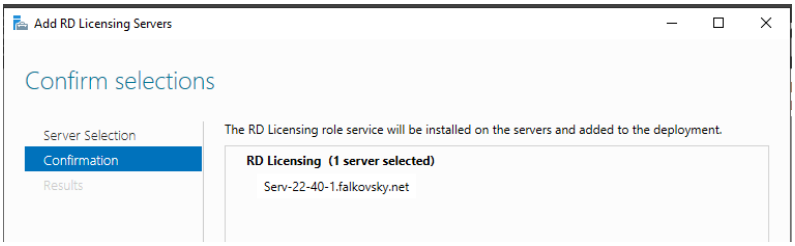


Рис. 9.13

Далі важливо переконатися, що до серверу можна під'єднуватися через служби віддаленого робочого столу. Це можна зробити через вузол *Server Manager* → *Local Server* на контролері домену Пункт меню Remote Desktop (Enabled) (рис. 9.14, рис. 9.15).

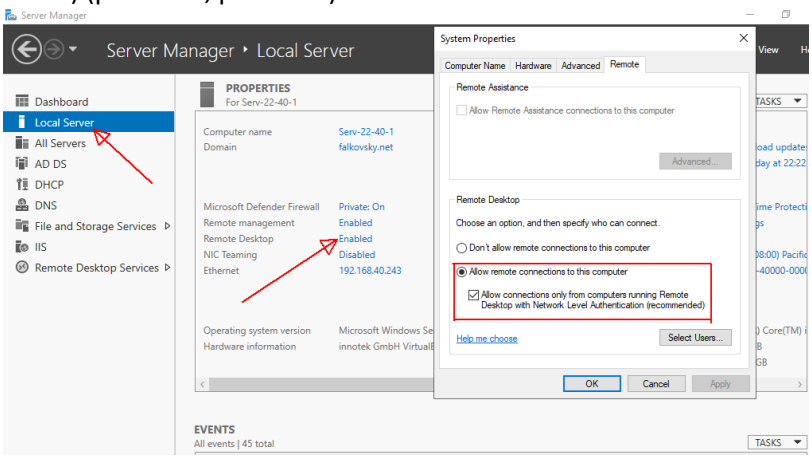


Рис. 9.14

Також потрібно додати користувачів, які використовуватимуть сервіси віддаленого робочого столу, до стандартної групи *Remote Desktop Users*. Це можна зробити для кожного користувача окремо, але у цій роботі ми додамо до цієї групи всіх членів групи Domain Users (рис. 9.15).

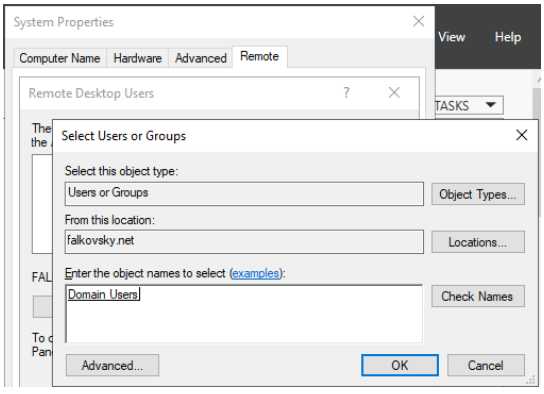


Рис. 9.15

Одержимо вміст вкладки *Members* у властивостях групи *Remote Desktop Users*, подібний до зображеного на рис. 9.16. Натисніть *Apply*.

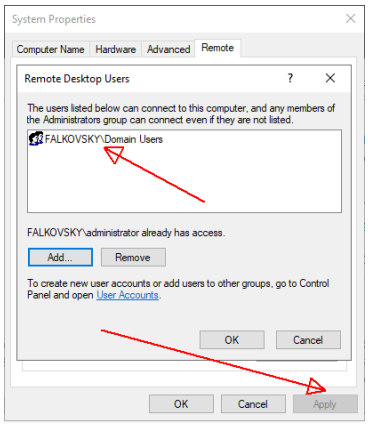


Рис. 9.16

Тепер доналаштуємо компонент RD Licensing. Для цього в області Deployment Overview оберіть *TASKS → Edit Deployment Properties* (рис. 9.17).

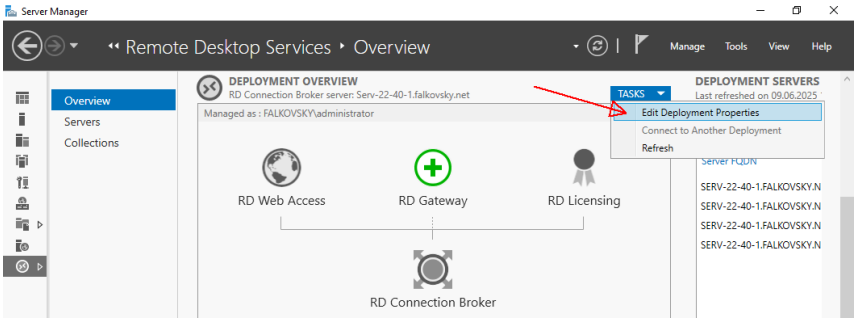


Рис. 9.17

Вкажемо, що ліцензування буде здійснюватися у режимі Per User і переконаймося, що у ролі серверу ліцензування обрано перший контролер домену (рис. 9.18).

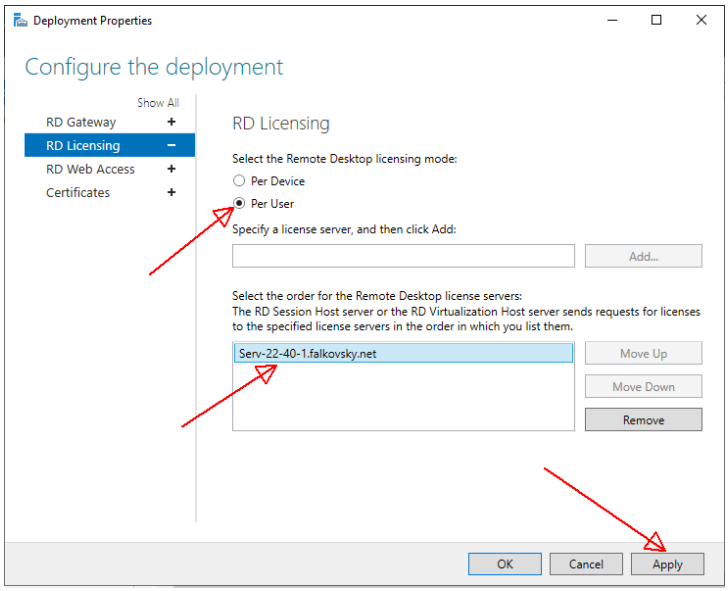


Рис. 9.18

Далі потрібно створити сертифікат, який використовуватиметься для ліцензування. У даному прикладі це буде самопідписаний сертифікат (selfsigned cetificate). Його можна створити засобами PowerShell.

Спочатку створимо сам сертифікат (виконання команди може зайняти трохи часу, це нормально):

New-SelfSignedCertificate -CertStoreLocation cert:\LocalMachine\My -DnsName "RDP" Потім задамо пароль для сертифікату (рис.9.19):

$pwd = ConvertTo-SecureString -String "Password2025" -Force –AsPlainText

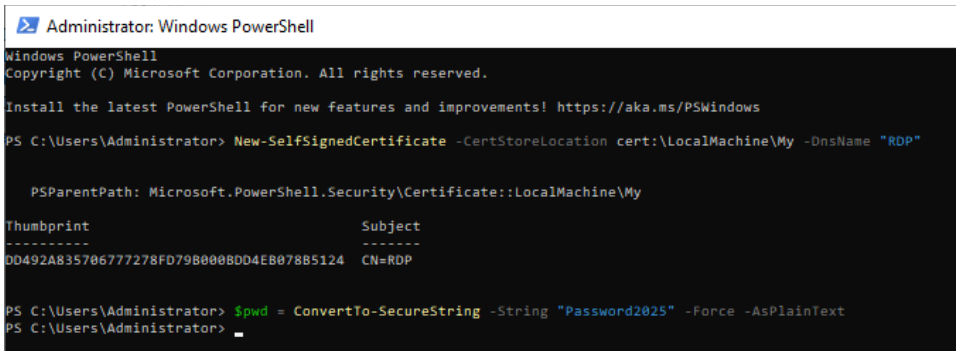


Рис. 9.19

Пароль, який ви вибрали на цьому кроці, знадобиться у наступних налаштуваннях.

Далі ми будемо завантажувати новостворений сертифікат у вигляді файлу. Для цього знадобиться консоль *mmc* та оснащення *Sertificates*.

Запустити *mmc* можна з вікна *Run* / *Виконати* (Win + R). Зробити це треба на сервері. У вікні консолі *mmc* оберіть *File* → *Add/Remove Snap-In,* як це показано на рис. 9.20.

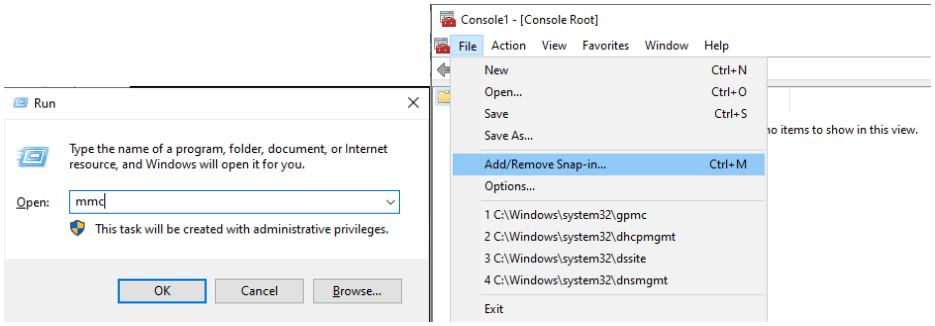


Рис. 9.20

Знайдіть потрібне оснащення та додайте його у вашу новостворену консоль (рис. 9.21).

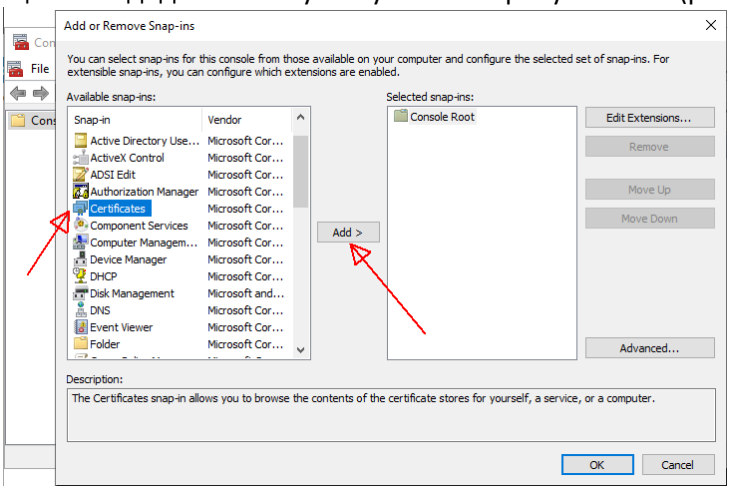


Рис. 9.21

Далі оберемо пункт *Computer Account* (рис. 9.22).

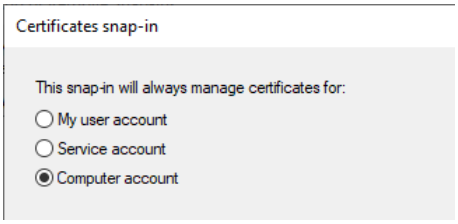


Рис. 9.22

Працювати дане оснащення буде локально, саме на цьому сервері (рис. 9.23).

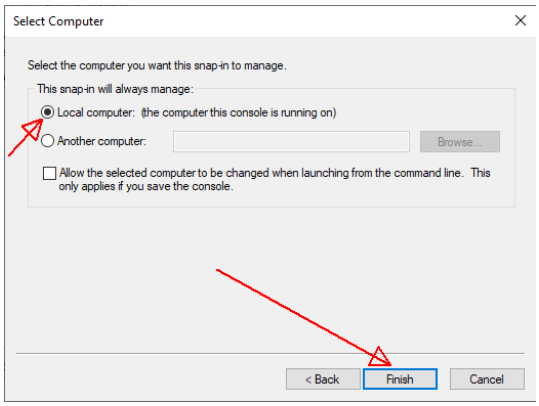


Рис. 9.23

Переконайтеся, що оснащення Certificates справді обране та натисніть OK (рис. 9.24).

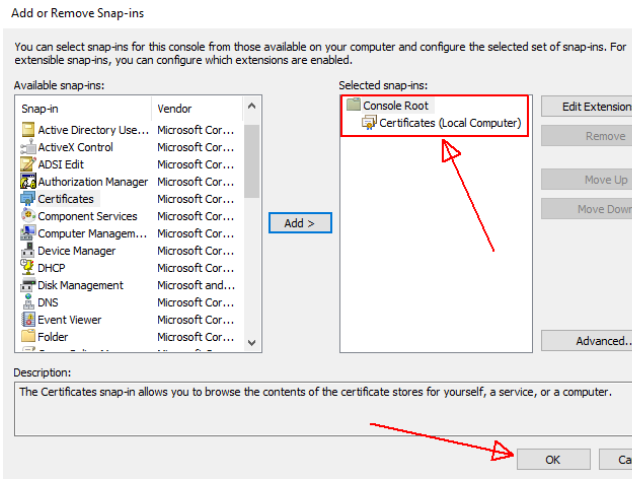


Рис. 9.24

Тепер у новоствореній консолі є перше оснащення - *Certificates* (рис. 9.25). Воно має багато вузлів, однак нас цікавить вузол *Personal* → *Cetificates*. Саме тут має відображатися сертифікат, який раніше було створено за допомогою PowerShell.

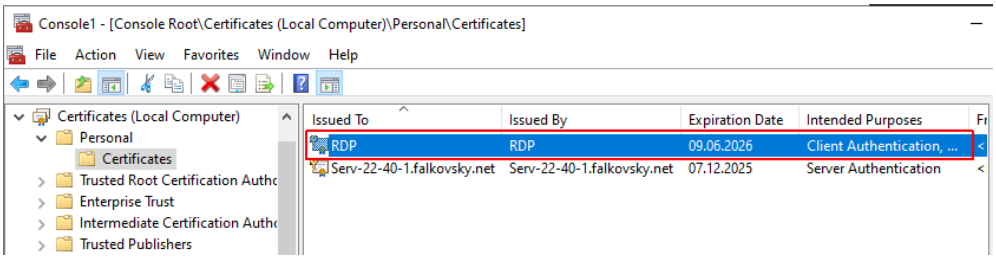


Рис. 9.25

Консоль збережемо на випадок, якщо вона знадобиться у майбутньому (рис. 9.26).

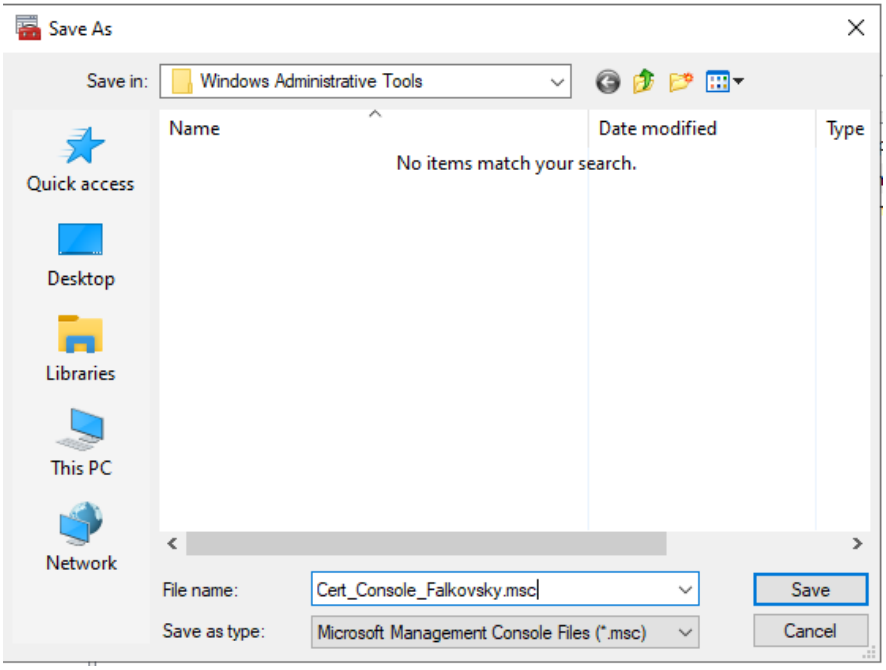


Рис. 9.26

Тепер експортуємо цей сертифікат на сервер у вигляді файлу. Для цього спершу виберемо відповідну опцію у контекстному меню сертифікату (рис. 9.27).

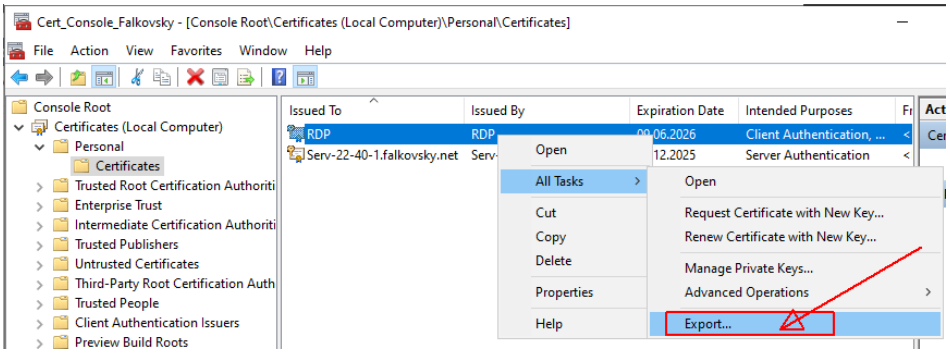


Рис. 9.27

Запуститься майстер експорту сертифікатів (рис. 9.28). Натисніть *Next*.

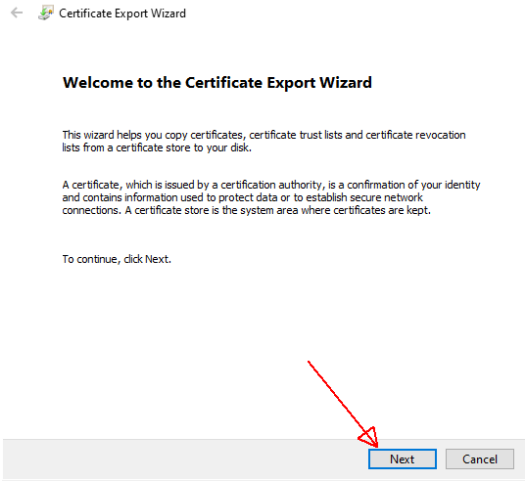


Рис. 9.28

Система попередить нас, що для наступної роботи з експортованим серитфікатом знадобиться пароль (рис. 9.29). Йдеться про пароль, який ми задали за допомогою PowerShell. Натисніть *Next*.

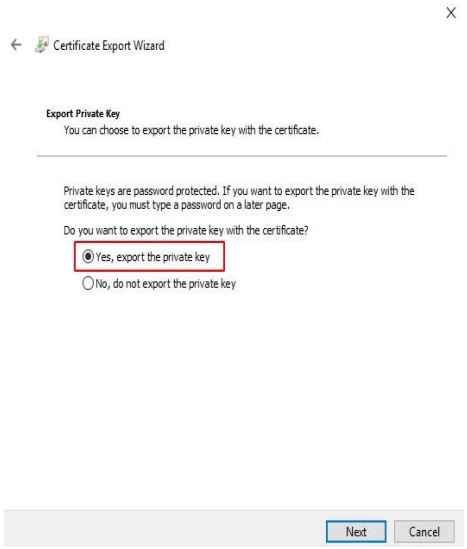


Рис. 9.29

Формат ключа лишаємо без змін (рис. 9.30).

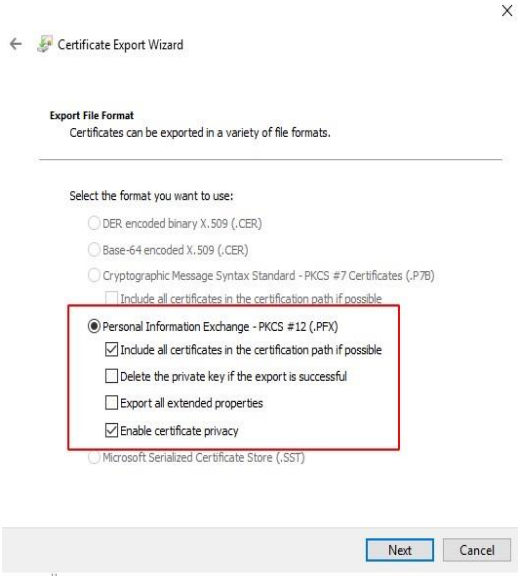


Рис. 9.30

Підтвердимо своє право на завантаження файлу сертифікату, ввівши пароль. Алгоритм шифрування оберіть на власний розсуд. На скриншоті вибрано AES256-SHA256 (рис. 9.31).

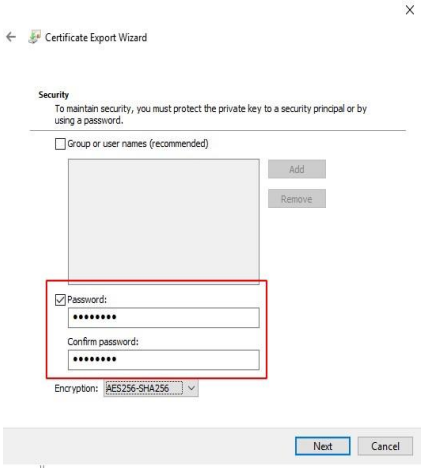


Рис. 9.31

Оберіть папку, в яку треба зберегти сертифікат, та його ім'я (рис. 9.32).

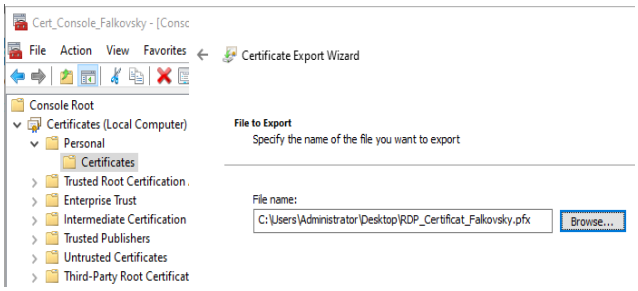


Рис. 9.32

Перевірте, що введено коректні дані (рис. 9.33) й натисніть *Export*.

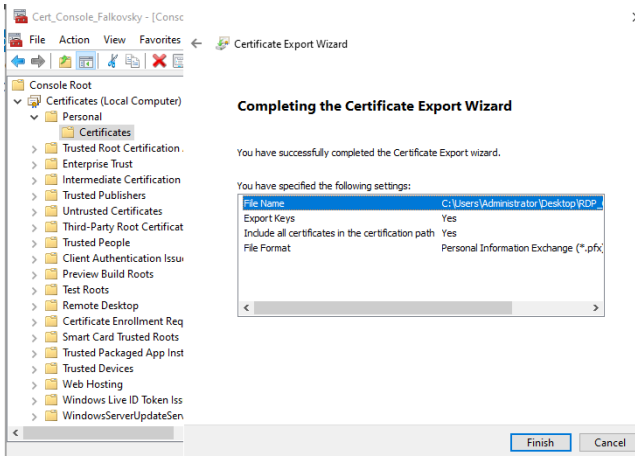


Рис. 9.33

Сертифікат експортовано (рис. 9.34).

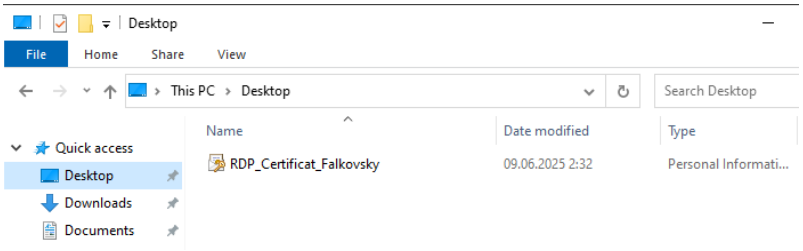


Рис. 9.34

Продовжуємо налаштовувати ліцензування у вікні *Deployment Properties*, крок *Cerificates*. Оберемо першу з трьох служб у списку й натиснемо *Select Existing Certificate* (рис.9.35).

На наступному кроці знадобиться ввести пароль, заданий раніше (рис. 9.36).

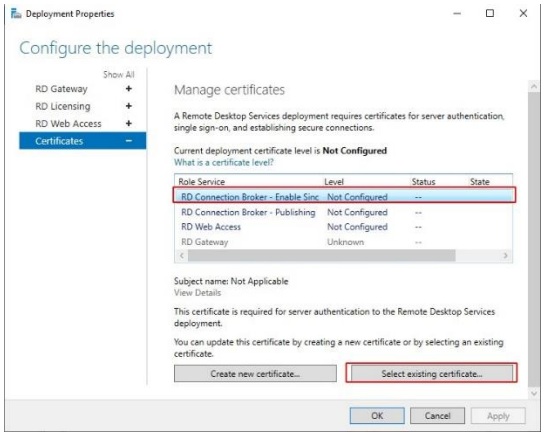


Рис. 9.35

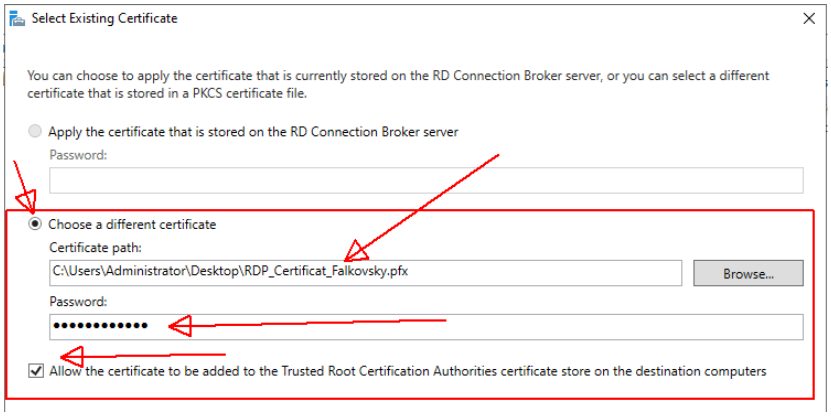


Рис. 9.36

Стан сертифікату першої служби зміниться на Ready to apply. Переконавшись, що цю службу вибрано у переліку, натисніть *Apply* (не *OK*) рис. 9.37. Застосування змін може зайняти деякий час.

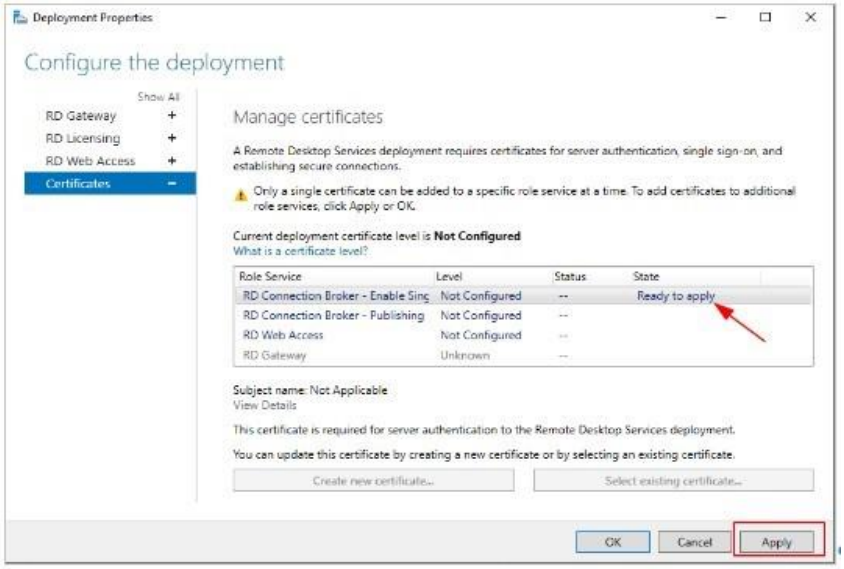


Рис. 9.37

Далі повторимо аналогічні дії з рештою двома службами у списку. У підсумку стан сертифікатів для всіх трьох служб повинен мати стан *Success* (рис. 9.39). Сертифікат для RD Gateway неактивний - це нормально, оскільки відповідну службу наразі не налаштовано. Рівень сертифікатів зараз *Untrusted*, що пов'язано з використанням самопідписаних сертифікатів. Для нашої навчальної моделі мережі це допустимий варіант.

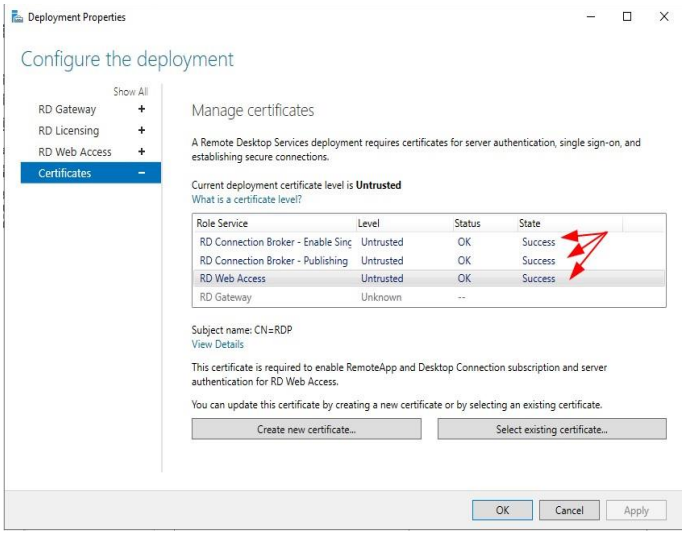


Рис. 9.39

Завдання №9.2

1. Спираючись на наведені вище рекомендації, налаштуйте раніше встановлену службу RD Licensing.

Вказівки:

- для ліцензування скористайтеся самопідписаним сертифікатом, згенерованим засобами PowerShell;
- пароль для сертифікату оберіть самостійно;
- ім'я для експортованого файлу сертифікату - *RDP_Certificate_Surname.pfx*, де - *Surname* ваше прізвище;
- консоль з оснащенням Certificates збережіть для майбутнього використання під іменем Cert_console_*Surname.msc*, де - *Surname* ваше прізвище.

Звіт має містити скриншоти одержаних відомостей та опис основних дій.

Додавання DNS-запису для доступу до служб віддаленого робочого столу

Звернення до служб віддаленого робочого столу буде зручнішим, якщо це можна буде робити за доменним ім'ям. Для цього на DNS-сервері потрібно створити відповідний запис.

У ролі DNS-серверу і серверу, що надає доступ до служб віддаленого робочого столу, у нашому випадку відповідає перший контролер домену. Тому налаштування здійснюємо на ньому.

Запустіть інструмент *DNS Manager* (*Tools* → *DNS*). У зоні прямого перегляду *surname*.net додайте DNS-запис типу A з ім'ям RDP. Як IP-адресу задайте адресу першого контролера домену (рис. 9.40). Створення відповідного PTR-запису у зоні зворотного перегляду - на ваш розсуд.

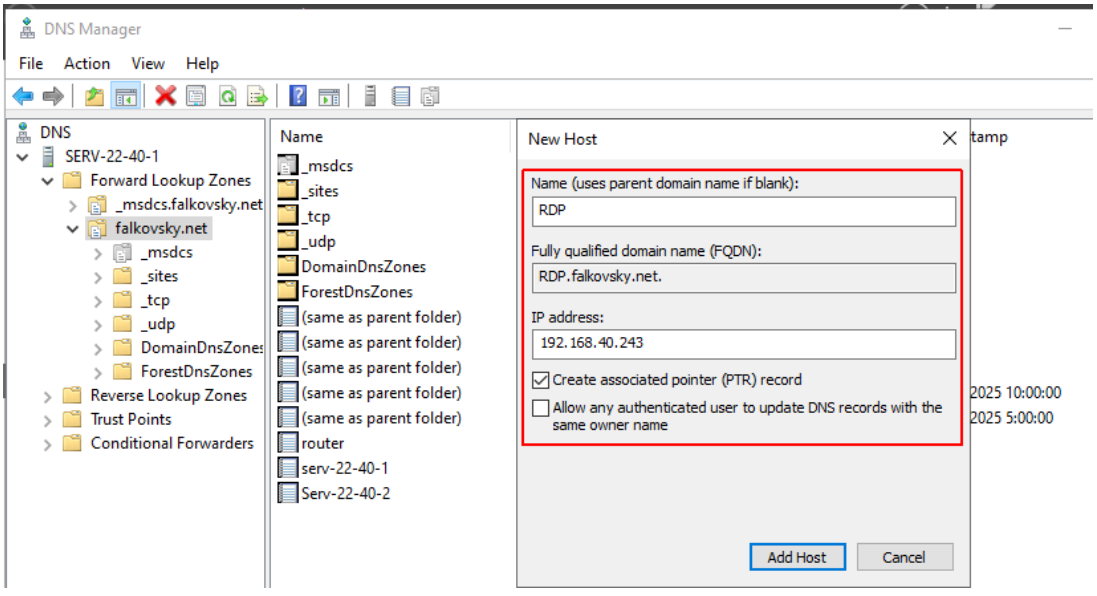


Рис. 9.40

Завдання №9.3

- Використовуючи подані вище інструкції, додайте на DNS-сервері запис типу A, що вказуватиме на сервер зі службами віддаленого робочого столу.

  Підказка. Якщо не вдається створити запис (кнопка *Add Host* неактивна), спробуйте перезавантажити DNS-область.

- Переконайтеся, що DNS-запис успішно створено.

Звіт має містити скриншоти одержаних відомостей та опис основних дій.

Доступ користувачів до програм через служби віддаленого робочого столу

Основні налаштування зроблено. Тепер можна надавати користувачам доступ до встановлених на сервері програм.

Спершу перевіримо, чи доступ у принципі надано. Увійдемо у систему на будь-якій робочій станції та введемо в адресному рядку веббраузера адресу https://rdp.*surname*.net.

Оскільки було використано самопідписаний сертифікат, ви можете побачити повідомлення про незахищеність вебсайту (рис. 9.41). Це нормально у даній ситуації - натисніть *Перейти на веб-сторінку* чи інше подібне посилання у вашому браузері.

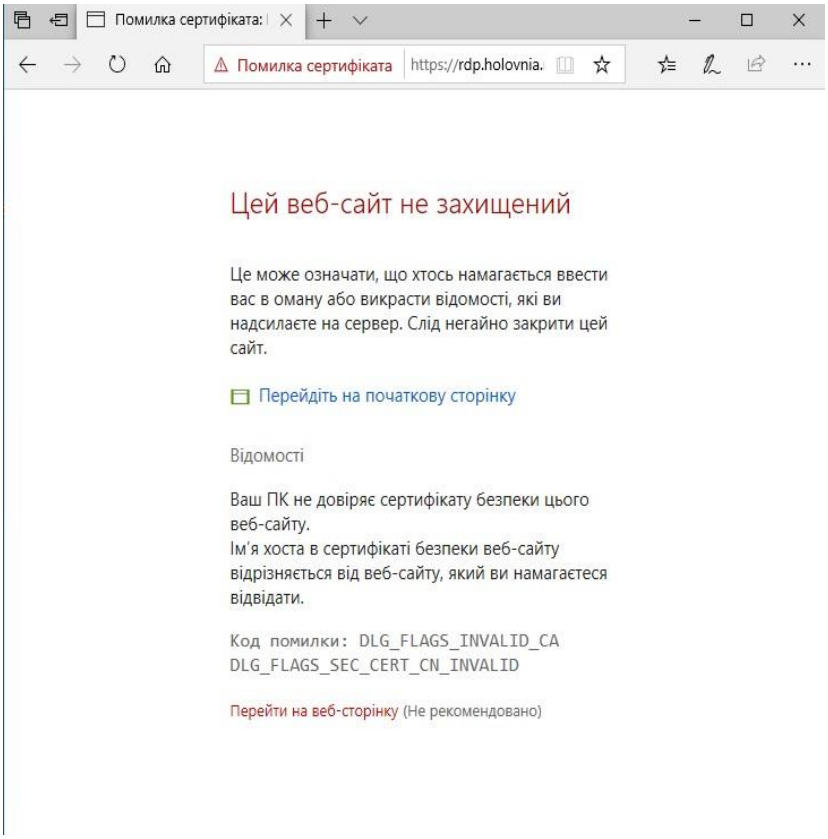


Рис. 9.41

Якщо з'єднання успішне, ви побачите стартову сторінку IIS Windows Server (рис. 9.42).

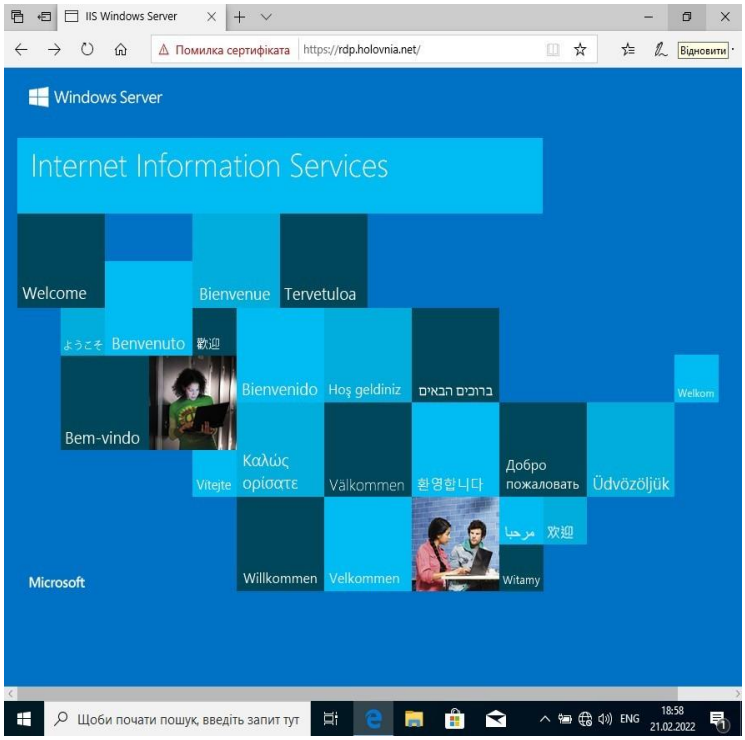
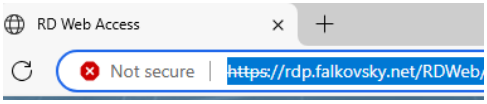


Рис. 9.42

Нас цікавлять служби, налаштовані у межах цієї роботи, тому до адреси в адресному рядку браузера додамо */rdweb*. Наприклад:



Автентифікуємося через один з облікових записів домену (рис. 9.43).

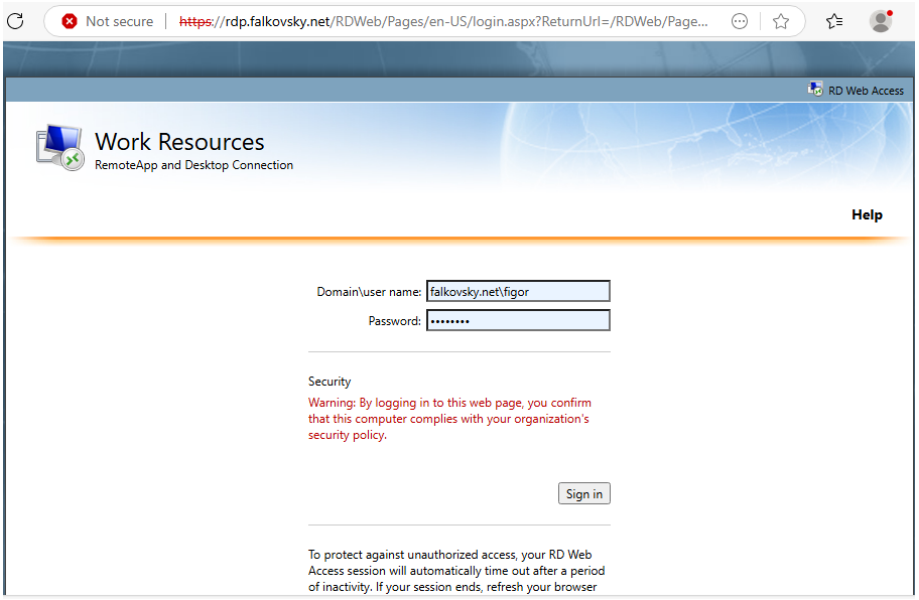


Рис. 9.43

Після успішного входу побачимо область RemoteApp and Desktops - поки що порожню (рис. 9.44).

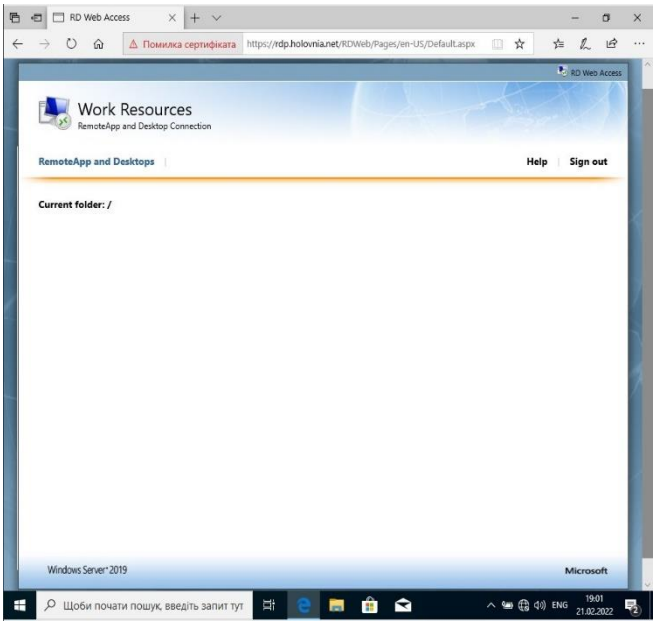


Рис. 9.44

Створимо першу колекцію для надання доступу до програм користувачам домену. Для цього у вікні *Server Manager* перейдіть до групи *Remote Desktop Services* та оберіть *Collections*. Далі оберіть *TASKS* → *Create Session Collection.*(рис. 9.45)

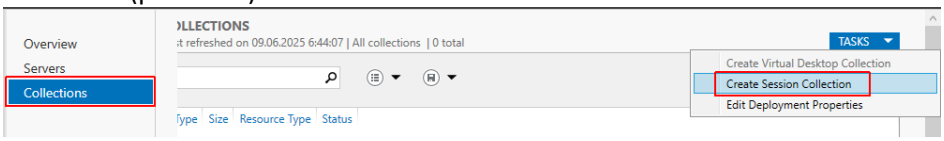


Рис. 9.45

Відкриється вікно майстра створення колекцій (рис. 9.46).

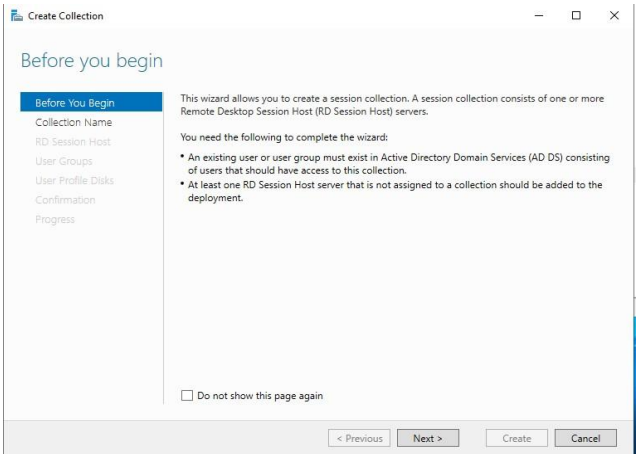


Рис. 9.46

Дамо колекції ім’я (рис. 9.47).

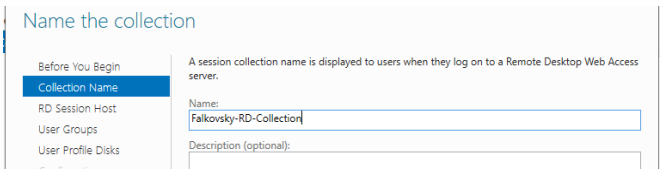


Рис. 9.47

Оберемо сервер, який є водночас першим контролером домену (рис. 9.48).

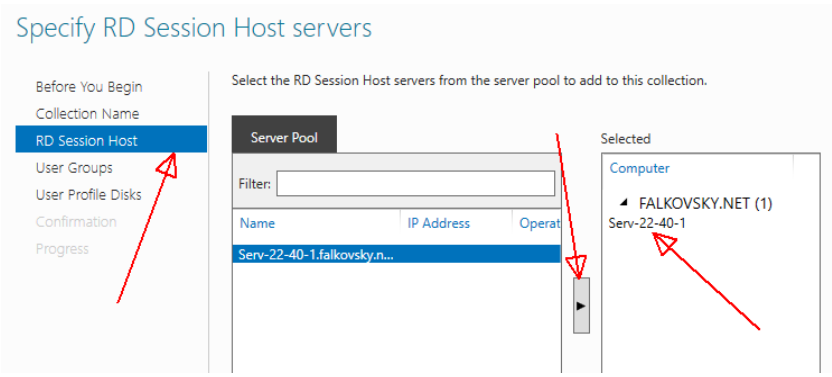


Рис. 9.48

Доступ до колекції за замовчуванням матимуть всі користувачі домену. Нас це влаштовує (рис. 9.49).

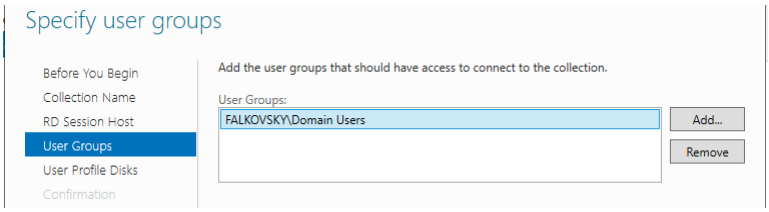


Рис. 9.49

Налаштовувати простір на диску для віддалених користувачів наразі не будемо. Перевірте налаштування (рис. 9.50) і натисніть *Create*. Створення колекції може зайняти деякий час.

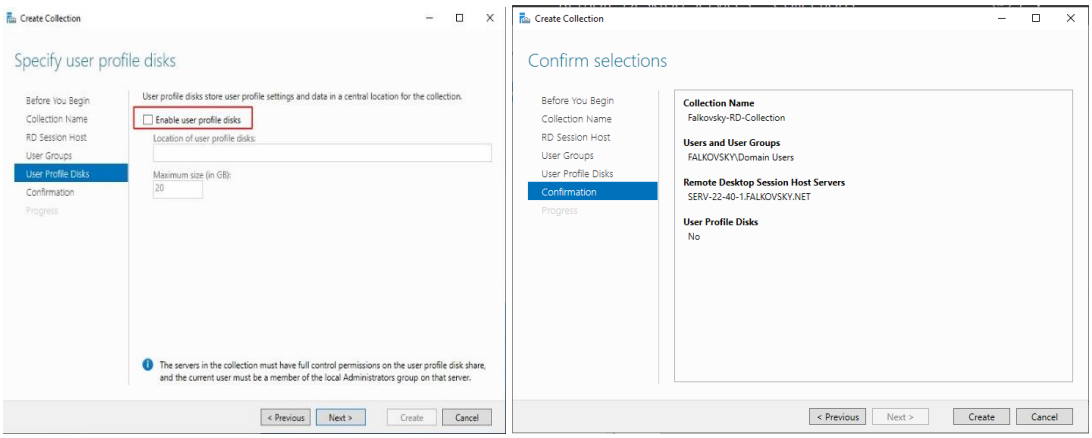


Рис. 9.50

Тепер додамо до новоствореної колекції програми (рис. 9.51).

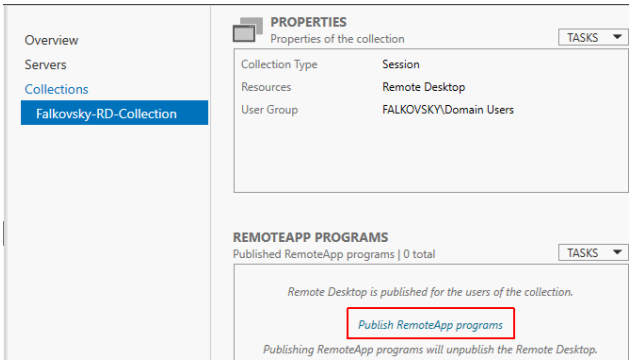


Рис. 9.51

Оберемо кілька програм (рис. 9.52) та натиснемо *Publish*.

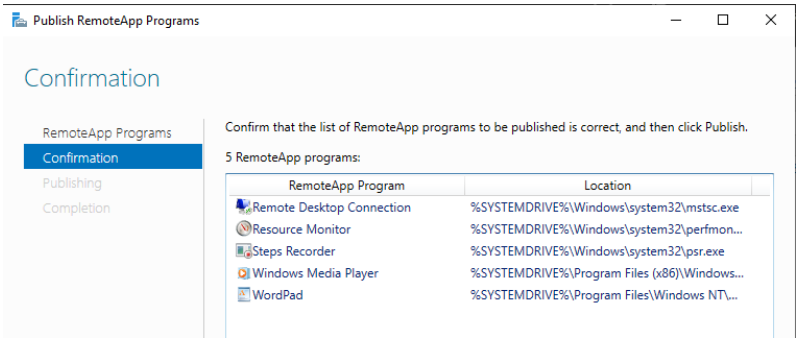


Рис. 9.52

Тепер з робочої станції на оновленій сторінці браузера видно опубліковані програми (рис. 9.53).

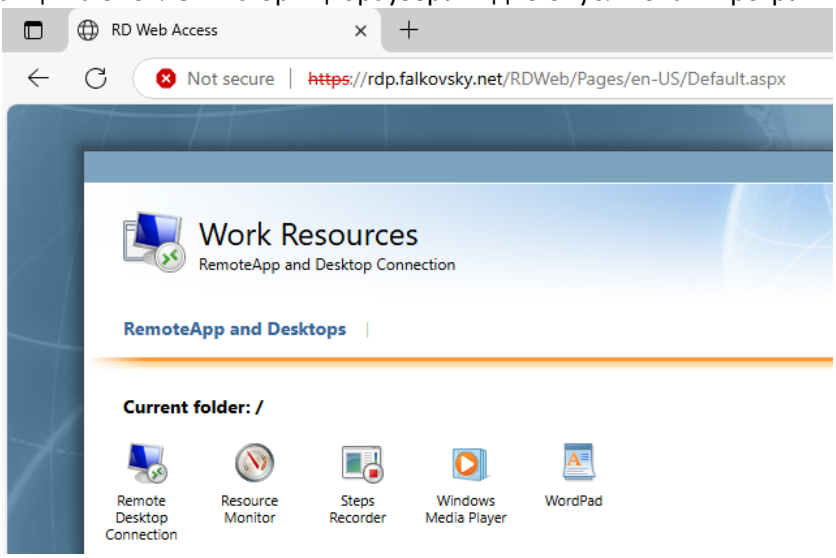


Рис. 9.53

Спробуємо запустити одну з них (рис. 9.54).

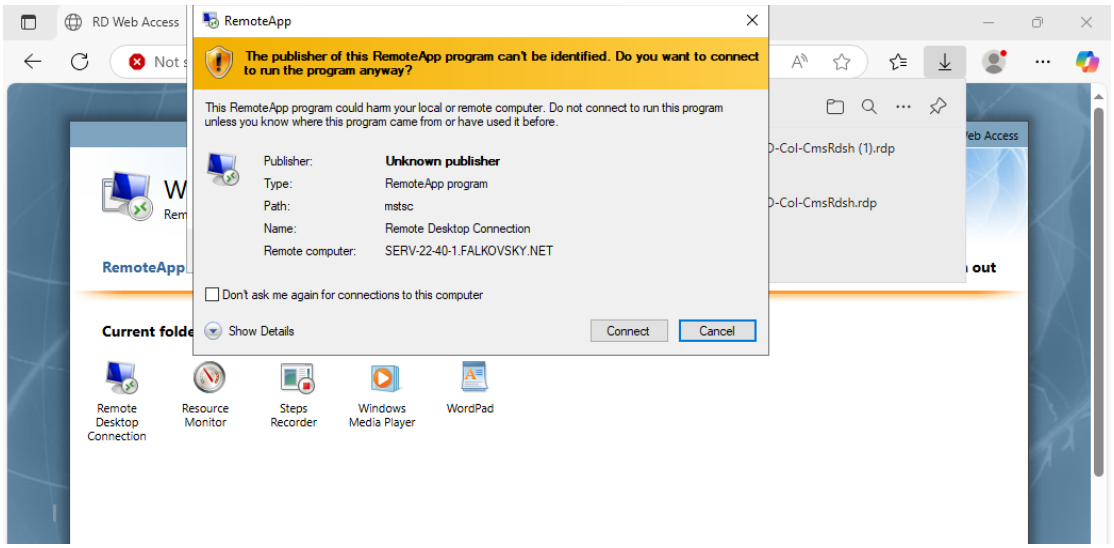


Рис. 9.54

Першого разу треба ввести пароль користувача домену. Після чого програма запуститься. У *Диспетчері завдань* видно, що насправді програма працює віддалено (рис. 9.55).

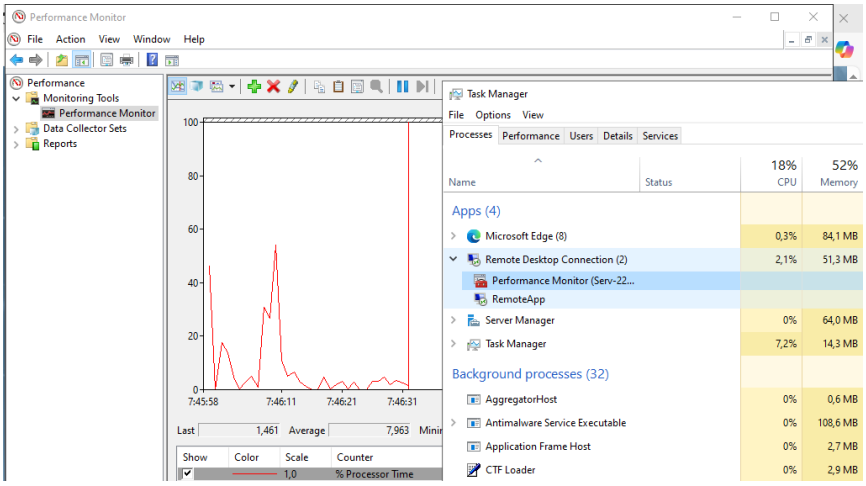


Рис. 9.55

Завдання №9.4

1. Спираючись на подані вище інструкції, надайте користувачам домену доступ до трьох програм, встановлених на сервері. Колекцію назвіть *Surname-RDCollection*, де *Surname* - ваше прізвище.
2. Переконайтеся, що доступ до усіх опублікованих програм цієї колекції наявний.
3. На прикладі однієї з опублікованих програм за допомогою *Диспетчера завдань* перевірте, де фізично виконується ця програма.
4. Лишаючи ввімкненою тестову робочу станцію, вимкніть віртуальну машину з Windows Server (можна шляхом збереження стану машини). Перевірте, чи доступні тепер:

- довільна програма з тих, котрі ви опублікували у колекції
- оновлення сторінки *https:/rdp.surname.net/RDWeb* **Поясніть одержаний результат.**

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 9.1-9.4.

Рекомендовані джерела

1. M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020
2. Orin Thomas. Windows Server 2016 Inside Out. Pearson Education, 2017.

Робота №10. Налаштування спільного принтера на базі Windows Server 2022 та Active Directory

Мета: навчитися здійснювати встановлення та базове конфігурування спільного принтера на базі домену Active Directory та Windows Server 2022.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-9.

Теоретичні відомості та завдання до лабораторної роботи

Додавання нового принтера у Windows Server 2022

Додавання нового принтера у Windows Server загалом подібне до аналогічної процедури у настільних версіях Windows. Продемонструємо це на прикладі принтера HP Neverstop Laser 1001nw.

На *Панелі керування* (*Control Panel*) оберіть пункт *Devices and Printers* і натисніть *Add a printer* (рис. 10.1).

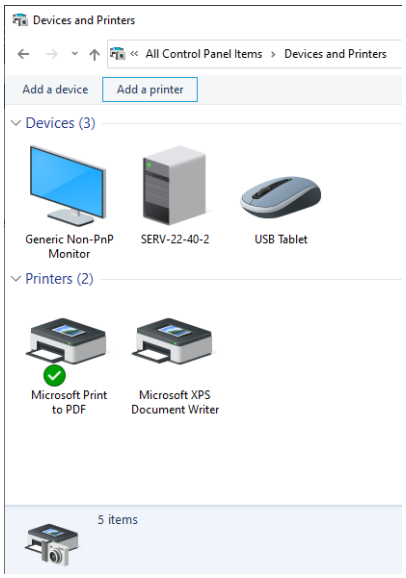


Рис. 10.1

Наша модель мережі навчальна, і реально підключений принтер відсутній, тож автоматично його знайдено не буде. Тож у наступному вікні одразу обираємо *The printer that I want isn't listed* (рис. 10.2).

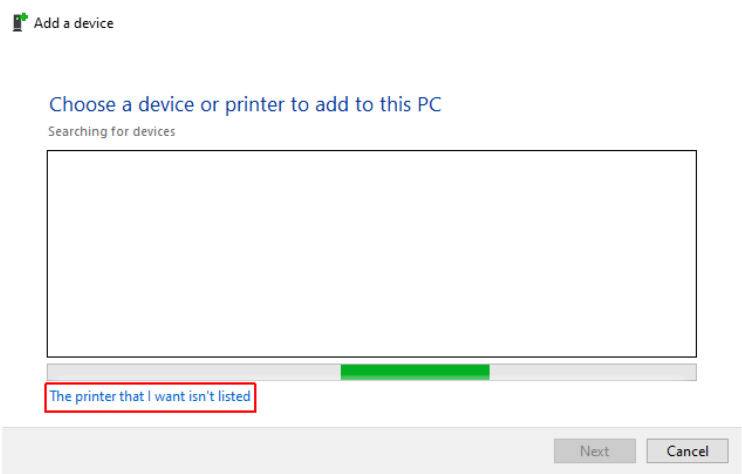


Рис. 10.2

Обираємо локальний принтер та порт, пропонований за замовчуванням (рис. 10.3).

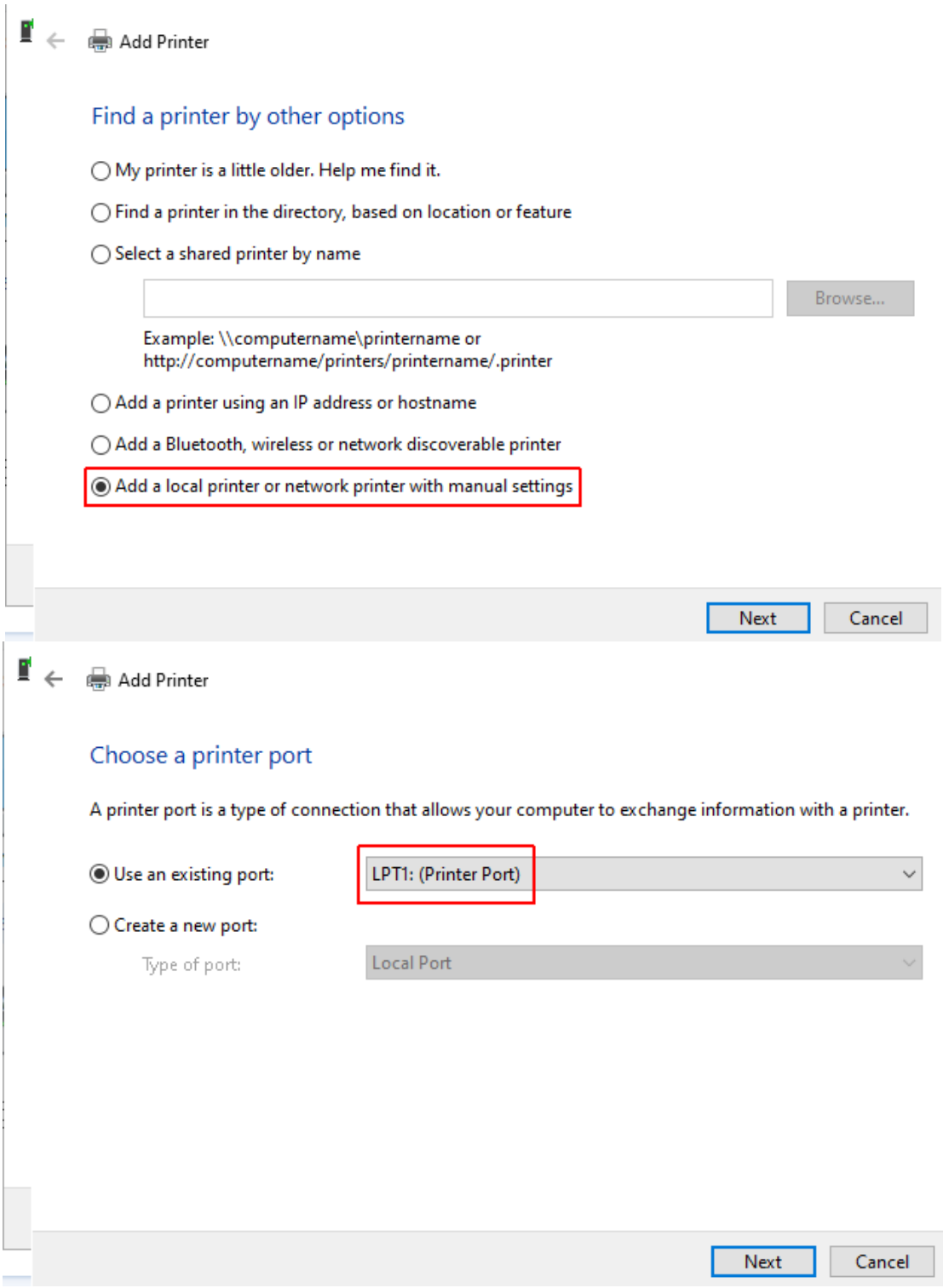


Рис. 10.3

На наступному кроці знадобиться драйвер. Завантажимо його з сайту виробника (*Epson*), відшукавши там необхідну модель (*Epson XP330*). Не забудьте вказати, що драйвер потрібний для Windows Server. Якщо драйвер для Windows Server 2022 відсутній, оберіть драйвер для найближчого випуску.
Завантажуємо архів, що саморозпаковується. За допомогою спільного каталогу робимо його доступним на віртуальній машині з Windows Server (перший контролер домену). У нашому випадку завантажений файл виглядає, як показано на рис. 10.4.

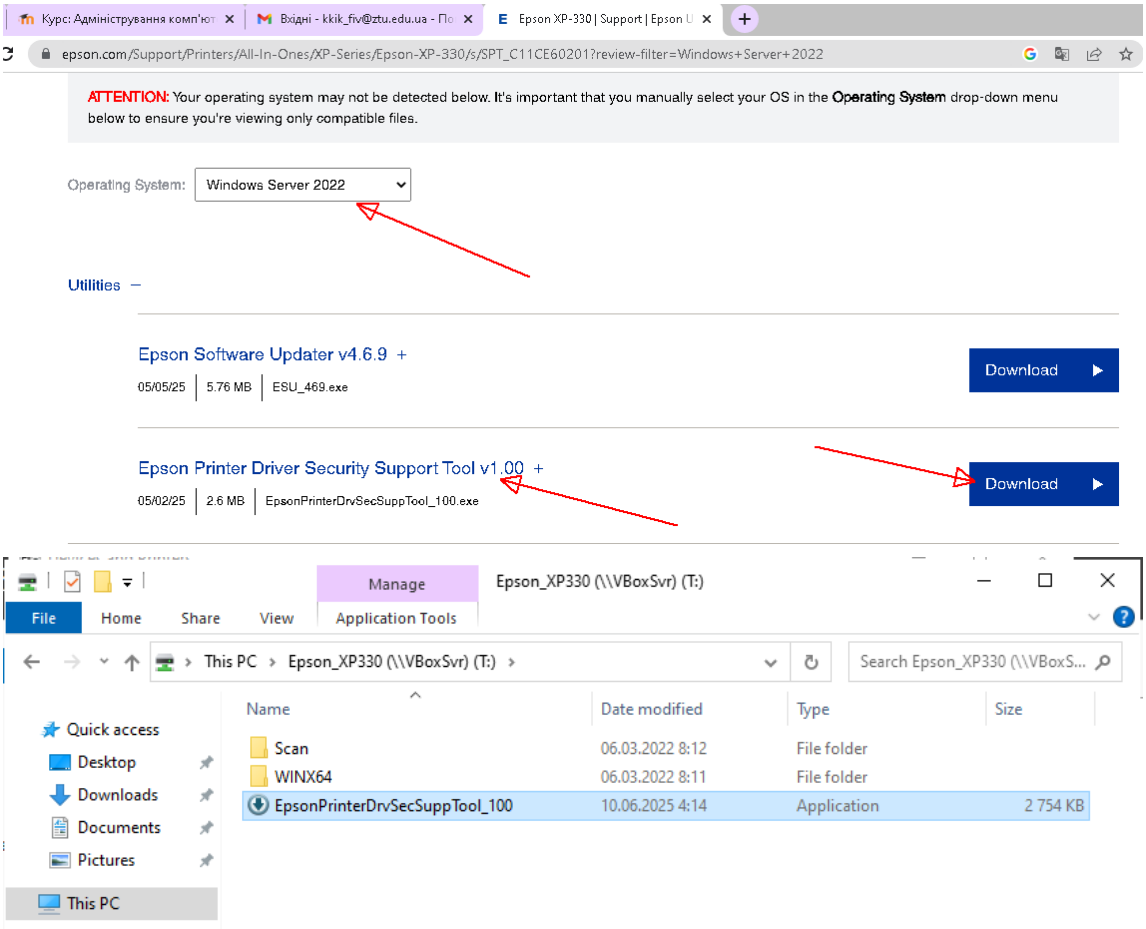


Рис. 10.4

Двічі клацніть по архіву. Архів саморозпакується (рис.10.5) до поточного каталогу Потрібну підпапку визначимо за датою останньої модифікації. На рис. 10.6 це верхня папка з системною назвою, створена нещодавно.)

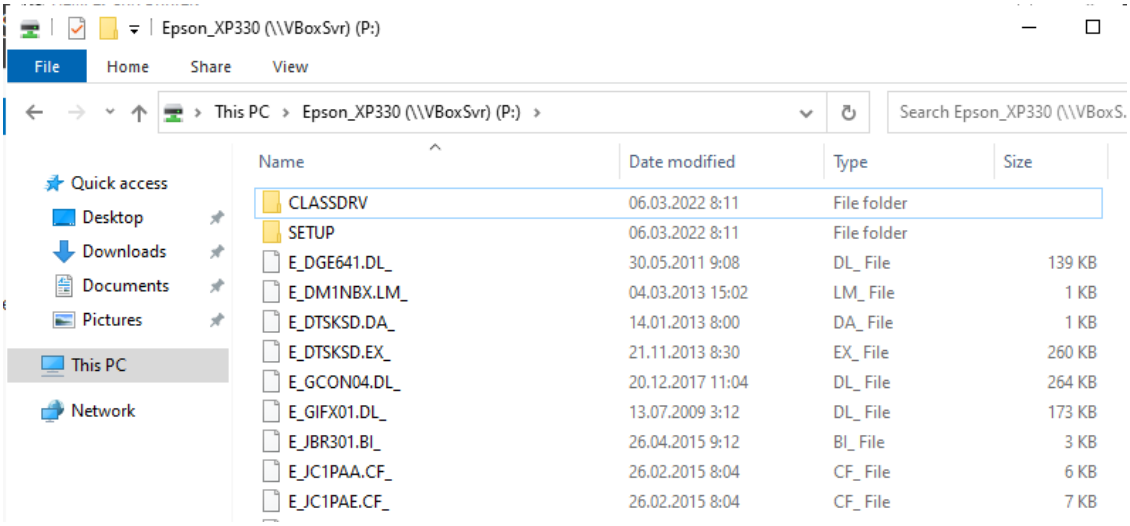


Рис. 10.5

Переконайтеся, що у папці є потрібні файли (передусім, *INF*, *dll*).

Повертаємося до вікна *Add Printer*. На кроці встановлення драйвера оберіть *Have Disk...* (рис. 10.6).

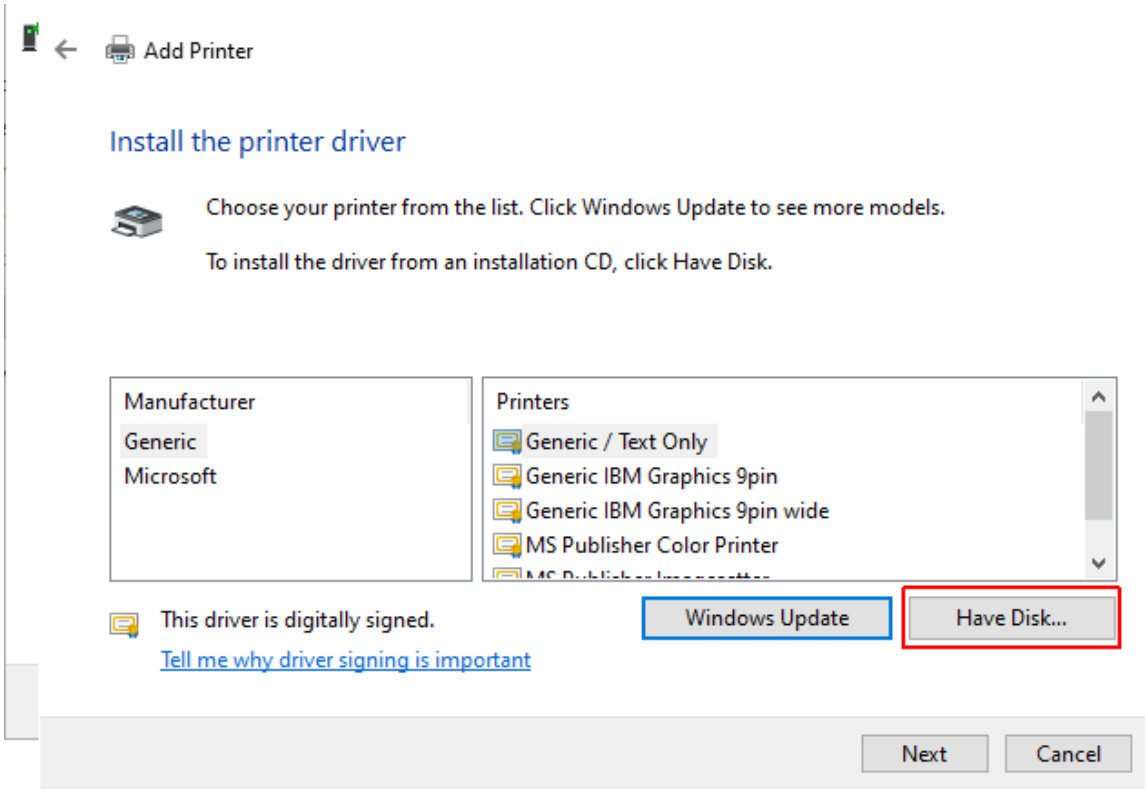


Рис. 10.6

У вікні, оберіть шлях до підпапки з файлами драйверів принтера (рис. 10.7).

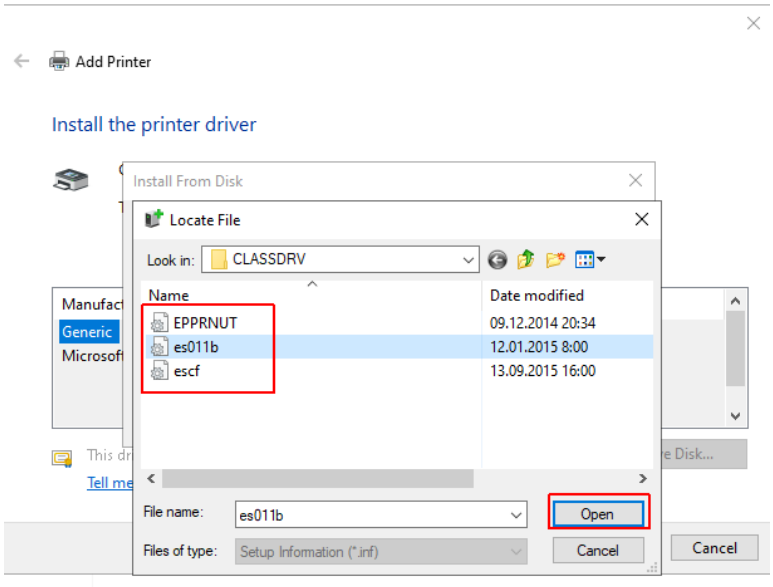


Рис. 10.7

Система знаходить драйвер і підтверджує, що він має цифровий підпис. Натисніть Next, щоб продовжити встановлення.

Далі буде запропоновано вказати ім’я принтера — за потреби змініть його або залиште запропоноване за замовчуванням (наприклад, Epson XP-330 Series), після чого натисніть Next.

Дайте принтеру ім’я, які містить ваше прізвище (рис. 10.8). Натисніть *Next*.

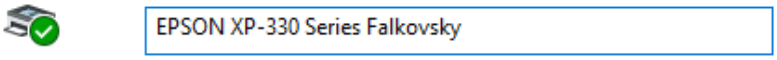


Рис. 10.8

На наступному етапі система може запропонувати спільний доступ до принтера (Sharing). Вкажемо, що принтер буде спільним (рис. 10.9). На цьому кроці можна також за потреби вказати IP-адресу принтера.

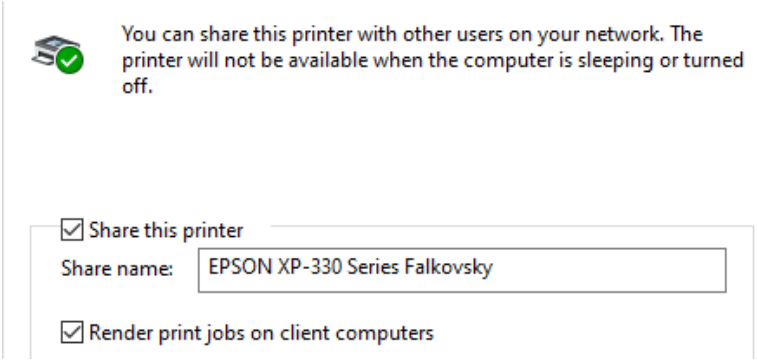


Рис. 10.9

У завершальному вікні з'явиться повідомлення про успішне встановлення драйвера. Натисніть Finish. Після цього вікно встановлення буде закрито, і встановлений принтер з'явиться в списку Devices and Printers з відповідною назвою (рис.10.10).

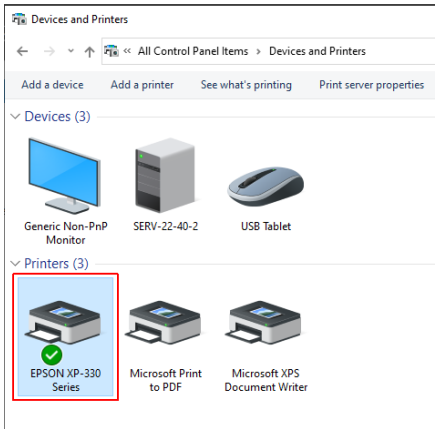


Рис. 10.10

Завдання №10.1

- Запустіть віртуальну машину з Windows Server (перший контолер домену).
- Користуючись поданими вище інструкціями, додайте на цій машині принтер. Виробника та модель принтера вказано у таблиці 10.1. **До імені принтера у вашій системі додайте номер вашої групи та ваше прізвище.**
- Переконайтеся, що додайний вами принтер відображається у групі *Devices and Printers* на *Панелі керування.*

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Таблиця 10.1

Виробники та моделі принтерів для завдання №10.1 за варіантами

Варіант	Виробник та модель принтера
1	Brother MFC-J6945DW INKvestment Tank Color Inkjet All-In-One Printer
2	Lexmark MC3426adw
3	Brother HL-L3290CDW
4	Lexmark MS431dw
5	Lexmark MB3442adw
6	Canon Color imageClass LBP664Cdw
7	Brother MFC-L9570CDW
8	Brother HL-L6400DW
9	Brother HL-L9310CDW
10	HP Color LaserJet Enterprise MFP M480f
11	Brother MFC-J4335DW
12	HP Envy Pro 6452 All-in-One
13	Epson Expression Premium XP-7100 Small-in-One Printer
14	Canon Pixma TS6420
15	Pantum P3012DW
16	HP Neverstop Laser MFP 1202w
17	Fujifilm Instax Link Wide
18	Epson EcoTank Photo ET-8550
19	Canon Pixma G7020 MegaTank All-in-One
20	HP OfficeJet Pro 9015e All-in-One Printer
21	Epson EcoTank Pro ET-5850
22	Epson EcoTank Pro ET-16650
23	Epson WorkForce Pro WF-7840 Wireless Wide-Format All-in-One Printer
24	Epson SureColor P900 17-Inch Photo Printer
25	Canon Color imageClass MF746Cdw
26	Epson WorkForce Pro WF-7310
27	Canon Pixma Pro-200
28	Epson WorkForce Pro WF-C8690 A3 Color MFP With PCL/PostScript
29	Canon Pixma TS9520 Wireless Inkjet All-In-One Printer
30	Brother MFC-J6945DW INKvestment Tank Color Inkjet All-In-One Printer

Встановлення ролі Print and Document Services в Active Directory

Для зручного керування спільним принтером в Active Directory встановимо роль *Print and Document Services*. У вікні *Server Manager* оберіть *Manage → Add Roles and Features* (рис. 10.11).

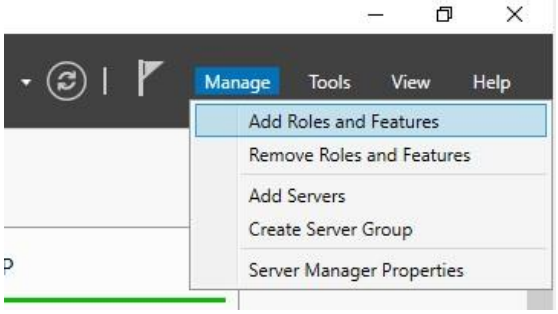


Рис. 10.11

Далі виберіть *Role-based or feature-based installation* (рис. 10.12).

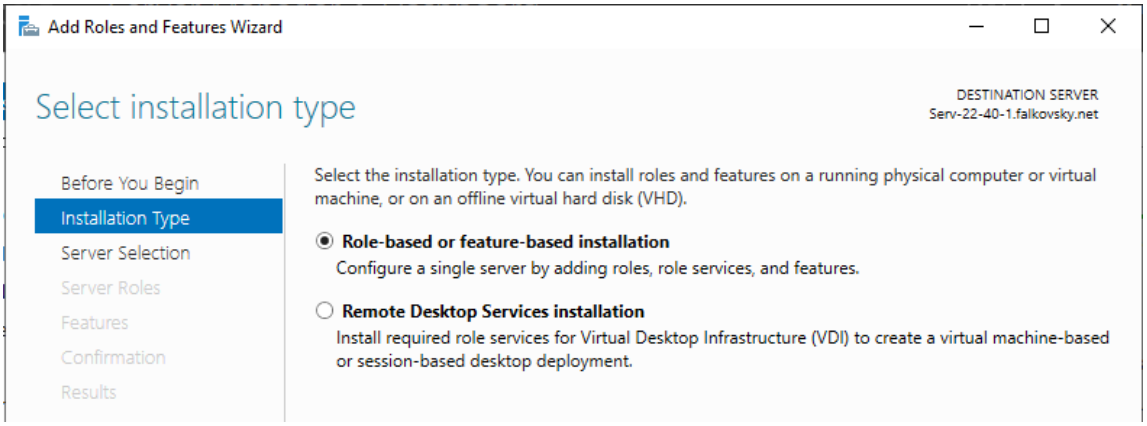


Рис. 10.12

Сервер вказуємо поточний (рис. 10.13).

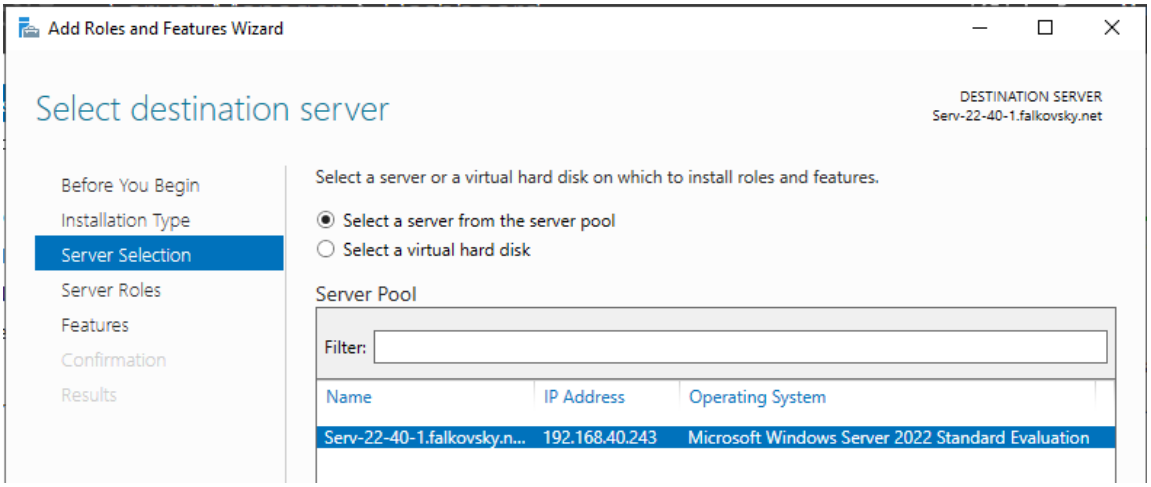


Рис. 10.13

На наступному кроці оберіть роль *Print and Document Services* (рис. 10.14).

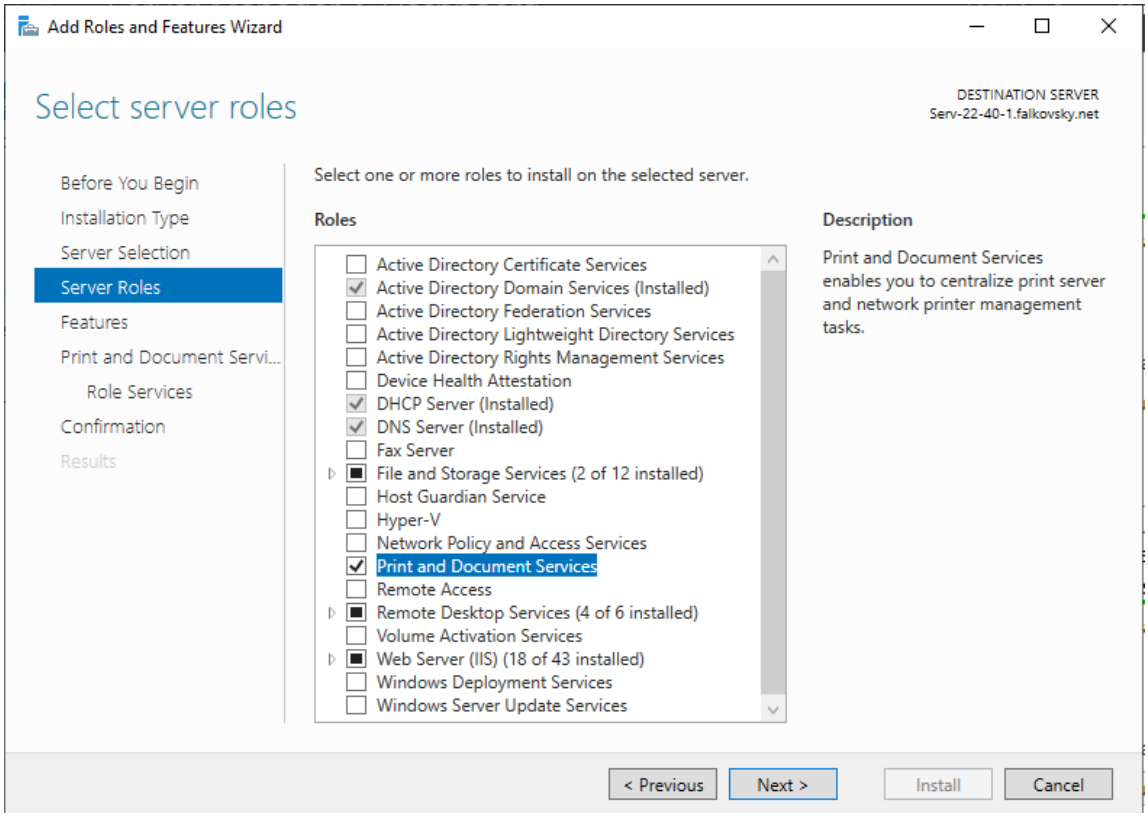


Рис. 10.14

Далі просто натисніть *Next* (рис. 10.15).

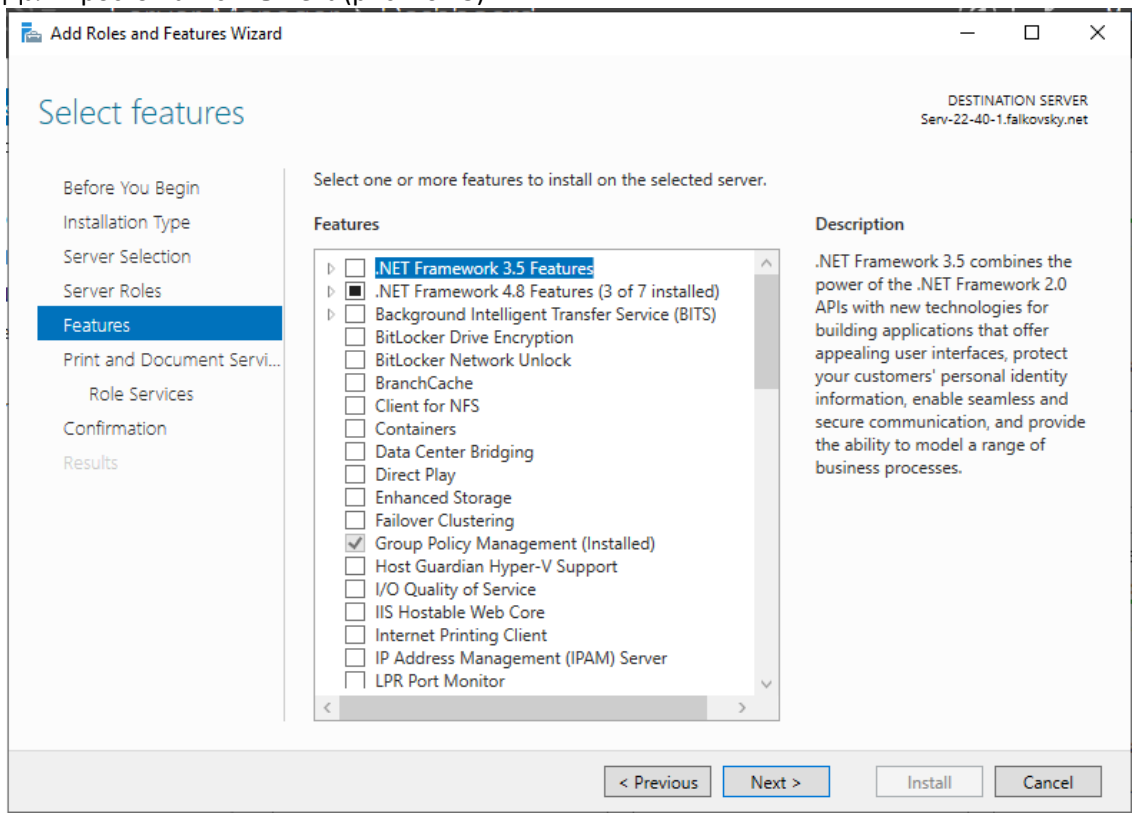


Рис. 10.15

На наступному кроці ознайомтеся з рекомендаціями щодо добору драйверів для принтерів та потенційних обмежень (рис. 10.16), після чого натисніть *Next*.

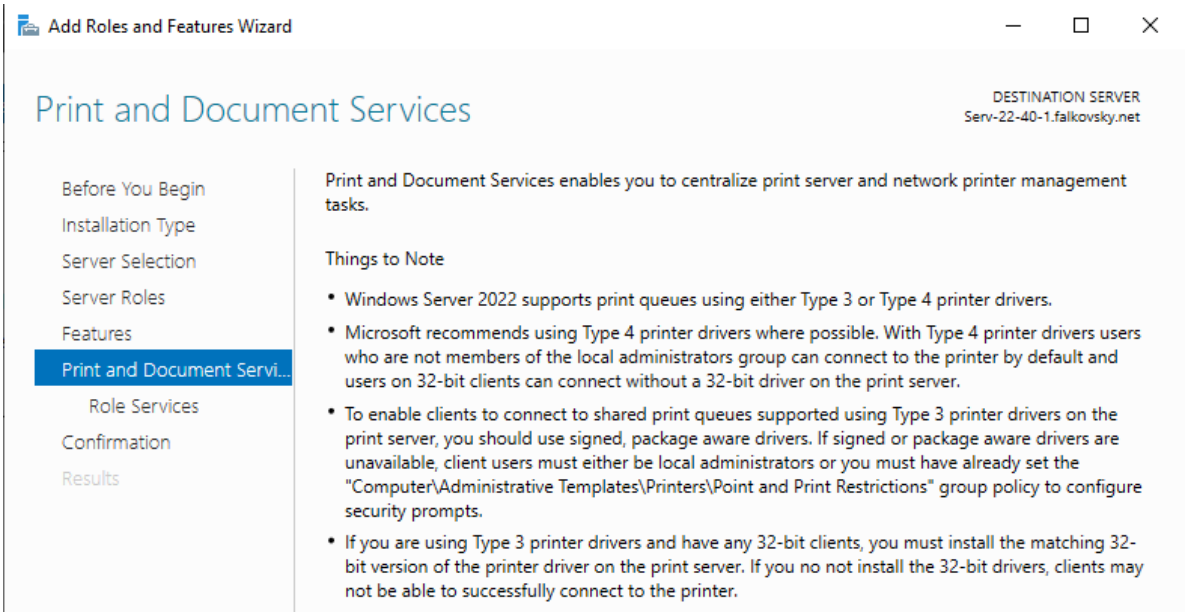


Рис. 10.16

Далі обмежимося вже обраною службою серверу друку й інших служб не обираємо (рис. 10.17).

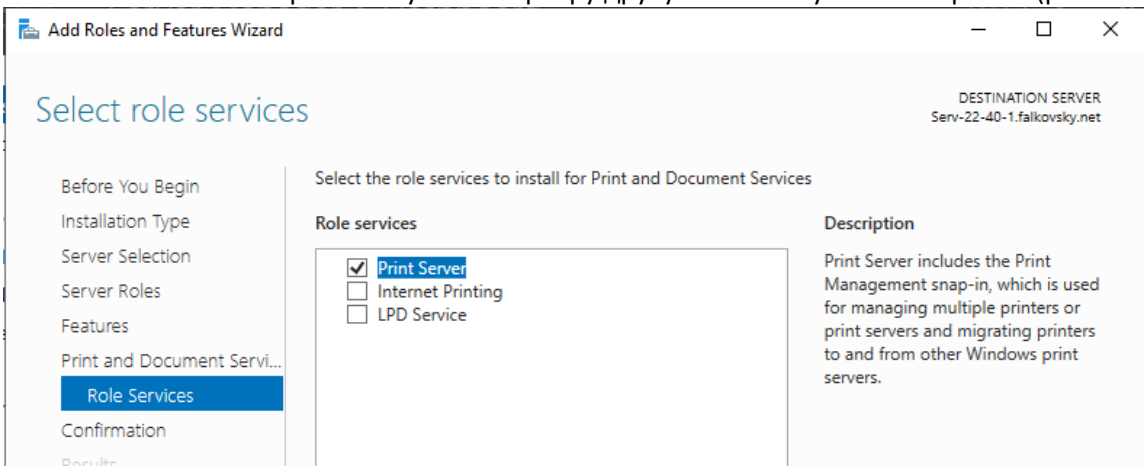


Рис. 10.17

Все готове до встановлення. Обираємо *Install* (рис. 10.18).

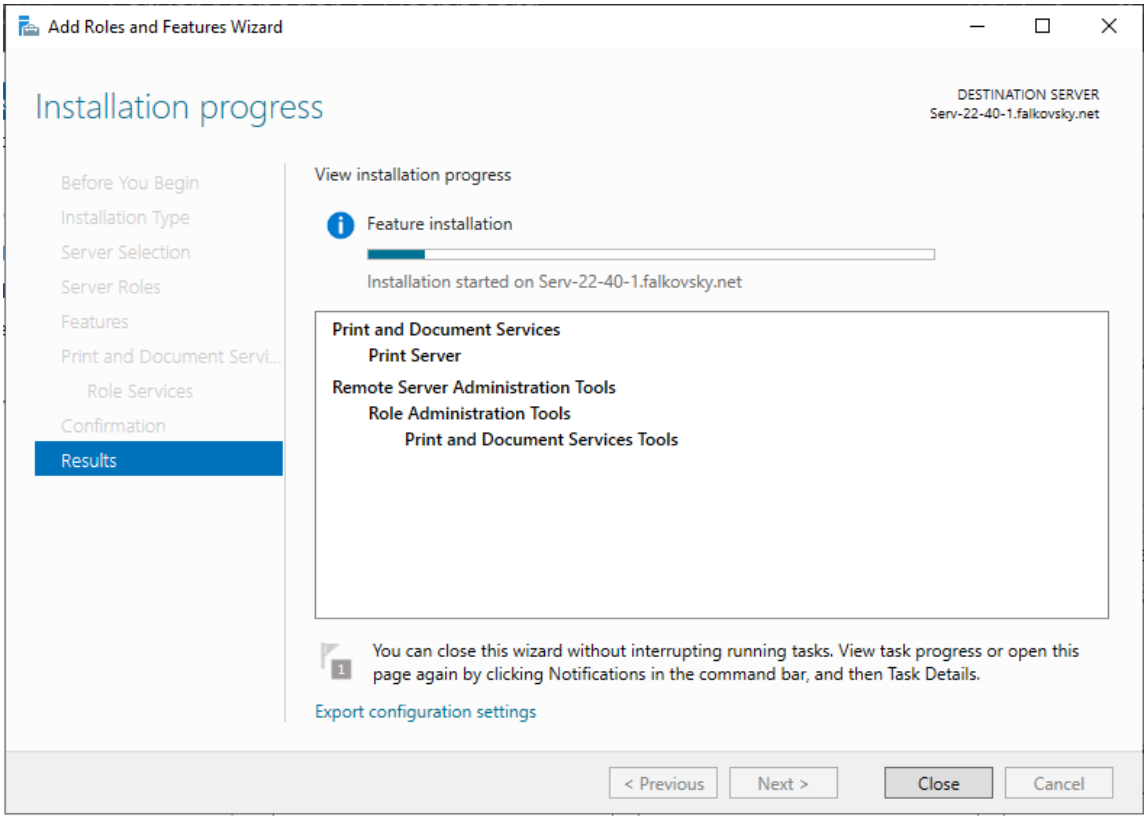


Рис. 10.18

Встановлення займе деякий час. Коли воно завершиться, натисніть *Close.* (рис. 10.19).

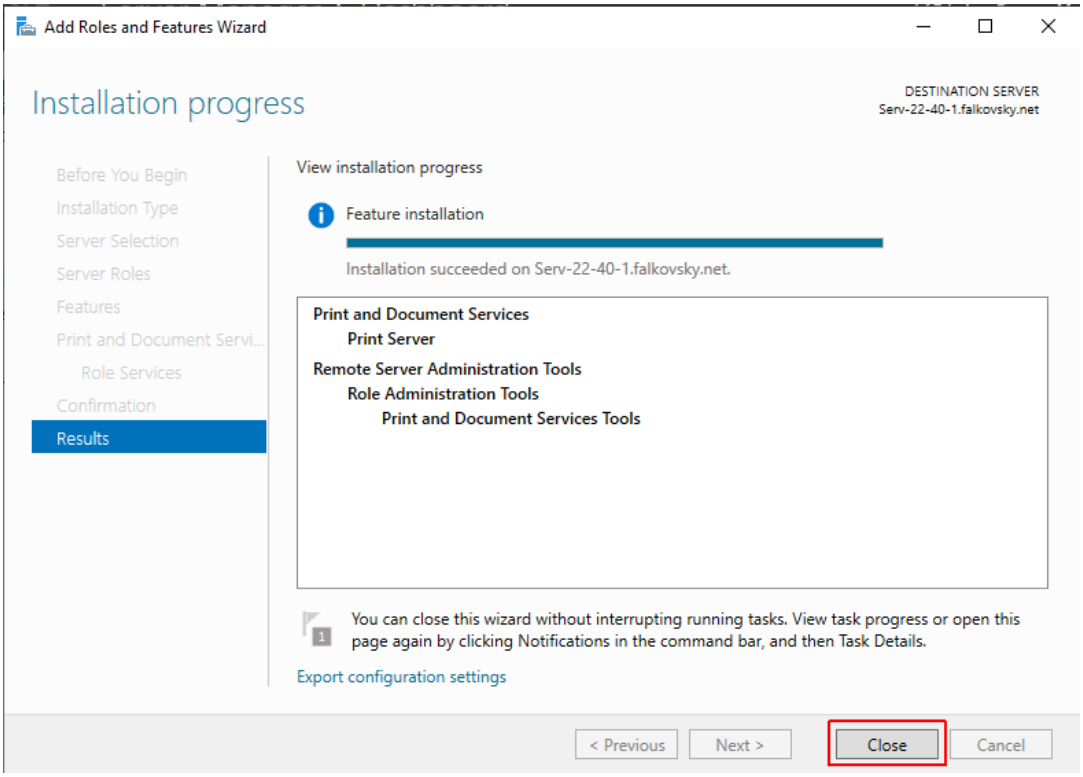


Рис. 10.19

У вікні *Server Manager* з'являться нові служби (рис. 10.20).

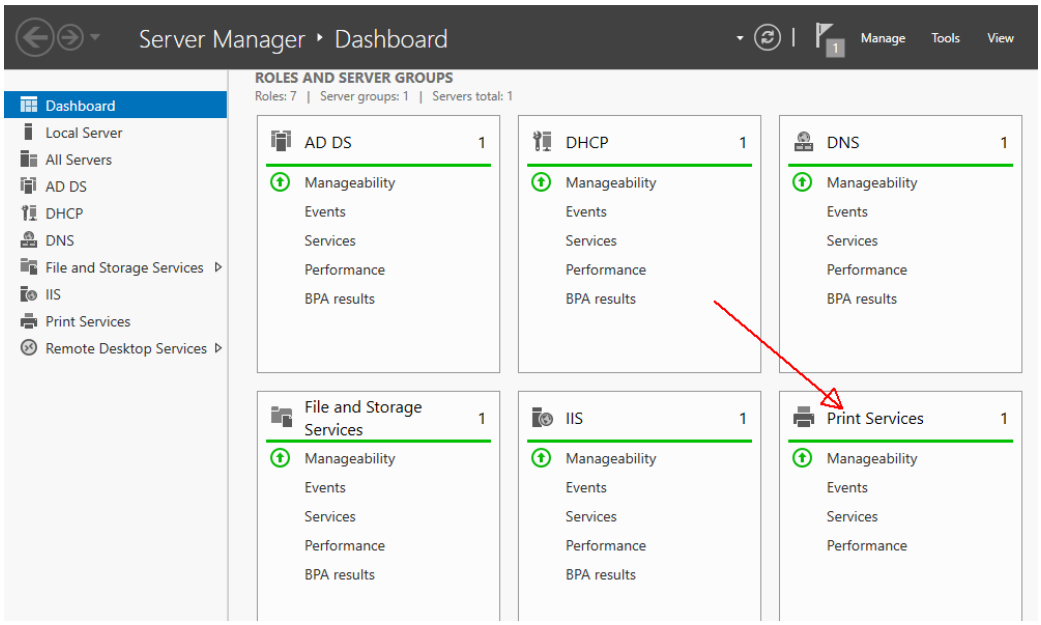


Рис. 10.20

Завдання №10.2.

1. Спираючись на подані вище вказівки, встановіть на першому контролері домену роль *Print and Document Services.*

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Розгортання принтера у домені

Для розгортання принтера у домені *surname.net* нам знадобиться оснащення *Print Management* (рис. 10.21).

Засіб *Print Management* дає змогу переглядати відомості про сервери друку, які працюють у домені, порти, драйвери, форми друку та принтери, а також налаштовувати їх.

Принтер, який ми нещодавно додали, доступний через вузол *Printers* наразі єдиного доступного серверу друку. Розпочнемо його розгортання у домені.

У контекстному меню принтера *HP Neverstop Laser KI4 Holovnia* оберемо *Deploy with Group Policy*. Це дасть змогу налаштувати, хто та з яких машин може мати доступ до принтера, через групові політики (рис. 10.22).

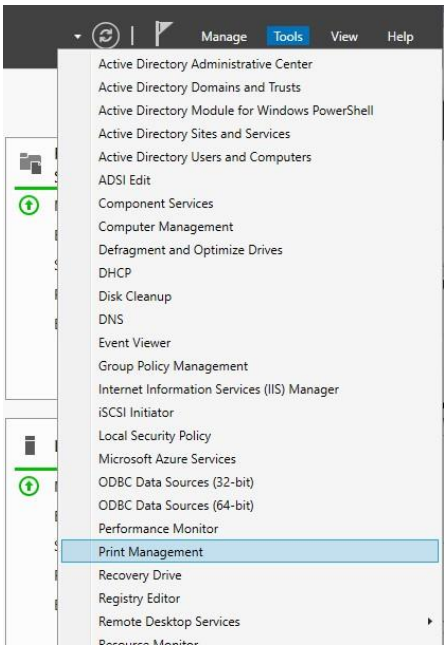


Рис. 10.21

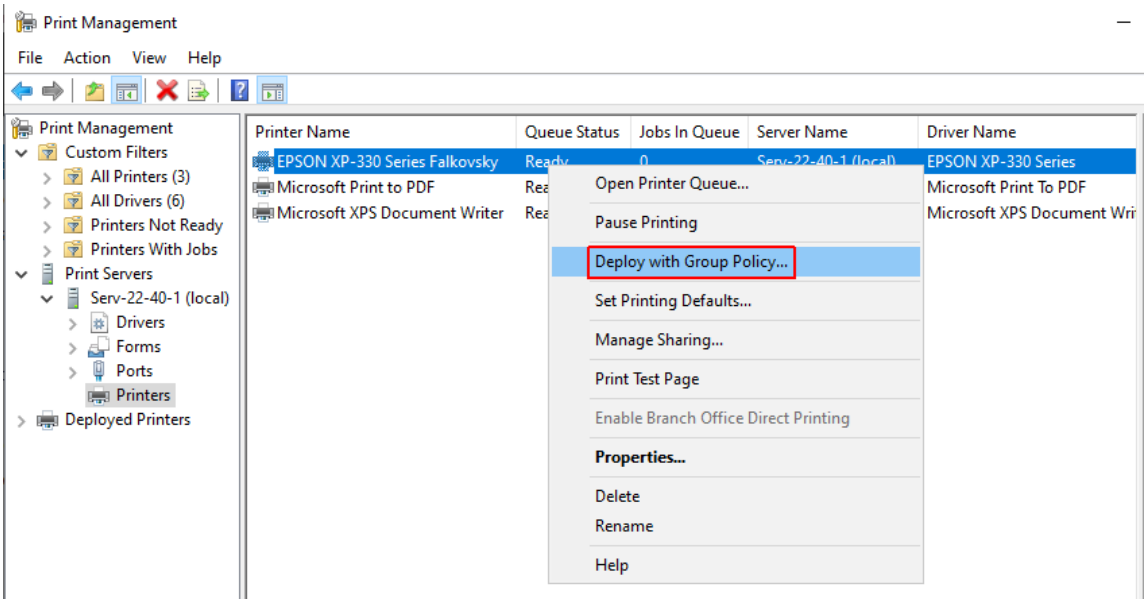


Рис. 10.22

Для вибору GPO, які матимуть доступ до принтера, натисніть *Browse*... (рис. 10.23).

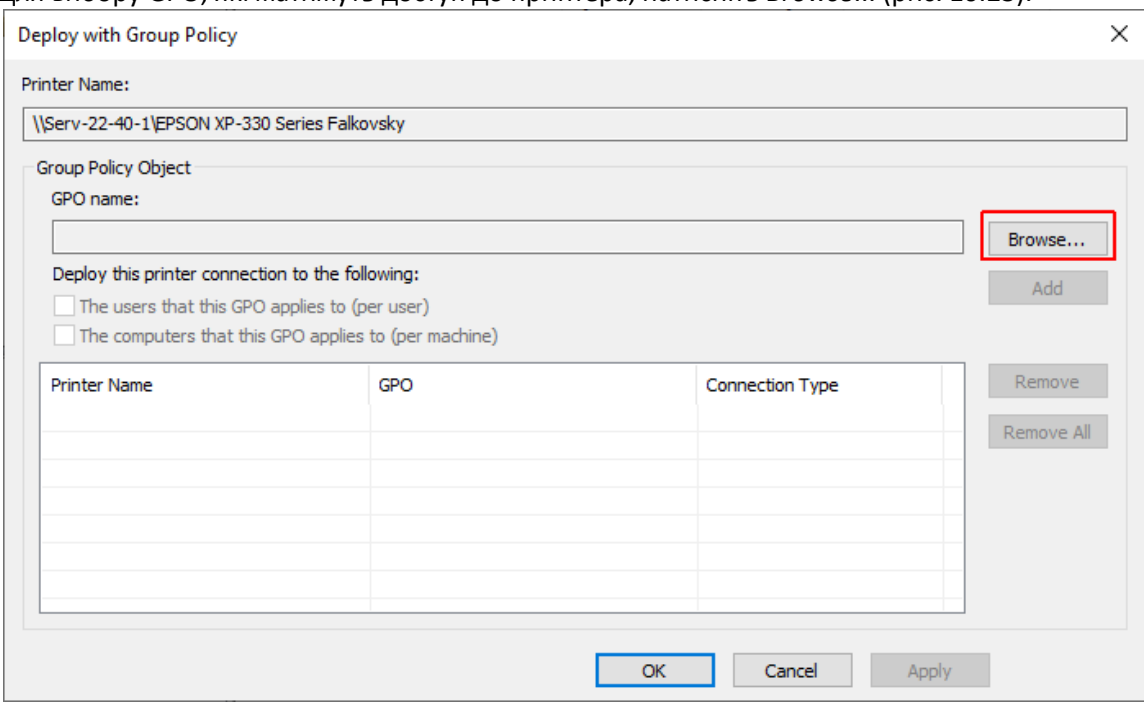


Рис. 10.23

У межах цієї роботи оберемо об’єкт групової політики *Default Domain Policy* (рис. 10.24).

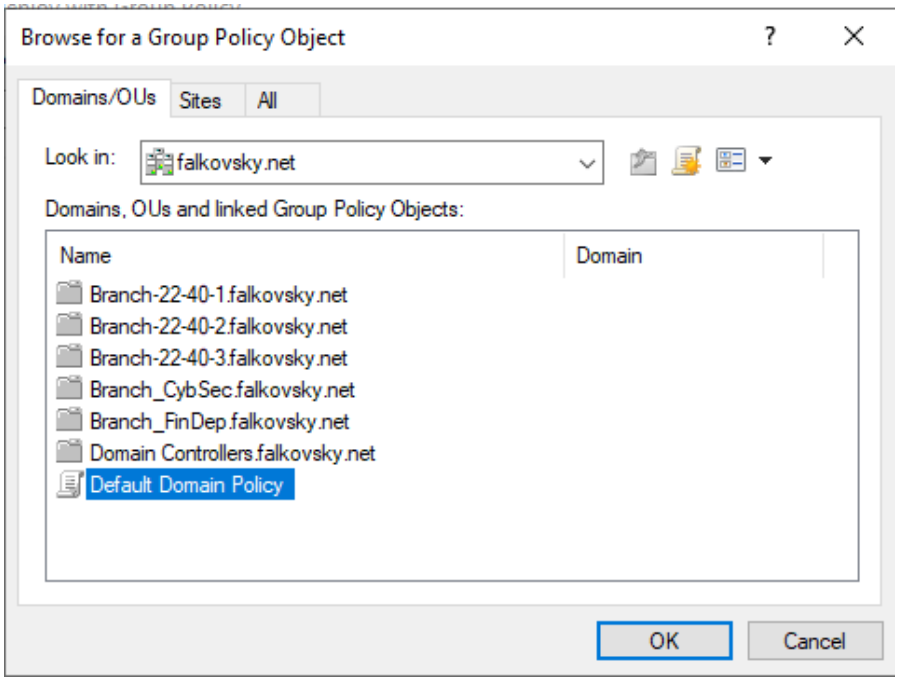


Рис. 10.24

У наступному вікні оберемо, яких суб'єктів має стосуватися налаштування - користувачів чи комп'ютерів. Якщо обрати користувачів, то для застосування конфігурації буде достатньо зачекати близько 15 хвилин або зробити оновлення конфігурації групової політики вручну. Якщо обрано комп'ютери, знадобиться перезавантаження. Оберемо користувачів (рис. 10.25) і натиснемо *Add*.

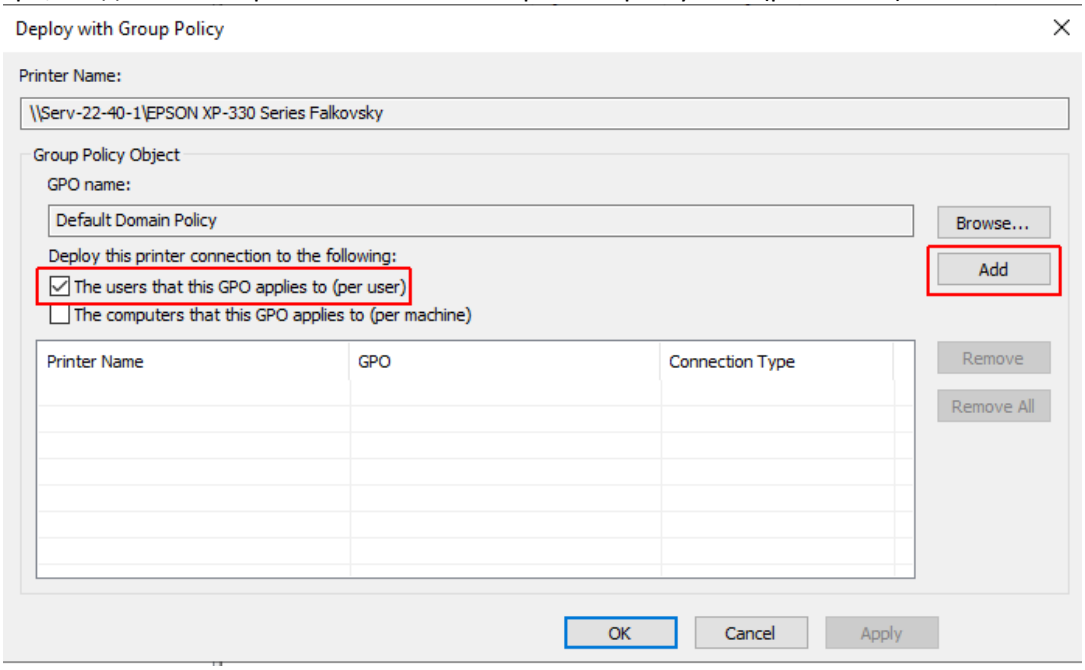


Рис. 10.25

Принтер додано (рис. 10.26). Переконайтеся у відповідності його налаштувань (ім'я, GPO, тип з'єднання) тим, які, ви встановили, і натисніть *Apply*.

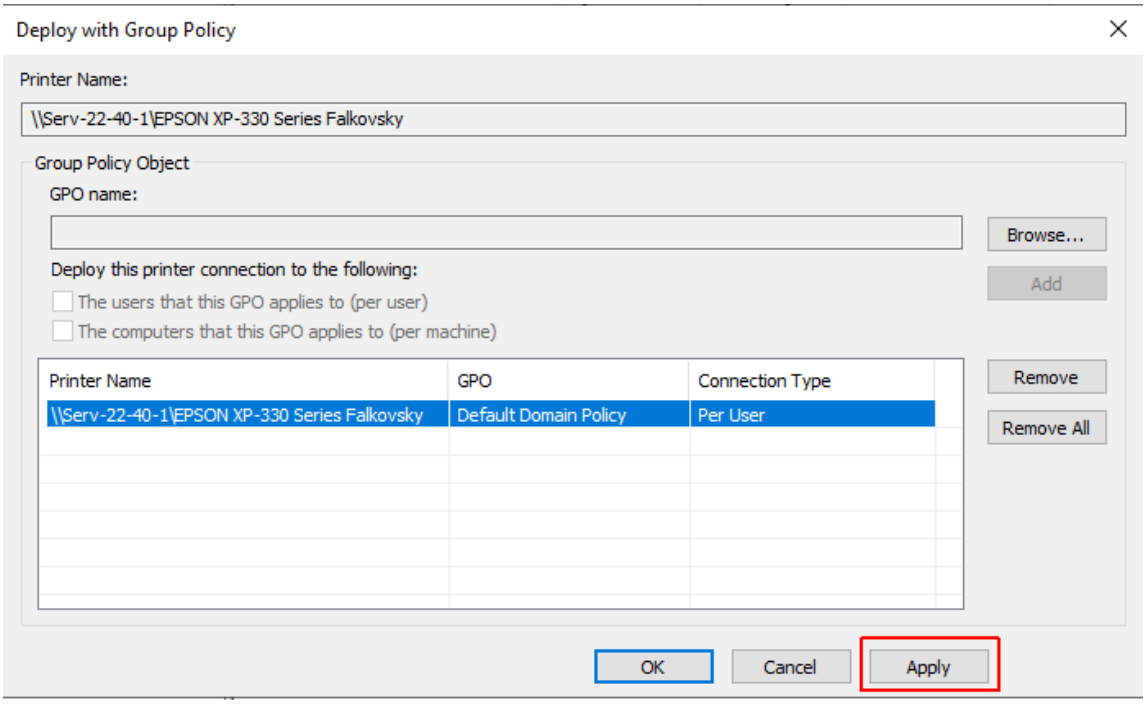


Рис. 10.26

Щоб внесені зміни швидше вступили в силу, здійсніть примусове оновлення групових політик у Power Shell:

gpupdate /force

Принтер готовий до використання членами домену (рис. 10.27).

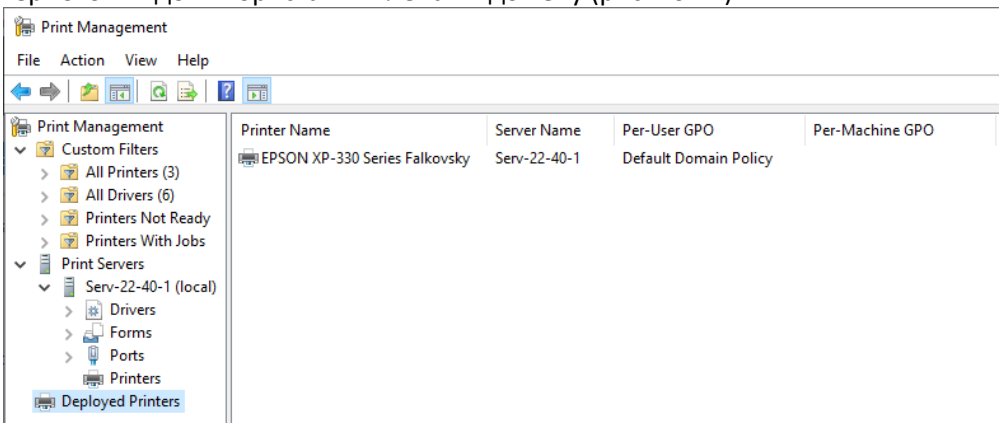


Рис. 10.27

Завдання №10.3.

1. Використовуючи подані вище інструкції, здійсніть розгортання новододаного принтера у домені *surname.net*. Принтер має бути доступний всім користувачам домену.

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Встановлення та використання принтера на робочій станції домену

Цей пункт показаний для іншої моделі принтера у іншому дереві каталогів.

В оснащенні *Print Management* у контекстному меню принтера оберемо пункт *Properties*. Для додавання принтера у бібліотеку встановіть прапорець біля відповідного налаштування (*Sharing → List in the directory*). Натисніть ОК (рис. 10.28).

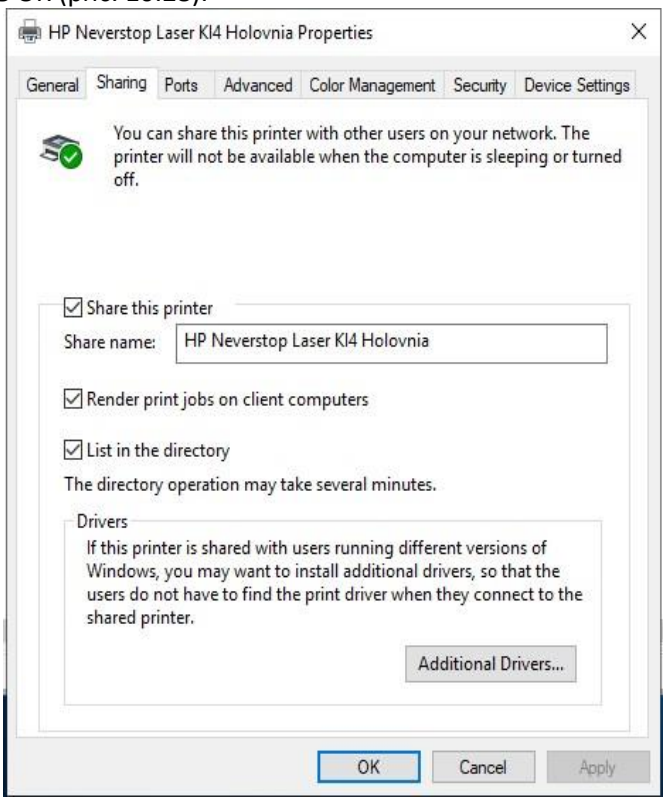


Рис. 10.28

Запустимо одну з робочих станцій домену *surname.net*. За допомогою *Панелі керування* запустимо процедуру додавання принтера з бібліотеки (рис. 10.29).

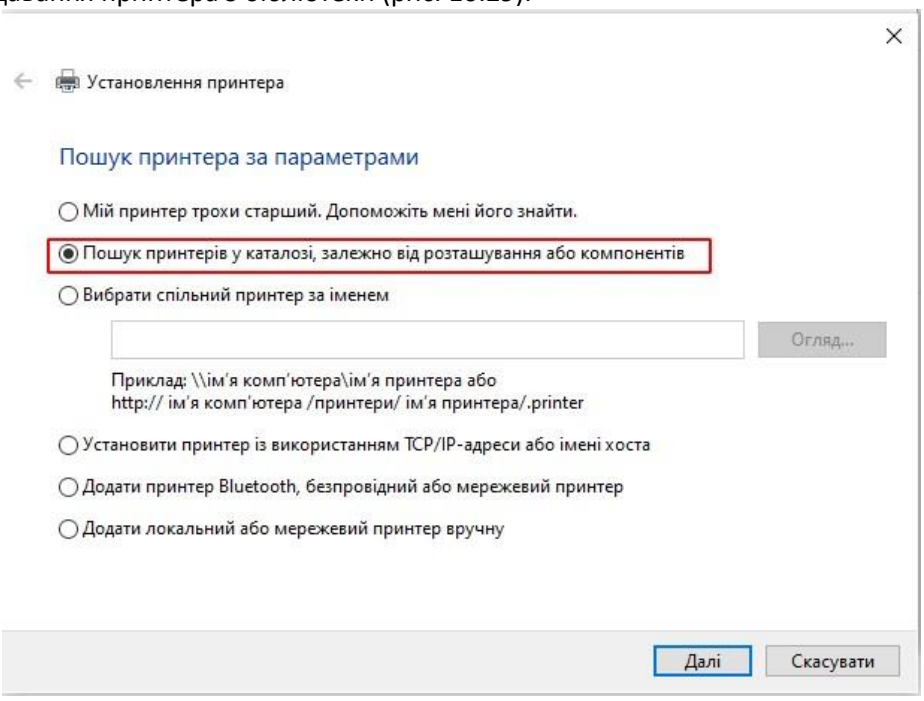


Рис. 10.29

Принтер має відображатися у вікні пошуку (рис. 10.30).

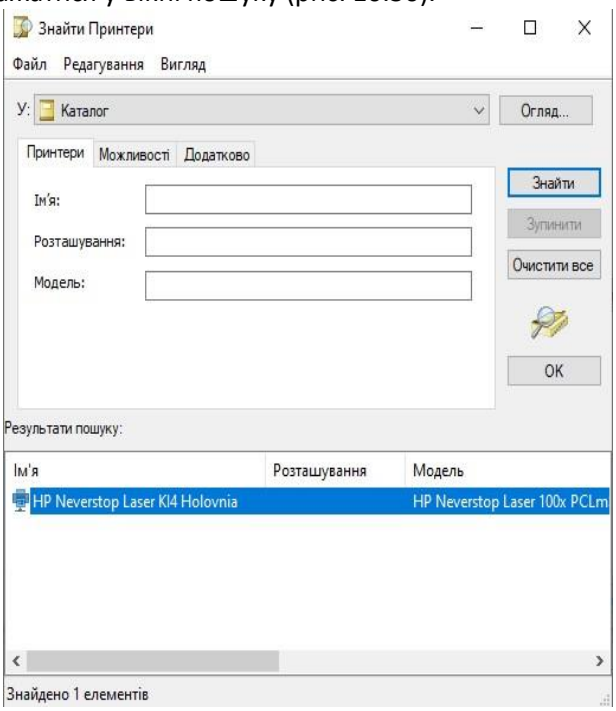


Рис. 10.30

Підтверджуємо надійність принтера - вибираємо інсталяцію драйверу і підтверджуємо це паролем адміністратора (рис. 10.31).

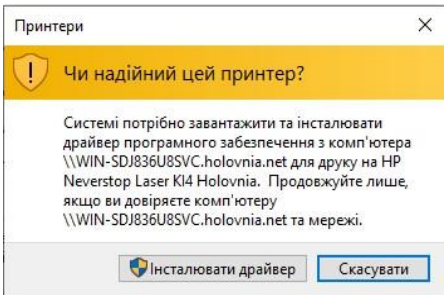


Рис. 10.31

Принтер встановлено на робочій станції разом з відповідним драйвером (рис. 10.32).

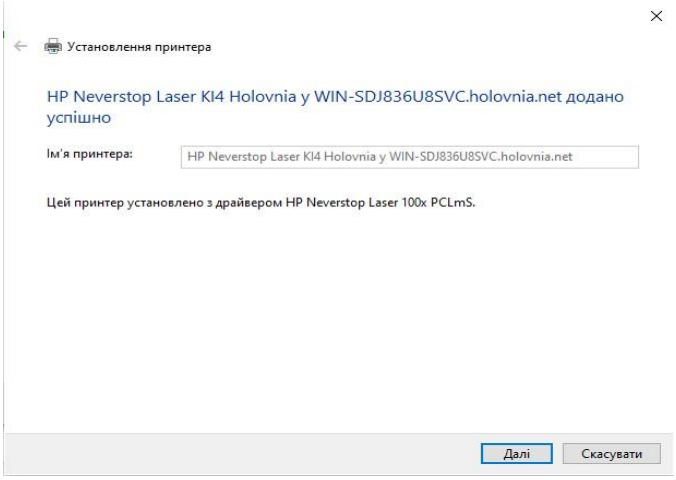


Рис. 10.33

Принтер успішно додано (рис. 10.34). Лишилося перевірити його роботу.

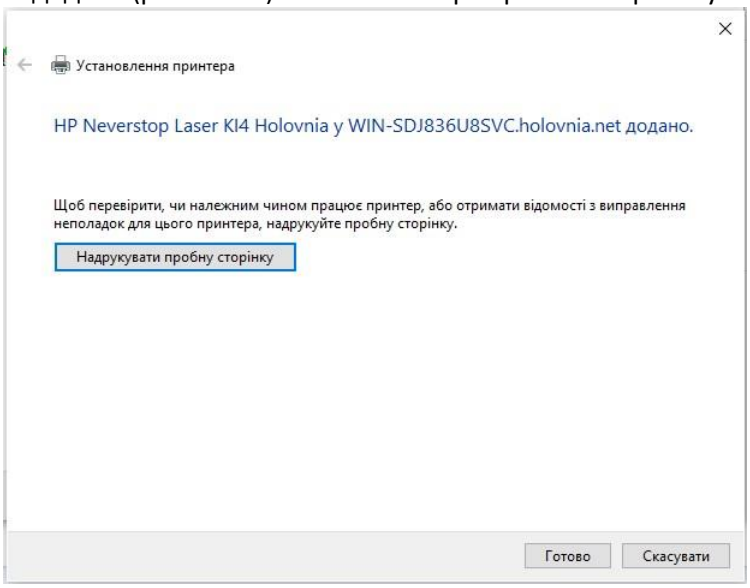


Рис. 10.34

Створимо на робочій станції текстовий файл *Holovnia.txt* і відправимо його на друк на принтері *HP Neverstop Laser KI4 Holovnia.* Файл відображається у черзі друку на робочій станції (рис. 10.35).

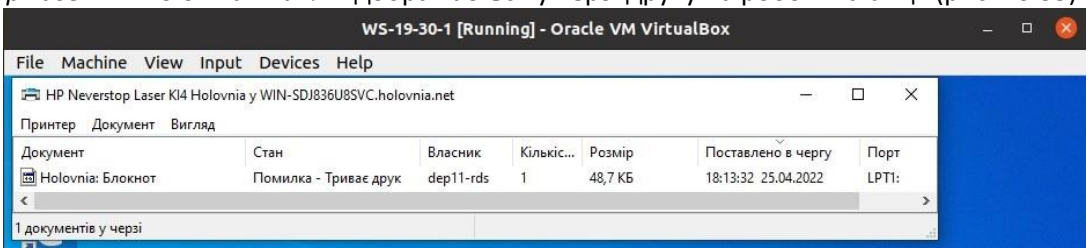


Рис. 10.35

Повідомлення про помилку друку є нормальним для нашої навчальної мережі, оскільки реальний принтер відсутній. Втім, документ відправлено на друк.

Перевіримо чергу друку на сервері. Один зі способів це зробити - через контекстне меню принтера в оснащенні *Print Management* (рис. 10.36).

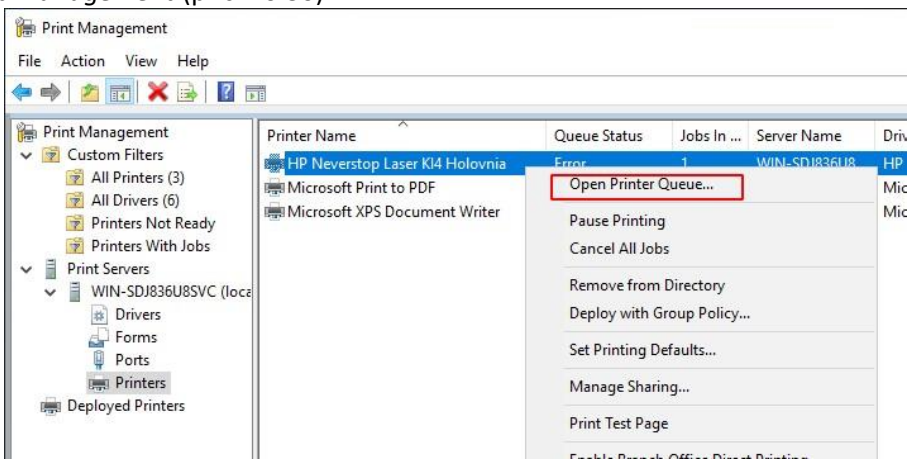


Рис. 10.36

Документ з аналогічними властивостями відображається і у черзі друку на сервері (рис. 10.37).

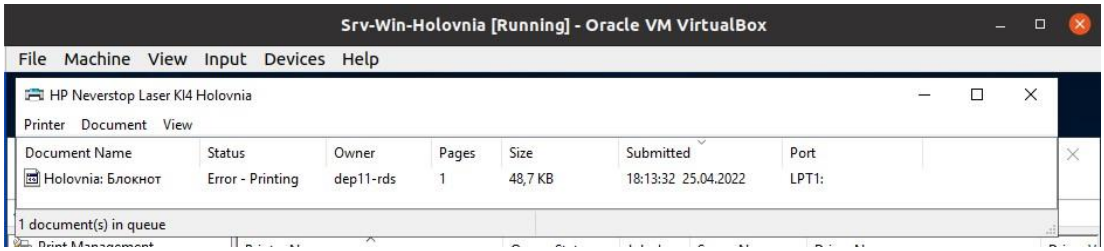


Рис. 10.37

Завдання №10.4

1. На сервері додайте принтер із попередніх завдань у бібліотеку.
2. Запустіть одну з робочих станцій домену і додайте цей принтер на даній робочій станції.
3. На робочій станції створіть текстовий документ *Surname.txt* з довільним вмістом, де *Surname* - ваше прізвище. Відправте документ на друк, обравши принтер із попередніх завдань.
4. Переконайтеся, що документ успішно надійшов у чергу друку на сервері. Переконавшись, видаліть документ із обох черг.

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 10.1-10.4.

Робота №11. Квотування у Windows Server 2022 та Active Directory

Мета: вивчити методи налаштування та види квот на базі домену Active Directory Windows Server 2019 та Windows Server 2022.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-10.

Теоретичні відомості та завдання до лабораторної роботи

Налаштування дискових квот користувачам Windows на томах

Дискові квоти дозволяють адміністраторам Windows контролювати, скільки місця використовують користувачі на файловій системі серверів і робочих станцій. Windows Server підтримує два типи квотування: квотування на базі File Server Resource Manager (дискові квоти FSRM) і NTFS квоти. Хоча FSRM квотування є більш гнучким і зручним, але в деяких простих випадках ефективно можна використовувати і NTFS квоти. Наприклад, для обмеження розмірів каталогів профілів, що переміщуються (але не User Profile Disks) та перенаправлених домашніх папок на RDS серверах, особистих каталогів користувачів на FTP сервері, особистих каталогів на сайтах IIS і т.і.

За допомогою дискових квот Windows можна обмежити максимальний розмір файлів і папок кожного користувача так, щоб він не перевищив встановленого ліміту і не зайняв своїми даними весь диск. Приналежність файлів та каталогів визначається відповідно до власника об'єкта файлової системи NTFS. Дискові квоти працюють як на серверних, так і клієнтських версіях Windows.

Основні особливості та обмеження NTFS-квот:

- Квотування може бути застосоване тільки до конкретного тому (розділу), відформатованого у файловій систем NTFS (на ReFS томах квотування не працює);
- Квоти діють на всіх користувачів, які зберігають дані на цьому розділі. Не можна застосувати квоту до групи користувачів або окремого каталогу. У цьому випадку краще використовувати квоти FSRM;
- Приналежність файлів користувачу визначається за його власником (owner) файлу, заданим у дескрипторі захисту NTFS;
- За замовчуванням Windows сканує розділ із увімкненим квотуванням і перераховує сумарний розмір файлів кожного користувача 1 раз на годину;
- При використанні NTFS-компресії враховується оригінальний розмір файлів (до стиснення).

Можна виділити такі сценарії використання дискових квот:

- *Моніторинг та оповіщення* – на додаток до першого сценарію, при перевищенні квоти в Event Viewer записується подія з інформацією про користувача та квоту.
- *Контроль використання диска* – при перевищенні квоти користувач не зможе зберегти нові файли.

Приклад налаштування NTFS квот на диску з даними користувачів на прикладі Windows Server 2019. У всіх попередніх версіях Windows (починаючи з Windows 2003) дискові NTFS квоти налаштовуються аналогічно.

Відкрийте вікно *Properties* диска, на якому потрібно включити квоти*, та перейдіть* на вкладку Quota.

Щоб увімкнути квоти для цього тому, встановіть чекбокс Enable quota management.

Подальші опції слід вибрати залежно від бажаного сценарію використання квот:

- Deny disk space to users exceeding quota limit – заборонити запис на диск користувачам, що перевищили ліміт;
- Limit disk space to – задати ліміт на сумарний розмір файлів одного користувача;
- Log event when a user exceeds their quota limit – записувати в Event Viewer подію при перевищенні квоти користувачем;
- Log event when a user exceeds their warning level – записувати у журнал події при наближенні до зазначеного порогу.

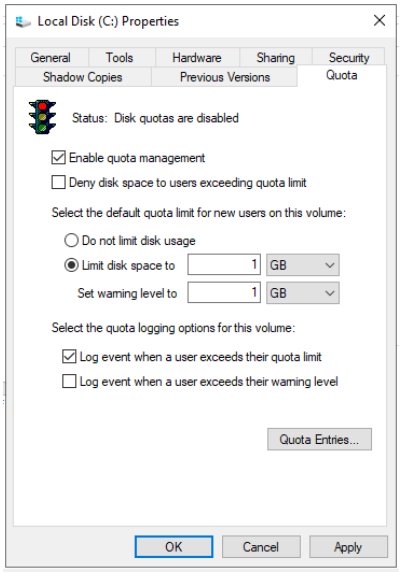


Рис.11.1.

Не рекомендується одразу вмикати режим заборони запису при перевищенні ліміту (Deny disk space to users exceeding quota limit). Спочатку доцільно оцінити поточне використання дискового простору користувачами.

У даній роботі встановлюється квота 1 ГБ для кожного користувача. Натисніть Apply. Через деякий час (залежно від розміру диска та кількості файлів) система виконає підрахунок використаного дискового простору для кожного користувача.

Натисніть кнопку Quota Entries. У таблиці відображаються:

- ✓ встановлені квоти;
- ✓ фактичне використання дискового простору користувачами.

Зверніть увагу на службові облікові записи

NT SERVICE\TrustedInstaller та NT AUTHORITY\SYSTEM.

Для них рекомендується встановити параметр Do not limit disk usage, оскільки обмеження може призвести до некоректної роботи служб операційної системи.

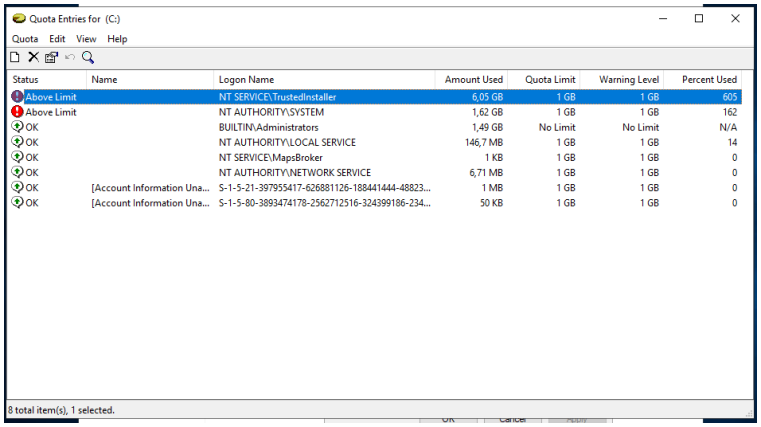


Рис.11.2.

За замовчуванням, для всіх користувачів встановлюються однакові квоти. З вікна *Quota Entries* можна створити, збільшити або вимкнути стандартну квоту для конкретного користувача.

Щоб квоти NTFS не застосовувалися до певного облікового запису, потрібно відкрити властивості запису в таблиці квот (*Properties*) і встановити опцію
Do not limit disk usage.

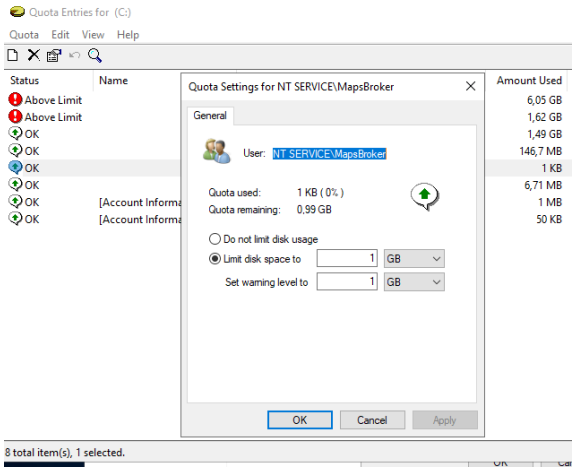


Рис.11.3.

З вікна зі списком квот можна експортувати параметри квот, а потім імпортувати та застосовувати їх для іншого диска або комп'ютера.

Якщо ви бажаєте вивести список файлів, які обліковуються в квоті конкретного користувача, потрібно вибрати пункт *Delete*.

З цього діалогового вікна можна змінити власника файлу (*Take ownership*), видалити (*Delete*) або перемістити файл (*Move*).

Після того, як навели лад з м'якими квотами в режимі аудиту, можна включати опцію
Deny disk space to users exceeding quota limit

Це увімкне режим жорстких квот. Тепер користувачі не зможуть перевищити виділене місце на диску. Зверніть увагу, що розмір диска на сесії користувача тепер відображається з урахуванням дискової квоти. Приклад, для облікового запису користувача на диску C:\ вільно 876 Мб з 1 Гб квоти.

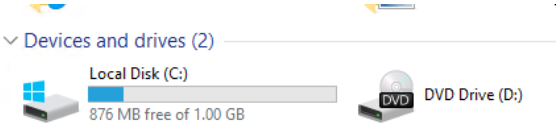


Рис. 11.4.

При перевищенні квоти користувач отримує повідомлення:

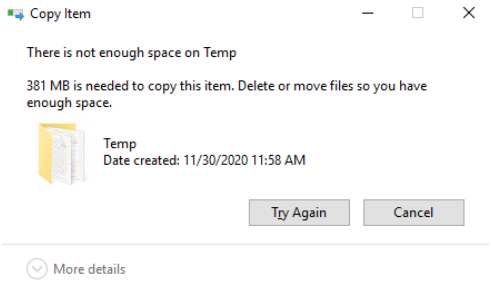


Рис. 11.5.

Одночасно у журналі системи фіксується подія з EventID 37, source: Ntfs

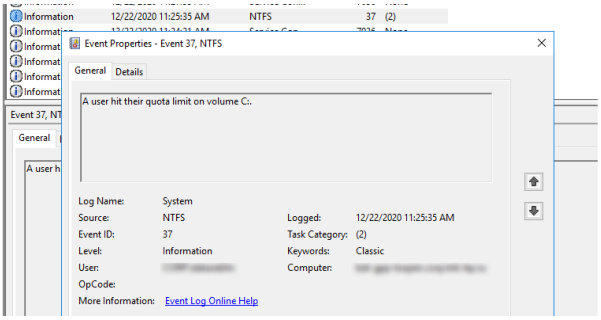


Рис. 11.6.

Увага! Перед зміною поточної сесії користувача обов'язково перевірте правильність виконаних налаштувань квот.

Неправильно задані параметри (зокрема занадто малі значення лімітів або відсутність виключень для службових облікових записів NT SERVICE\TrustedInstaller та NT AUTHORITY\SYSTEM) можуть призвести до некоректної роботи служб операційної системи або блокування сервера.

Усунення наслідків неправильно налаштованих квот не входить до змісту даної роботи.

Завдання №11.1

1. Запустіть віртуальну машину з Windows Server (перший контолер домену).
2. Створіть у групі користувачів admin-1 домену користувача з іменем ***Ваше_Прізвище_Варіант***. Наприклад *falkovsky_NN*.
3. Користуючись поданими вище інструкціями, для тому C: задайте режим м'якого квотування з обмеженням виділеного місця до 1 Гб та порогом попередження 900 Мб для створеного користувача.
4. Зніміть обмеження квот для системних облікових записів TrustedInstaller та System.
5. Увімкніть режим жорстких квот.
6. Змініть сеанс поточного користувача на ***Ваше_Прізвище_Варіант*** та перегляньте доступне місце на томі C:

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Налаштування дискових квот за допомогою групових політик

Керування та налаштування дискових квот на комп'ютерах та серверах домену за допомогою групових політик виконується через оснащення *Group Policy Management Console*. Параметри налаштування квот знаходяться в розділі GPO Computer Configuration -> Administrative Templates -> System -> Disk Quotas.

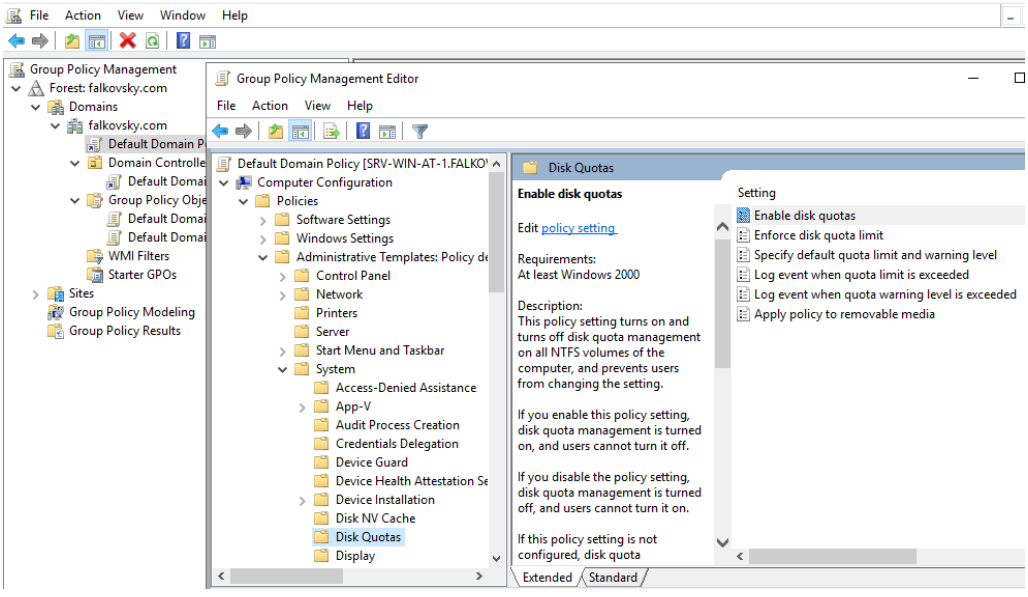


Рис. 11.7.

Щоб увімкнути дискові квоти, аналогічні розглянутим вище, задайте наступні політики:

- Apply Policy To Removable Media: Enable (якщо потрібно використовувати квоти для знімних носіїв, у тому числі USB флешок)

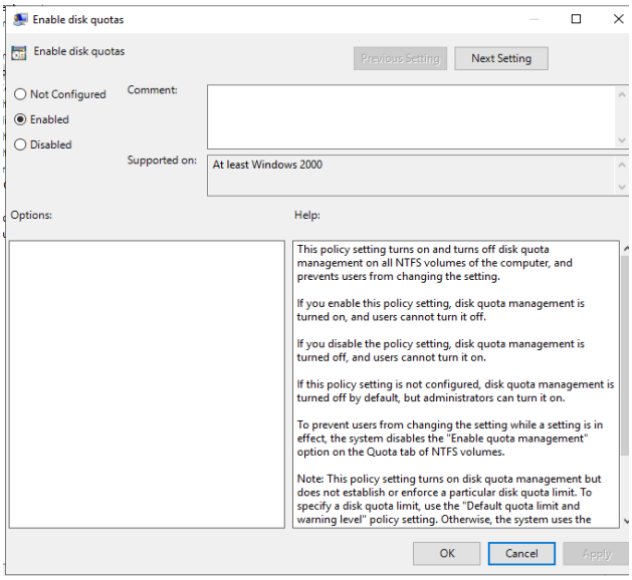


Рис. 11.8.

Enable Disk Quotas: Enable

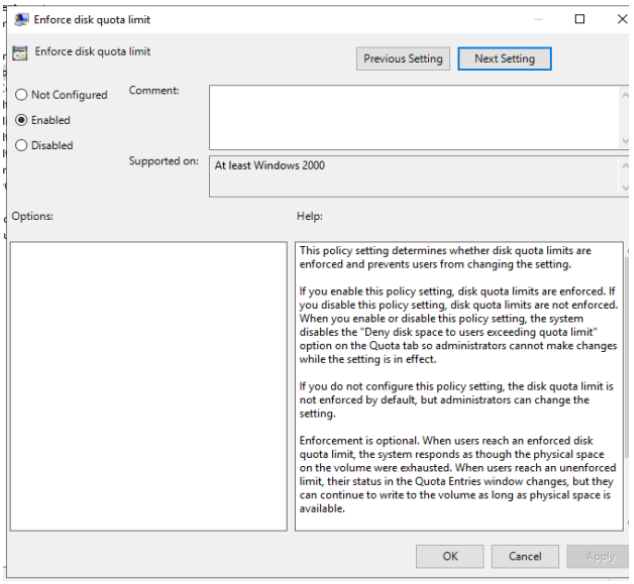


Рис. 11.9.

Enforce Disk Quota Limit: Enable

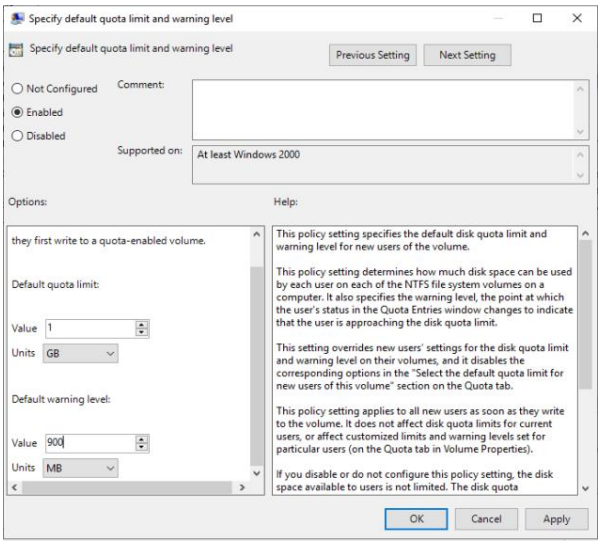


Рис. 11.10.

Default Quota Limit And Warning Level: Enable (Default quota limit 1Gb/warning level: 900 Mb)

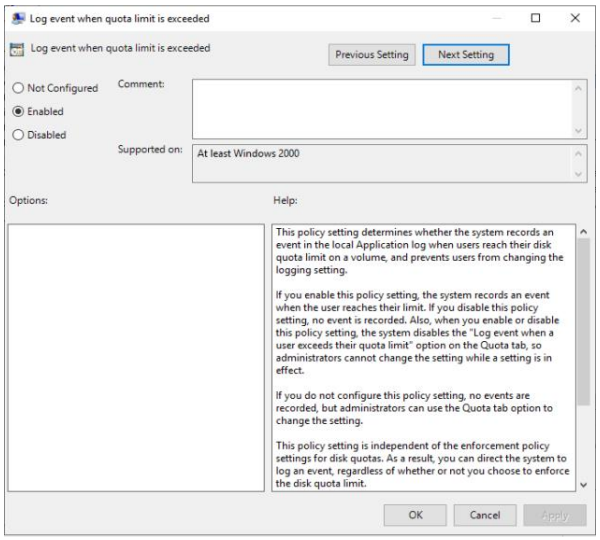


Рис. 11.11.

Log Event When Quota Limit Exceeded: Enable

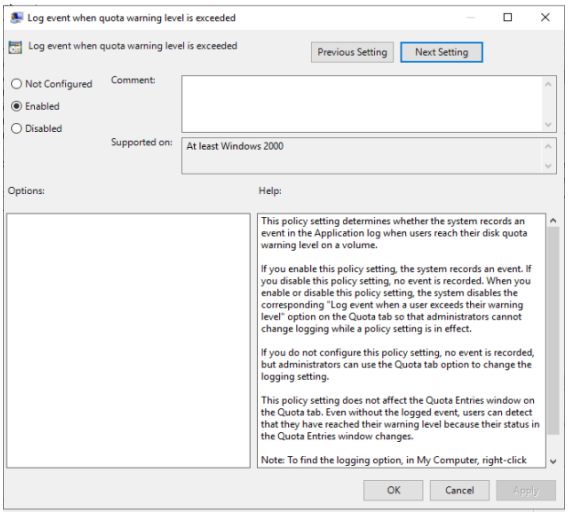


Рис. 11.12.

Log Event When Quota warning is Exceeded: Enable

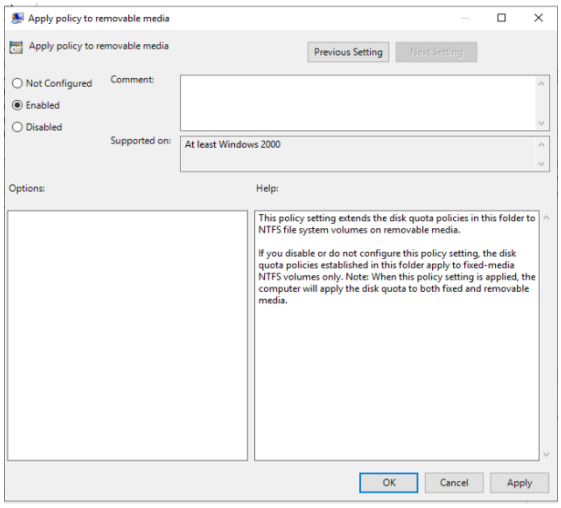


Рис. 11.13.

Apply Policy To Removable Media: Enable (якщо потрібно використовувати квоти для змінних носіїв, у тому числі флешок)

Залишилося оновити GPO на OU із комп'ютерами/серверами, на яких потрібно впровадити дискові квоти. Оновлення виконувати під користувачем Administrator.

Завдання №11.2

1. Запустіть віртуальну машину з Windows Server (другий контолер домену).
2. Користуючись поданими вище інструкціями, задайте на сервері за допомогою групових політик режим м’якого квотування з обмеженням виділеного місця до 1 Гб та порогом попередження 900 Мб.
3. Змініть сеанс поточного користувача на створеного у п.11.1.2 (***Ваше_Прізвище_Варіант***) та перегляньте доступне місце на томах серверу.

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Керування дисковими квотами з командного рядка/PowerShell

NTFS-квотами можна керувати з командного рядка Windows за допомогою утиліти fsutil quota.

Увімкнення режиму відстеження (м’які квоти):

fsutil quota track C:

У цьому режимі система лише відстежує використання диска користувачами.

Увімкнення режиму жорстких квот:

fsutil quota enforce C:

Після цього користувачі не зможуть перевищувати встановлений ліміт.

Вимкнення квот:

fsutil quota disable C:

Перегляд параметрів квот:

fsutil quota query C:

Перегляд зафіксованих порушень квот:

fsutil quota violations

Налаштування частоти повідомлень про порушення:

Перегляд поточного значення:

fsutil behavior query quotanotify

Встановлення нового значення (у секундах):

fsutil behavior set quotanotify <seconds>

Наприклад, 1 година:

fsutil behavior set quotanotify 3600

У більшості випадків перезавантаження системи не потрібне.

Зміна порогів квоти для користувача:

fsutil quota modify C: <warning> <limit> DOMAIN\user

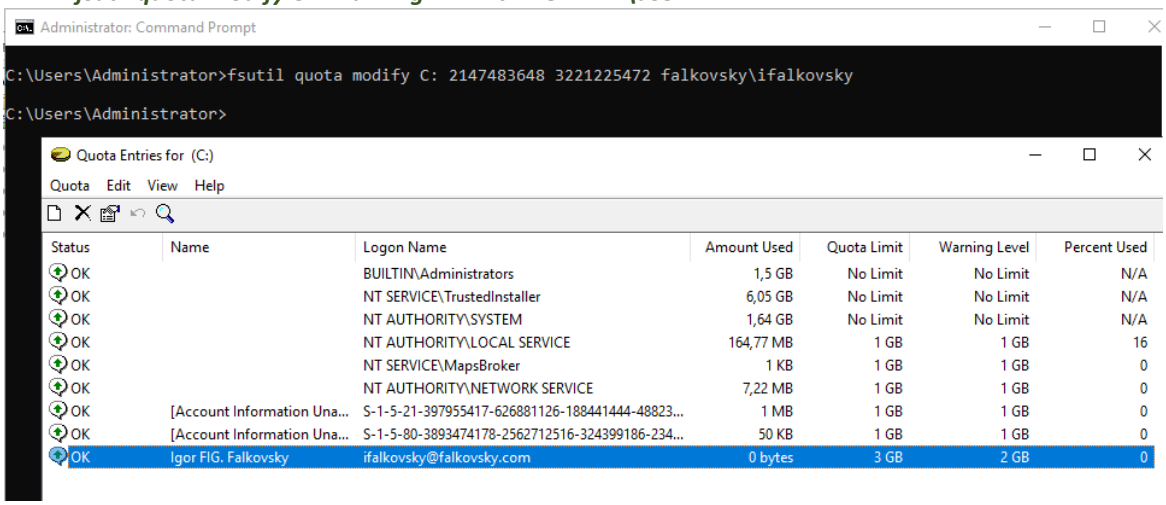


Рис. 11.13.

Розміри задаються у байтах. Наприклад, команда:

fsutil quota modify C: 3221225472 2147483648 DOMAIN\user

Розміри квот задаються у байтах (3 ГБ = 3×1024×1024×1024; 2 ГБ = 2×1024×1024×1024).

перше значення — рівень попередження (warning level);

друге значення — максимальний обсяг даних користувача на диску (жорстка квота, limit);

DOMAIN\user — обліковий запис користувача.

У PowerShell немає спеціалізованих командлетів для керування NTFS-квотами. Однак отримати інформацію про квоти можна через WMI-клас Win32_DiskQuota. PowerShell слід запускати від імені адміністратора.

Отримання інформації про квоти користувачів:

Get-CimInstance -ClassName Win32_DiskQuota |

Select-Object QuotaVolume, User, DiskSpaceUsed, Limit, WarningLimit

Ця команда відображає: том квоти, користувача, використаний обсяг, рівень попередження, жорсткий ліміт. Властивість User є об’єктом WMI; для відображення імені користувача можна звернутися до User.Name.

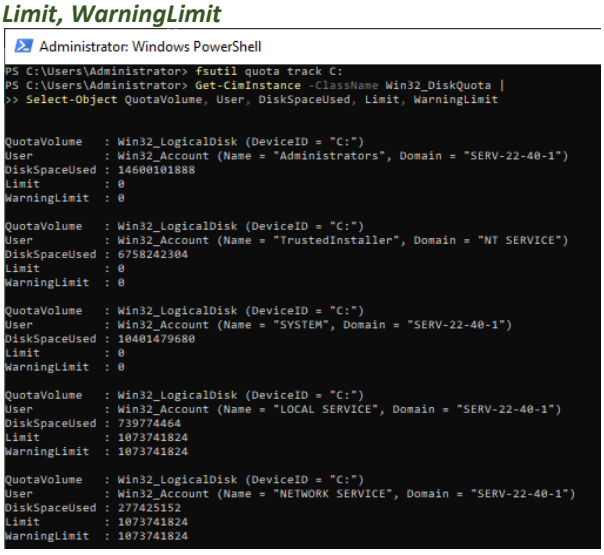


Рис. 11.14.

Після ввімкнення квот система виконує фоновий перерахунок використання дискового простору. Повне оновлення статистики може зайняти деякий час і залежить від

- обсягу тома,
- кількості файлів,
- продуктивності сервера.

Завдання №11.3

1. Змініть квоту користувача з п.11.1.2 у командному рядку на обох серверах з обмеженням виділеного місця до 2 Гб та порогом попередження 900 Мб.
2. Перегляньте новий розмір квот у Quota Entries for (C:)
3. Перегляньте поточні квоти користувачів через PowerShell на обох серверах.

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Більш гнучкі та розширені можливості квотування надає розгорнута роль файлового серверу. Для цього необхідно встановити файлові служби, служби ролі BranchCache для мережевих файлів та службу ролі дедуплікації даних.

Відкрийте Dashboard Server Manager, а потім натисніть кнопку Додати ролі та компоненти. Відкриється майстер додавання ролей та компонентів. На сторінці Перед початком роботи натисніть кнопку Next.

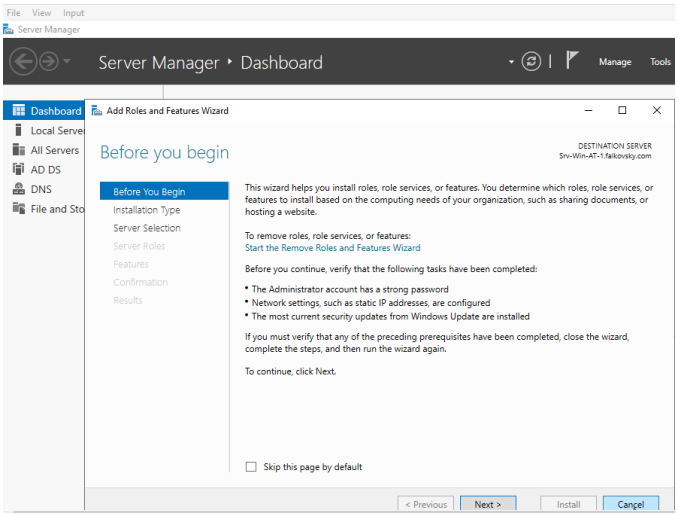


Рис. 11.15.

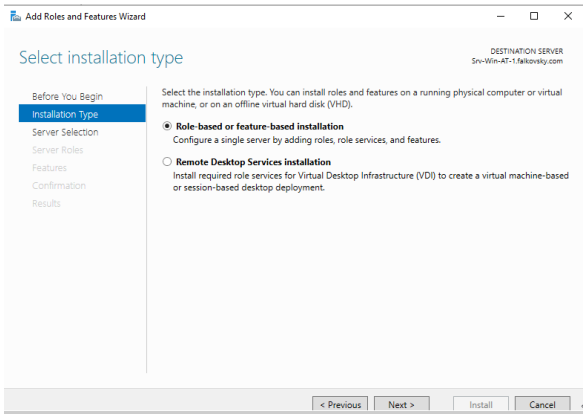


Рис. 11.16.

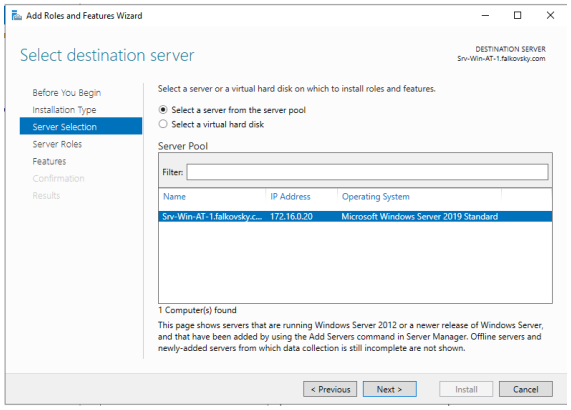


Рис. 11.17.

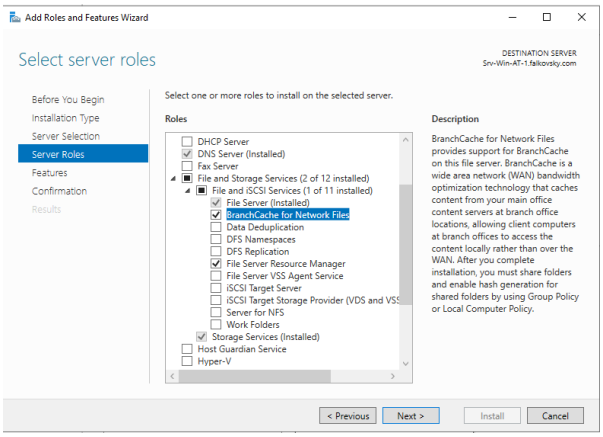


Рис. 11.18.

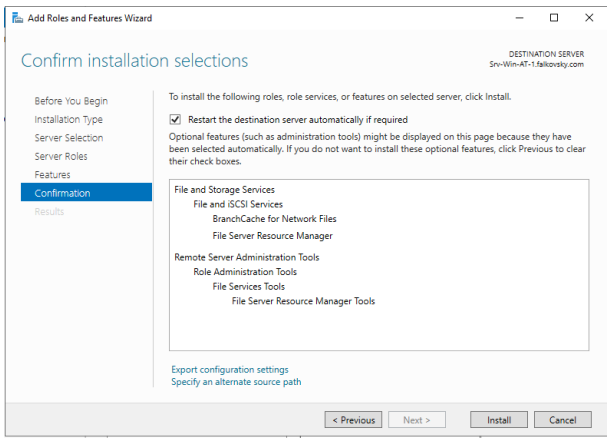


Рис. 11.19.

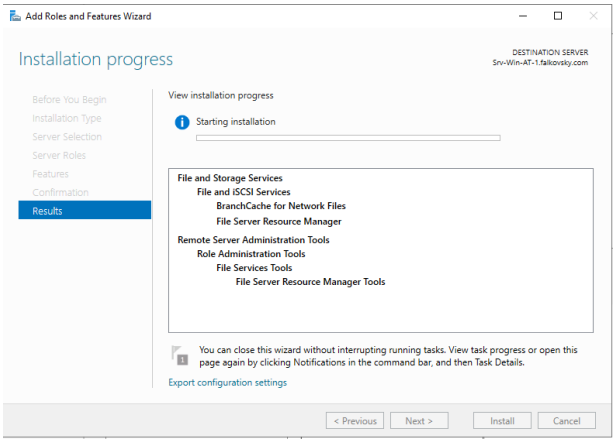


Рис. 11.20.

Щоб виконати цю процедуру за допомогою Windows PowerShell, запустіть Windows PowerShell від імені адміністратора, введіть по черзі наступні команди в командному рядку:

Install-WindowsFeature -Name FS-BranchCache -IncludeManagementTools
Install-WindowsFeature -Name FS-Data-Deduplication -IncludeManagementTools
Restart-Computer

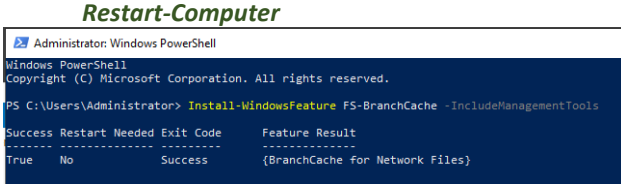


Рис. 11.20.

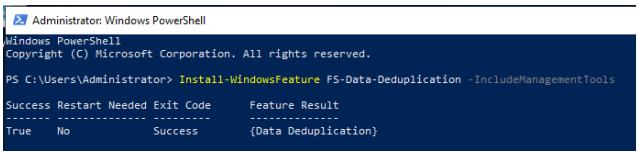


Рис. 11.21.

Відповідно, отримання інформації про встановлену роль:

Get-WindowsFeature -Name FS-BranchCache, FS-Data-Deduplication

Видалення цієї ролі:

Remove-WindowsFeature -Name FS-BranchCache, FS-Data-Deduplication

Після перезавантаження серверу доступне оснащення File Server Resource Manager (FSRM) Console.

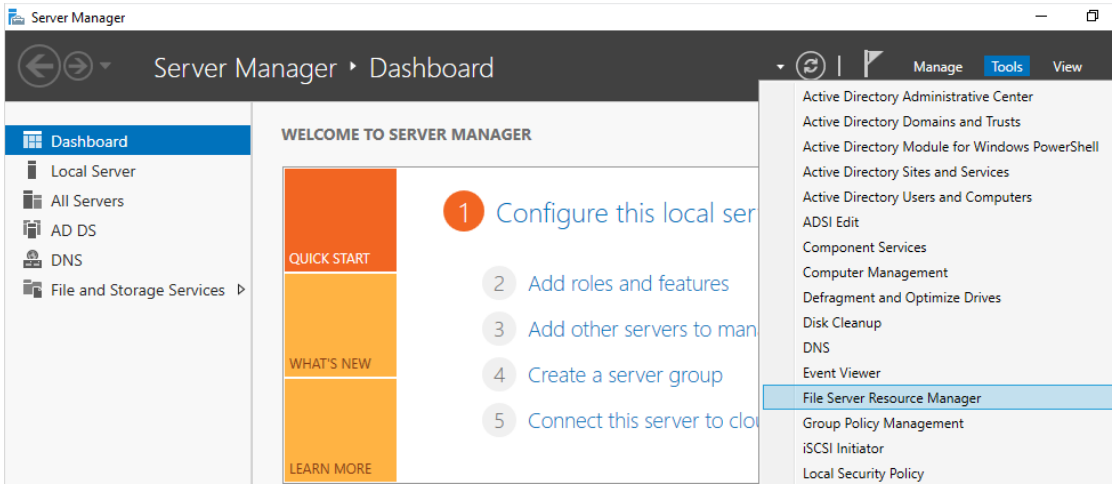


Рис. 11.22.

Диспетчер ресурсів файлового сервера (*FSRM*) — це служба ролі Windows Server, яка дозволяє керувати даними, що зберігаються на файлових серверах, і класифікувати їх. Диспетчер

ресурсів файлового сервера можна використовувати для автоматичної класифікації файлів, виконання завдань на основі цих класифікацій, встановлення квот для папок та створення звітів про використання сховища.

Диспетчер ресурсів файлового сервера включає такі функції:

- Керування квотами (*Quota Management*) дозволяє обмежити простір, відведений для тома або папки, і вони можуть автоматично застосовуватися до нових папок, створених на томі. Також можливо визначити шаблони квот, які можна застосовувати до нових томів або папок.
- Інфраструктура класифікації файлів (*Classification Management*) дозволяє краще зрозуміти дані, автоматизуючи процеси класифікації для ефективного управління даними. Можливо класифікувати файли та застосовувати політики на основі цієї класифікації. Приклади політик включають динамічний контроль доступу для обмеження доступу до файлів, шифрування файлів та закінчення терміну дії файлів. Файли можна класифікувати автоматично, використовуючи правила класифікації файлів або вручну, змінюючи властивості обраного файлу чи папки.
- Завдання управління файлами (*File Management Tasks*) дозволяють застосовувати умовну політику чи дію до файлів з урахуванням їх класифікації. Умови завдання керування файлами включають розташування файлу, властивості класифікації, дату створення файлу, дату останньої зміни файлу або час останнього звернення до файлу. Дії, які може виконувати завдання управління файлами, включають можливість закінчення терміну дії файлів, шифрування файлів або запуск команди користувача.
- Управління фільтруванням файлів (*File Screening Management*) допомагає контролювати типи файлів, які користувач може зберігати на файловому сервері. Можливо обмежити розширення, яке може зберігатися у спільних файлах. Наприклад, можна створити фільтр файлів, який не дозволяє зберігати файли з розширенням MP3 в особистих спільних папках на файловому сервері.
- Звіти про сховище (*Storage Reports Management*) допомагають визначити тенденції використання диску та класифікацію даних. Також можливо відстежувати вибрану групу користувачів щодо спроб збереження неавторизованих файлів.

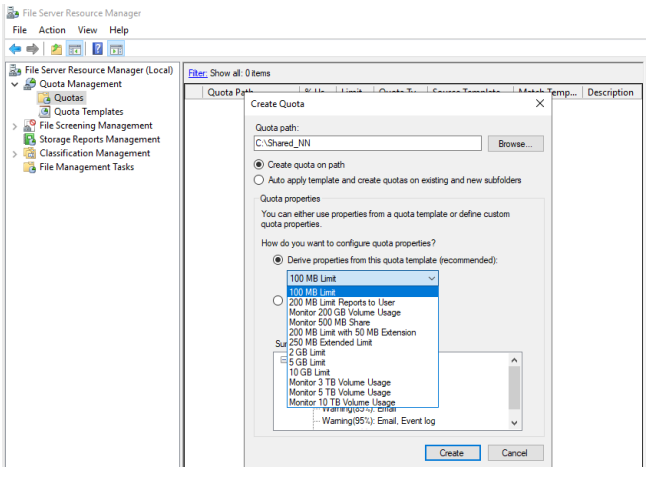


Рис. 11.23.

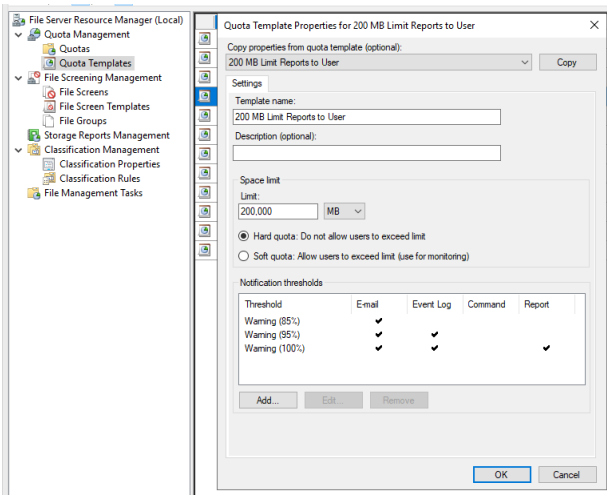


Рис. 11.24.

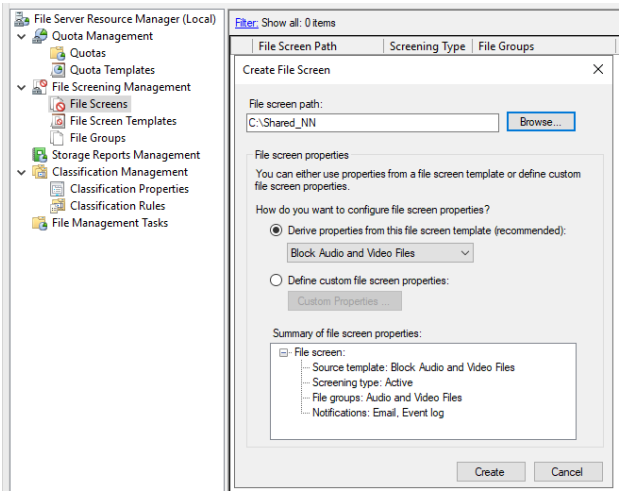


Рис. 11.25.

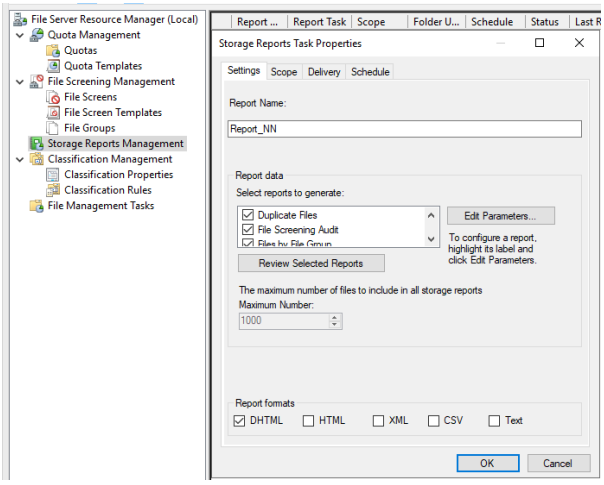


Рис. 11.26.

Функції, включені до диспетчера ресурсів файлового сервера, можна налаштовувати та керувати ними за допомогою програми диспетчера ресурсів файлового сервера або за допомогою Windows PowerShell.

Для отримання чи встановлення квот NTFS диспетчера ресурсів файлового сервера, можливо використовувати командлети FileServerResourceManager PowerShell. Раніше отримання і встановлення квот каталогів NTFS виконувалося за допомогою команди *dirquota*, яка є застарілою, але залишилась у системі при розгортанні FSRM для сумісності.

Сучасна версія дозволяє досить легко керувати квотами за допомогою PowerShell. Створюємо нову квоту:

New-FsrmQuota -Path "ШЛЯХ-ДО_РЕСУРСУ" -Description "limit usage to 1 GB." -Size Квота

Отримуємо інформацію про квоти ресурсу:

Get-FsrmQuota -PATH "ШЛЯХ-ДО_РЕСУРСУ"

Змінюємо квоту ресурсу:

Set-FsrmQuota -PATH "ШЛЯХ-ДО_РЕСУРСУ" –Size Нова_квота

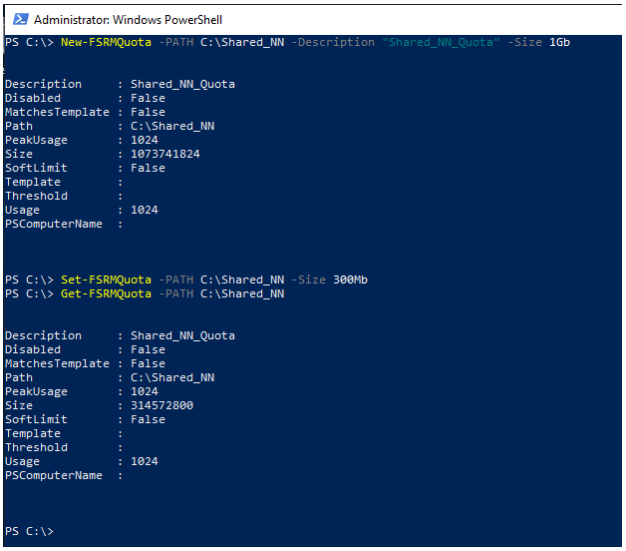


Рис. 11.26.

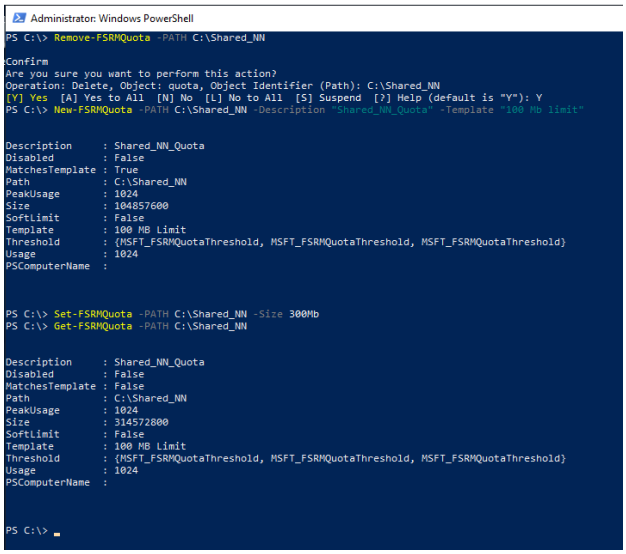


Рис. 11.27.

Завдання №11.4

1. Додайте будь-яким методом на ВМ з Windows Server (перший контролер домену) роль файлового серверу.
2. Створіть на томі (C:) серверу файловий ресурс Shared_NN, де NN – номер Вашого варіанту.
3. Застосуйте до створеного спільного ресурсу шаблон квот “100 Mb limit” (hard quota), та змініть його таким чином, щоб відправка попередження на пошту користувачу відбувалась при перевищенні граничного ліміту 50 Mb.
4. Заплануйте створення у кожну неділю звіту Report_NN на підставі стандартного шаблону звітів у форматі txt на файловому ресурсі Share_NN, де NN – номер Вашого варіанту.
5. За допомогою PowerShell збільшіть граничний ліміт квоти для файлового ресурсу Share_NN, де NN – номер Вашого варіанту до 200 Mb. Покажіть стан файлового ресурсу до та після зміни ліміту квоти.

Звіт має містити скриншоти одержаних відомостей, опис основних дій, відповіді на поставлені запитання.

Корисні посилання

Managing Disk Quotas
https://learn.microsoft.com/en-us/windows/win32/fileio/managing-disk-quotas

Enable or Disable Disk Quotas in Windows. Tutorials
https://www.tenforums.com/tutorials/99888-enable-disable-disk-quotas-windows.html

File Server Resource Manager (Part 1: Install FRSM - Part 7: File Management Tasks)
https://4sysops.com/archives/file-server-resource-manager-fsrm-part-3-quota-management/

Module PowerShell GetCimInstance
https://learn.microsoft.com/en-us/powershell/module/cimcmdlets/get-ciminstance?view=powershell-7.3

PowerShell File Server Resource Manager
https://learn.microsoft.com/en-us/powershell/module/fileserverresourcemanager/?view=windowsserver2022-ps&redirectedfrom=MSDN&viewFallbackFrom=winserverr2-ps

Робота № 12. Налаштування сайту на веб-сервері IIS з використанням Windows Server 2022 та Active Directory

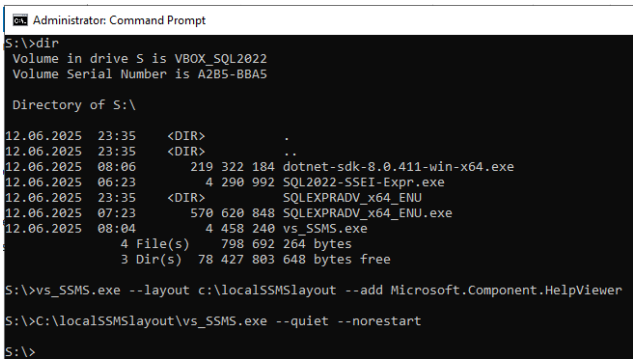
Мета: Вивчити практичні аспекти налаштування IIS для DevOps-орієнтованого розгортання сучасних вебзастосунків у середовищі Windows Server 2022 та AD.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-11.

Підготовчі роботи.

Наша модель мережі навчальна, і на її віртуальних машинах може бути відсутнє інтернет-з'єднання. Перед виконанням лабораторної роботи можливо знадобиться завантажити на свій ПК наступне програмне забезпечення:

- **SQL Server Management Studio 21.x.x.** Завантаження офлайн-інсталятора SSMS 21 (SQL Server Management Studio) «трохи приховане», оскільки Microsoft зазвичай пропонує онлайн-завантажувач. Для його отримання переходимо на офіційну сторінку завантаження, отримуємо файл онлайн інсталяції



https://aka.ms/ssms/21/release/vs_SSMS.exe
запускаємо його у командному рядку

vs_SSMS.exe --layout c:\localSSMSlayout --add Microsoft.Component.HelpViewer

Повний інсталяційний пакет збережеться у каталозі c:\localSSMSlayout. Актуальний на момент написання цих рекомендацій архів інсталяційного пакету доступний по лінку:
https://drive.google.com/file/d/14_-xYhUMxC-OYNG4GTOJBL88xiQDIfn3/view?usp=drive_link

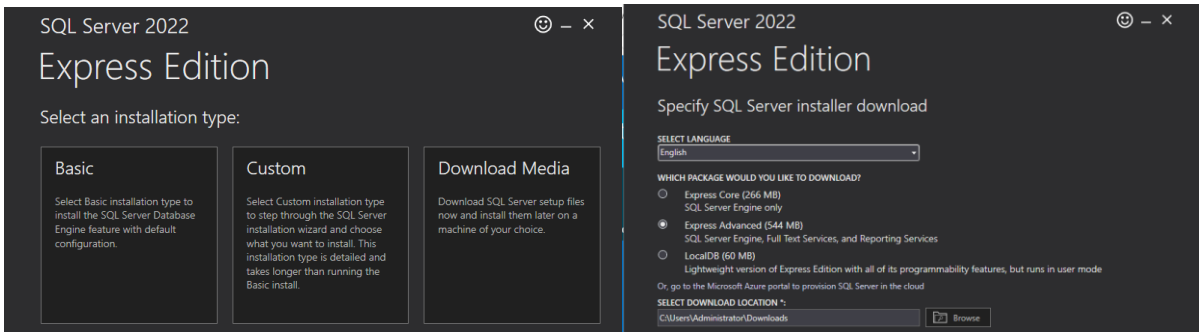
- **.NET SDK 8**
https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/sdk-8.0.411-windows-x64-installer
https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.17-windows-hosting-bundle-installer

- **MS SQL Express 2022** offline installer

Microsoft трохи "заховала" офлайн-інсталятор SQL Server Express 2022 — зазвичай пропонується маленький web-installer. Для завантаження повноцінного офлайн-інсталятора SQL Server 2022 Express Edition необхідно виконати наступні кроки:

Переходимо на офіційну сторінку Microsoft: https://www.microsoft.com/en-us/sql-server/sql-server-downloads

Прокручуємо до секції SQL Server 2022 Express та натискаємо кнопку Download now – це завантажить невеликий файл онлайн інсталятора SQL2022-SSEI-Expr.exe (розмір ~4,2 МБ). Запускаємо його і у вікні, що завантажиться висвічується можливі режими встановлення: Basic, Custom або Download Media



Обираємо Download Media і у цьому вікні потрібну мову (English) Express Advanced та місце збереження файлу. Натискаємо Download. Це завантажить повну офлайн-версію (~600 МБ).

Ви також можете завантажити цей файл по посиланню
https://drive.google.com/file/d/1iuUj9EvCvf3FendAw2jI2DjqPh2SQXk2/view?usp=drive_link

Завантаження інсталяційних пакетів на віртуальний сервер Serv-G-N-01 DC1 навчальної мережі виконується безпосередньо через лінки або через створений загальний ресурс VirtualBox в залежності від налаштувань мережі. На рис. 12.1 показане монтування спільного каталогу та флешки.

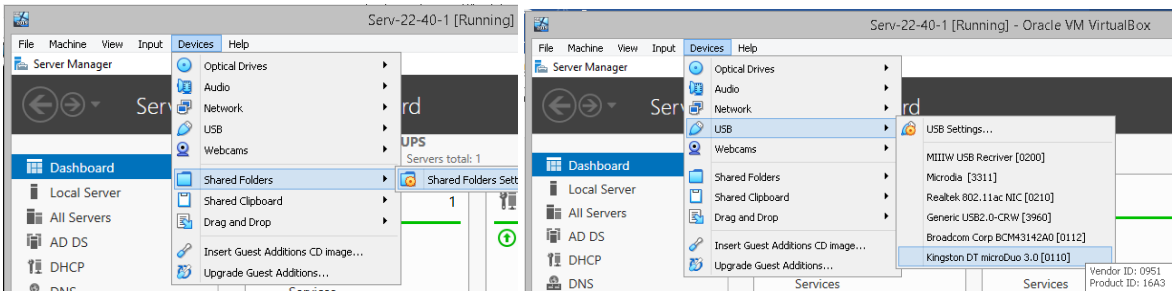


Рис. 12.1

Примітка. Для роботи зі спільними папками потрібні гостьові доповнення. Якщо вони ще не встановлені на цю віртуальну машину, їх потрібно встановити через системне меню машини Devices – Insert Guest Additions CD image (Рис. 12.2)

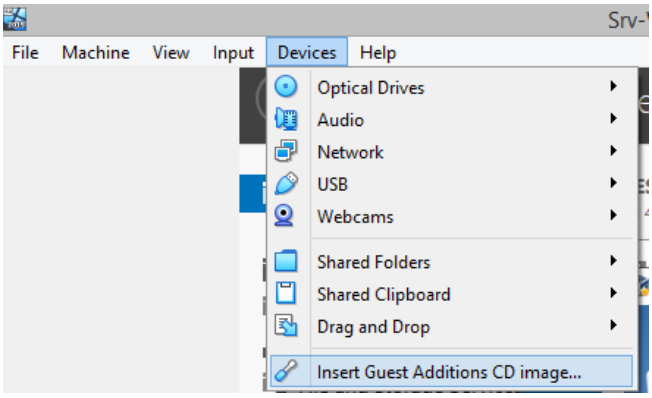


Рис.12.2

У віртуальній машині виконуємо встановлення ПЗ з змонтованого віртуального носія (рис. 12.3-12.6).

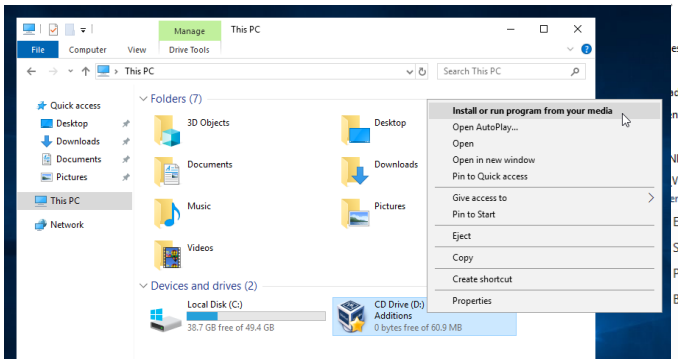


Рис.12.3

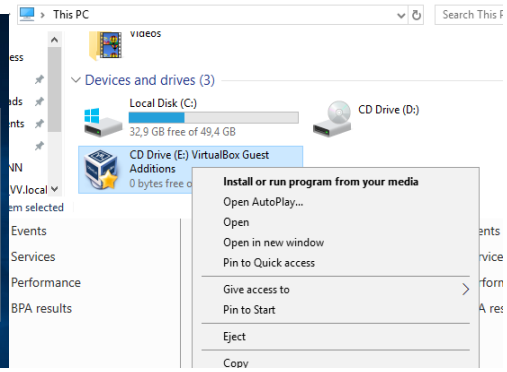


Рис.12.4

Рис.12.5

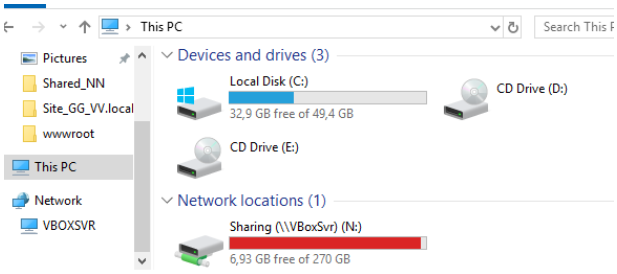


Рис.12.6

Після завершення встановлення, вилучаємо диск з гостьовими доповненнями з віртуального пристрою.

Теоретичні відомості та завдання до лабораторної роботи

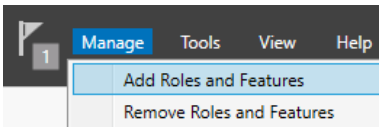
Розгортання Web Server IIS

Зазвичай, коли мова іде про веб-сервери, мається на увазі рішення на базі платформи Linux. Але якщо інфраструктура розгорнута на базі Windows Server, логічно та набагато зручніше використовувати веб-сервер IIS. З іншого боку, це дуже популярна платформа, яка дозволяє працювати як з більшістю популярних CMS, так і має широкий спектр систем, призначених для роботи саме на Windows і IIS.

Головним бонусом використання IIS є його тісна інтеграція з іншими технологіями та засобами розробки Microsoft. Зокрема, веб-рішення для IIS можуть використовувати багаті можливості .NET і легко взаємодіяти з десктопними додатками на цій платформі. Якщо вас це поки не цікавить, то до ваших послуг багатий вибір готових CMS, у тому числі розроблених спеціально для IIS.

Розглянемо, як встановити і налаштувати IIS для роботи з веб-рішеннями на базі ASP.NET і встановити одну з популярних CMS для цієї платформи.

Для встановлення веб-сервера на платформі Windows відкриваємо Dashboard Server Manager, а потім натисніть кнопку Додати ролі та компоненти. Відкриється майстер додавання ролей та компонентів.



На сторінці Перед початком роботи натисніть кнопку Next. Обираємо встановлення ролей Web Server IIS. Якщо не обирати додаткові Features, ми отримаємо Web Server IIS у мінімальній конфігурації.

Але не поспішаємо натискати Next, ліворуч, під назвою кожної ролі, доступна опція Служби ролей, перейдемо на неї і встановимо для Сервера програм такі опції: Підтримка веб-сервера (IIS), Загальний доступ до TCP-портів та Активація через HTTP.

У п. Application Development обов'язково додаємо ASP.Net 4.8.(рис.12.7.) Для функціонування CMS Orchard Core 2.x вимагається ASP.Net 4.7, або вище.

Ці складові можуть бути вже встановлені при виконанні попередніх лабораторних робіт.

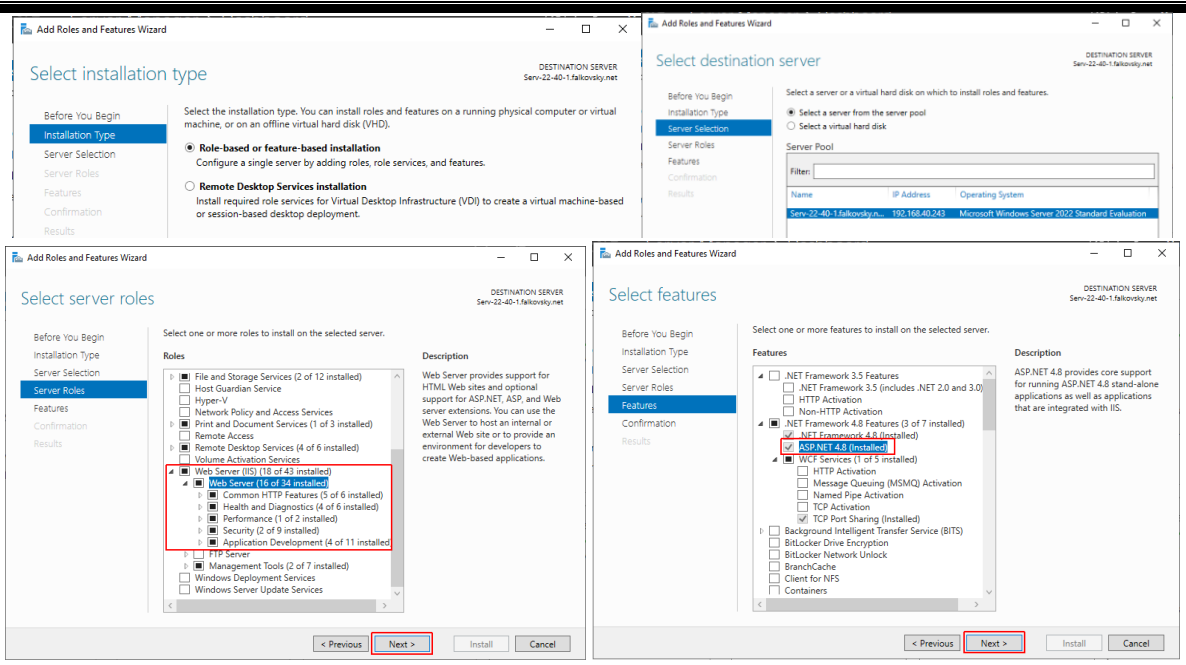


Рис. 12.7

Обов'язково встановлюємо компоненти Net FrameWork 4.8 та ASP.NET 4.8. (рис.12.7).

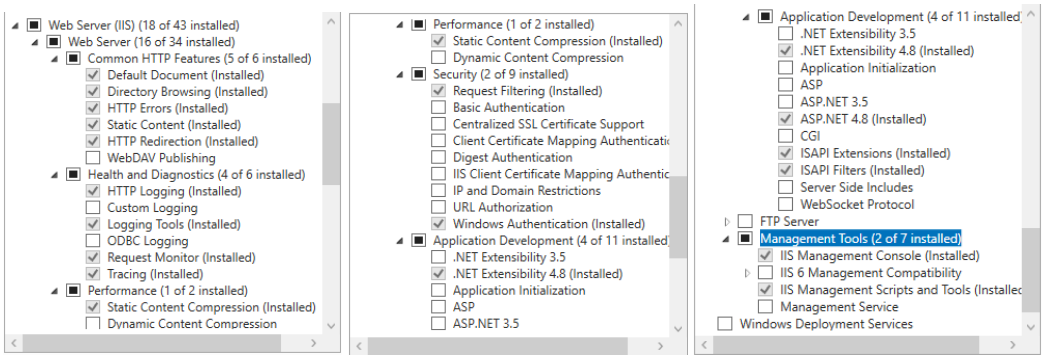


Рис. 12.8

На рис. 12.8 показані компоненти IIS (Roles & Features), які необхідні для функціонування WEB-стеку на основі Orchard Core 2.x. Ось їх перелік:

<u>Роль: Web Server (IIS) Web Server</u>

- Common HTTP Features
- Static Content
- Default Document
- HTTP Errors
- Performance Features
- Static Content Compression *(опційно, але бажано)*

- Security
- Request Filtering
- Windows Authentication *(опціонально, якщо потрібна аутентифікація через Windows)*
- Basic Authentication *(опційно)*
- Application Development
- .NET Extensibility 4.8 *(не критично, але іноді потрібно для інтеграції з іншими додатками)*
- ASP.NET 4.8 *(необов'язково, Orchard Core працює на ASP.NET Core)*
- ISAPI Extensions
- ISAPI Filters
- WebSocket Protocol *(опційно для Orchard Core, але може бути корисно для реального часу)*

Після розгортання Web-server IIS, його дієздатність простіше всього перевірити виконавши на сервері вхід через Microsoft Edge на сторінку 127.0.0.1 (рис.12.9)

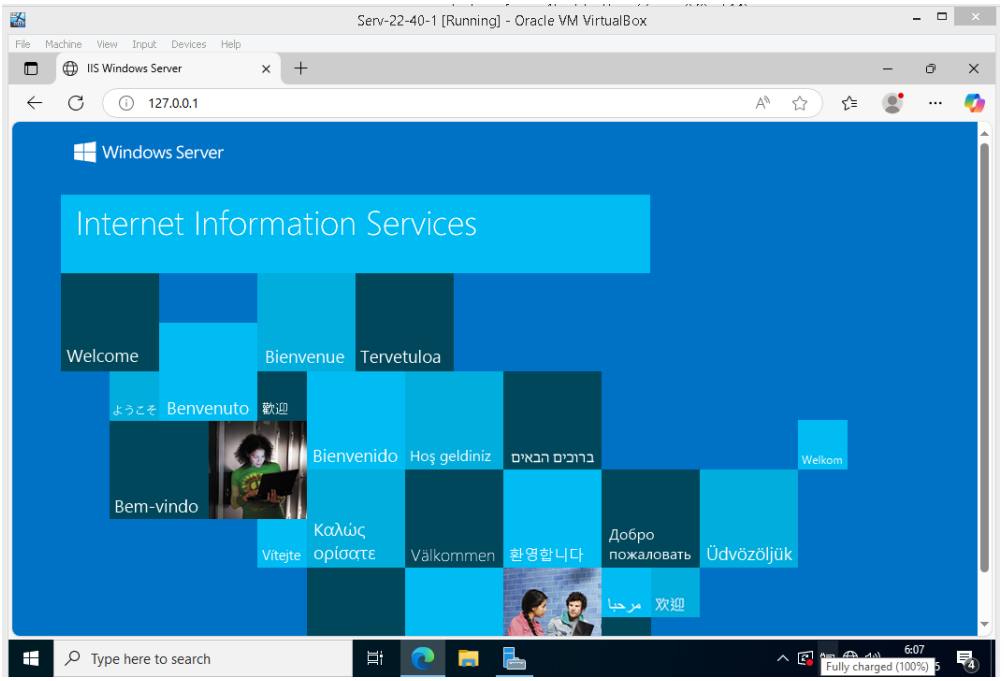


Рис. 12.9

Завдання №12.1

1. Запустіть віртуальну машину з Windows Server 2022, на якій Ви виконували лабораторну роботу №10 «Налаштування спільного принтера на базі Windows Server 2022 та Active Directory».

2. Користуючись, описаними вище рекомендаціями, перевірте, чи розгорнуто роль Web-server та його працездатність. Додайте, за необхідності, компоненти IIS (Roles & Features), які необхідні для функціонування WEB-стеку на основі Orchard Core 2.x.

Розгортання MS SQL

Для функціонування повноцінного сайту необхідно розгорнути систему управління базою даних (СУБД). Це дозволить отримати в розпорядження повноцінний веб-сервер, який дасть змогу запускати весь спектр веб-додатків як платних, так і безкоштовних. Однією з типових СУБД для MS IIS є MS SQL. Поточна версія MS SQL 2022 випущена в наступних редакціях:

- *Enterprise Edition* – повноцінна редакція MS SQL Server, призначена для використання в реальних проектах і не має обмежень щодо обчислювальних потужностей.
- *Standard Edition* - повноцінний випуск, що має певні апаратні обмеження.
- *Express Edition* - безкоштовний випуск для роботи простих програм. Може використовуватися на вирішення реальних завдань, але має деякі апаратні обмеження.
- *Developer Edition* – повнофункціональна безкоштовна редакція для розробників. Даний випуск не може використовуватися для роботи як реальний SQL-сервер, але може бути застосований для вивчення і тестування механіки MS SQL Server.
-

Як описано у п. підготовчі роботи, на сервер завантажено дистрибутив СУБД - безкоштовна версія *MS SQL Express Edition 2022* offline installer.

Виконуємо інсталяцію MS SQL-express-2022.

Лінк для завантаження файлу offline інсталятора SQLExpress Advanced 2022:

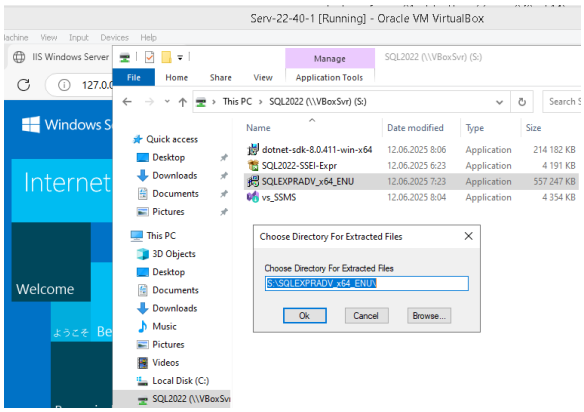


Рис.12.10.

https://drive.google.com/file/d/1iuUj9EvCvf3FendAw2jI2DjqPh2SQXk2/view?usp=drive_link

Обираємо новий SQL-server без кластеризації, погоджуємось на оновлення та з умовами ліцензійної угоди (рис.12.11, 12.12):

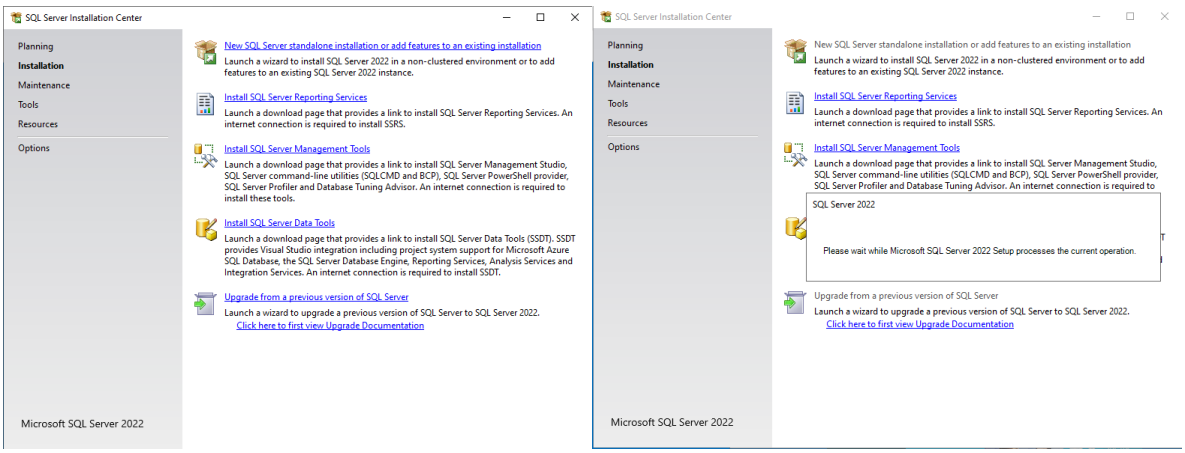


Рис.12.11.

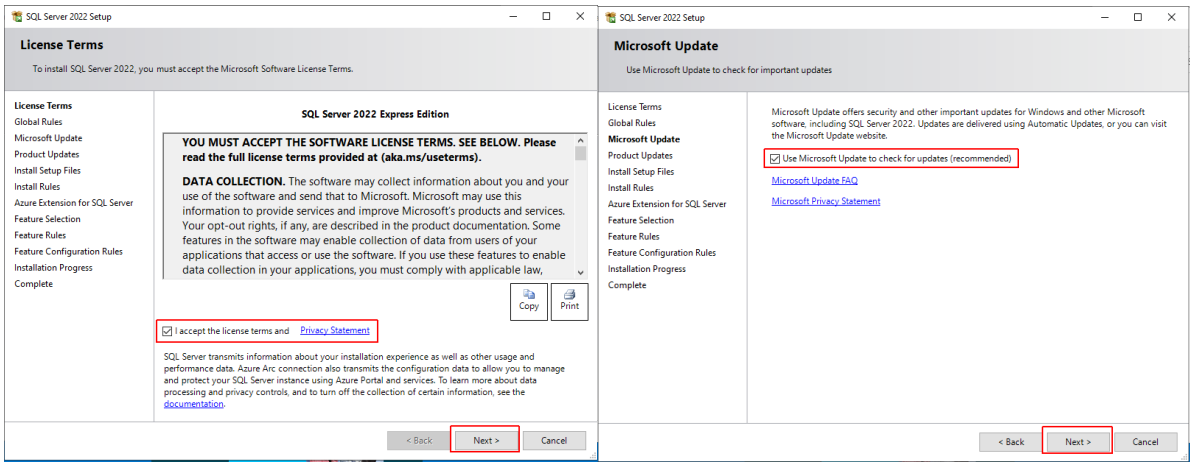


Рис.12.12.

Через обмеженість ресурсів у роботі, ігноруємо попередження, про розгортання СУБД на домен-контролері. Відмовляємось від встановлення розширень MS Azure. У компонентах для встановлення вимикаємо Machine Learning Service and Language Extensions та залишаємо ім'я екземпляру серверу без змін (рис.12.13). Компонент Machine Learning Service and Language Extensions дозволяє запускати зовнішні скрипти мовами R, Python, Java безпосередньо всередині SQL Server і є складовою Enterprise SQL Server.

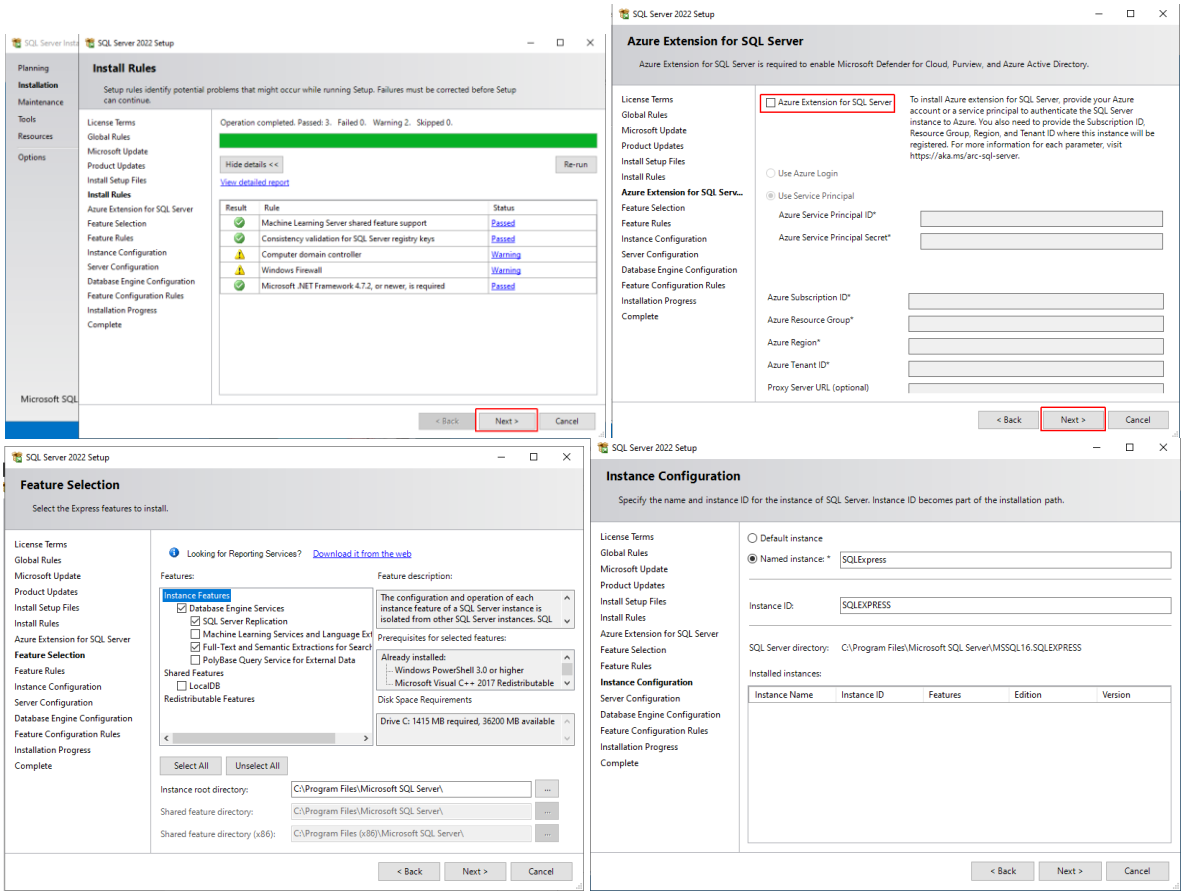


Рис.12.13.

Залишаємо без змін права права облікових записів та права на том. Обираємо змішаний режим автентифікації та вводимо пароль для суперюзера MS SQL sa. Також на цьому кроці можливо змінити робочі каталоги СУБД (рис.12.14).

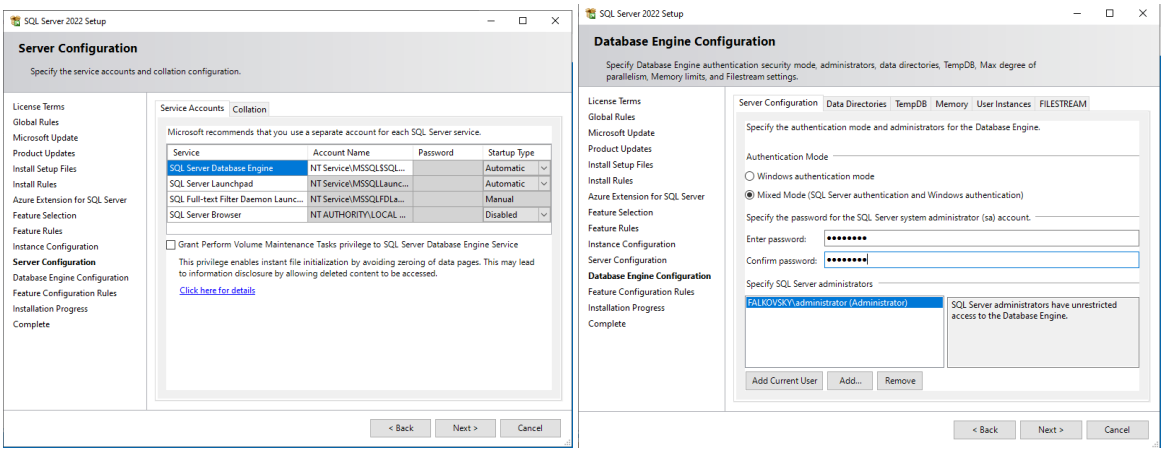


Рис.12.14.

На цьому кроці розгортання серверу SQL Express 2022 завершено (рис.2.15).

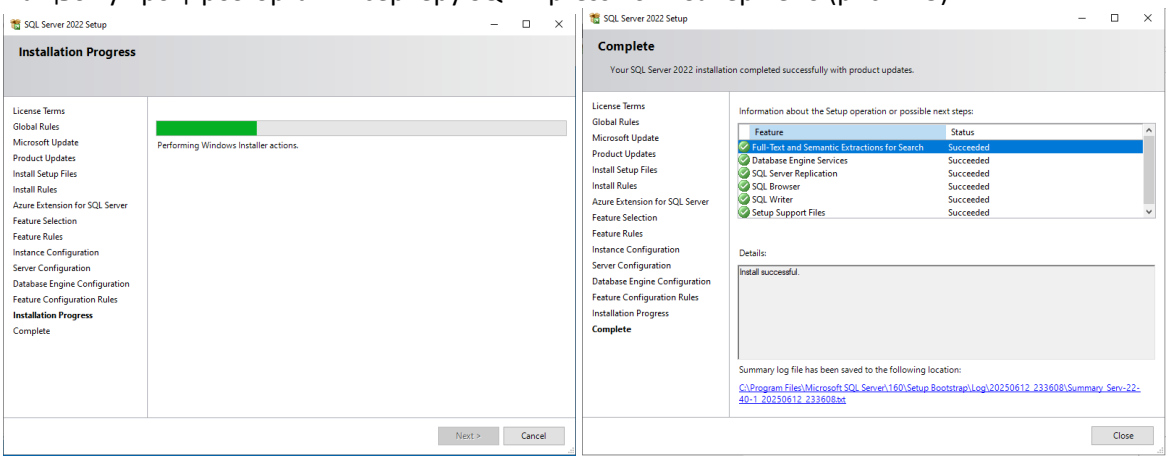


Рис.12.15.

Як описано у розділі «Підготовчі роботи» отримуємо інсталяційний пакет SQL Server Management Studio 21.x.x та виконуємо його «тихе» встановлення через командний рядок:

C:\localSSMSlayout\vs_SSMS.exe --quiet –norestart

Результатом встановлення буде поява відповідного пункту системного меню сервера (рис.12.16). Зверніть увагу на відмітку “Trust Server Certificate”

Після успішного підключення у SSMS виконуємо правий клік по серверу → Properties → вкладка Security. Має бути "SQL Server and Windows Authentication mode". Якщо Ви змінили цей параметр, виконайте перезапуск сервісу (процес показаний на рис.12.18).

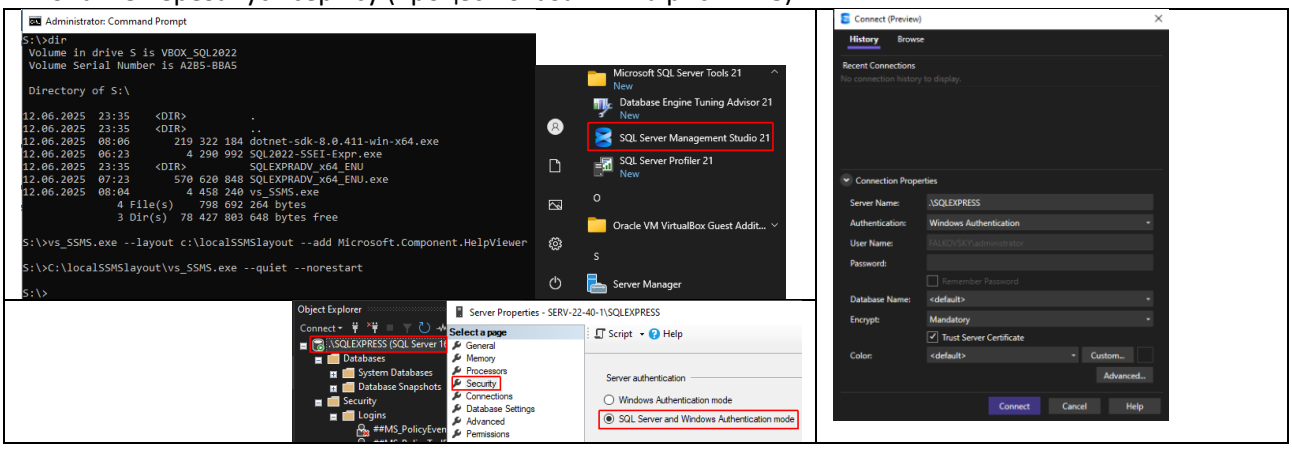


Рис.12.16.

Якщо підключення не відбулось перевіряємо відкритість порту TCP 1433. Це порт SQL Server за замовчанням. Це офіційний номер сокету IANA (агентство з виділення імен та унікальних параметрів протоколів Інтернету) для SQL Server. Клієнтські системи використовують порт TCP 1433 для підключення до системи керування базами даних; у середовищі SQL Server Management Studio (SSMS) порт призначено для керування екземплярами SQL Server через мережу. Можливо налаштувати SQL Server для прослуховування іншого порту.

Розгортання серверу виконано без зміни портів, а тому перевіряємо відкриття портів 1433

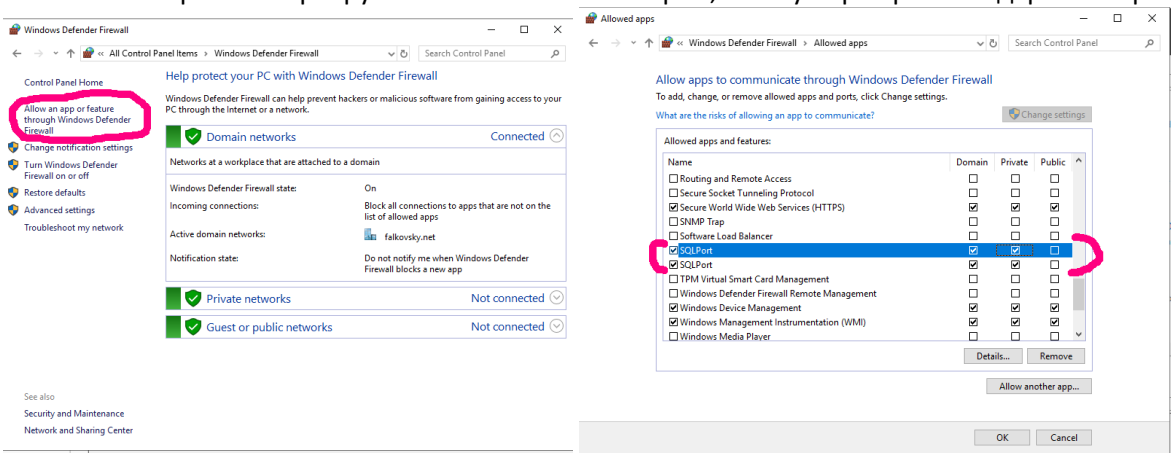


Рис. 12.17

Якщо відповідні порти після розгортання MS SQL та SQL Management Studio не відкриті, відповідні правила на Windows Defender Firewall не створено (рис. 12.17), виконуємо під Administrator Command Promt наступні команди:

netsh firewall set portopening protocol = TCP port = 1433 name = SQLPort mode = ENABLE scope = SUBNET profile = CURRENT

netsh advfirewall firewall add rule name = SQLPort dir = in protocol = tcp action = allow localport = 1433 remoteip = localsubnet profile = DOMAIN

Наступний момент. Запустивши SQL Server Configuration Manager перевіряємо роботу SQL Server Browser. Якщо служба не запущена, змінюємо її тип запуску та перестартуємо (рис.12.18).

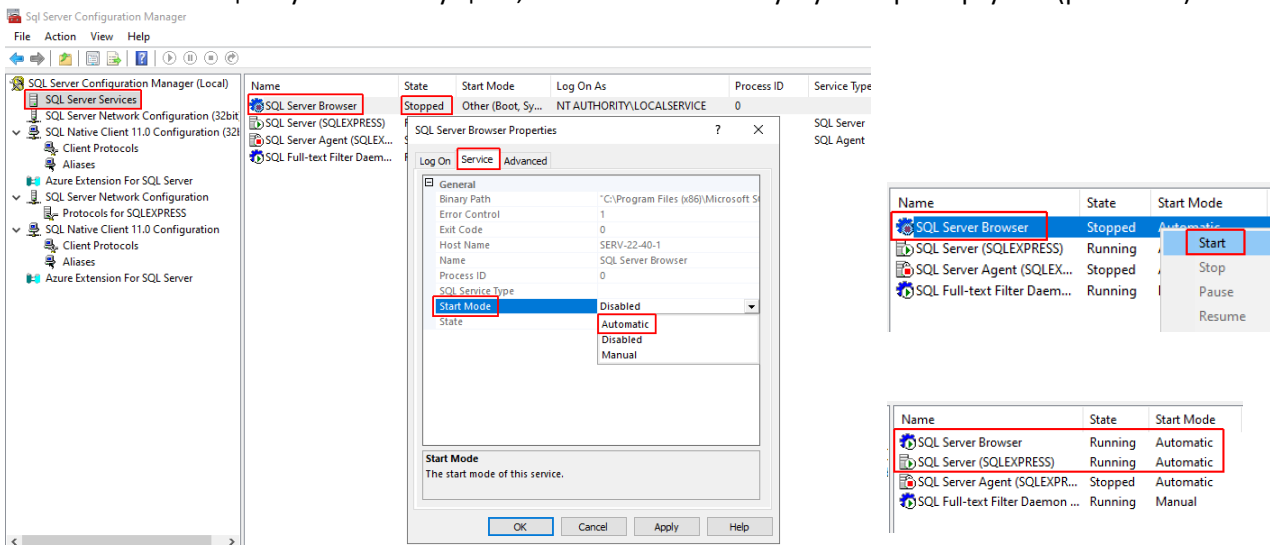


Рис. 12.18

Для використання SQL Server як бази даних веб-стека достатньо запущених служб SQL Server і SQL Server Browser, а також відкритого порту **1433** у брандмауері.

На рис. 12.19 - успішне підключення до бази даних через SQL Server Management Studio 21.

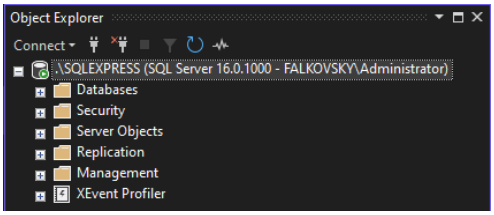


Рис. 12.19

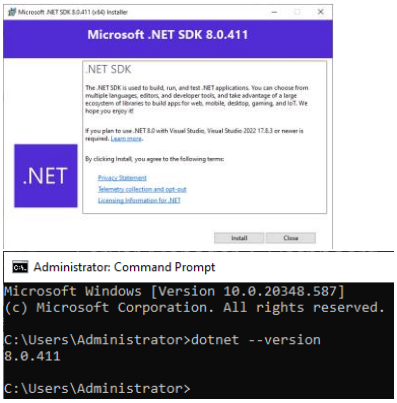
Завдання №12.2

Виконайте встановлення СУБД MS SQL 2022 Express на сервері з працюючим IIS.
При інсталяції ігноруйте попередження, що вона виконується на Computer Domain Controller.
Оберіть змішаний режим автентифікації та задайте пароль суперкористувачу SQL-сервера sa.
Виконайте встановлення MS SQL Management Studio (SSMS) та підключення до бази даних.

Встановлення .NET SDK 8

Orchard Core 2.1.7 працює на .NET 8, тому потрібен саме SDK, а не лише Runtime (SDK включає і компілятор, і Runtime). Файл інсталяції dotnet-sdk-8.0.411-win-x64.exe. На етапі підготовчих робіт на сервер були завантажені інсталяційні файли. Ви можете їх завантажити по лінкам
https://drive.google.com/file/d/1U2ifUdDA_w8NZvk3NCAJpRfPx-Lt1-sz/view?usp=drive_link
https://drive.google.com/file/d/1V-gfTO8Cin-bXSElUAJOZKZ1zOi9xN6c/view?usp=drive_link

Виконуємо встановлення та перевірку його коректності (команда ***dotnet –version***):



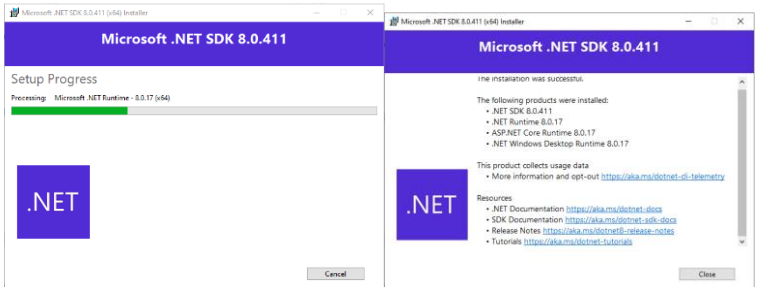


Рис. 12.20

Встановлюємо середовище виконання ASP.NET Core дозволяє запускати існуючі веб/серверні програми. У Windows рекомендовано встановити пакет хостингу, який включає підтримку середовища виконання .NET та IIS. Файл інсталяції dotnet-hosting-8.0.17-win.exe.

Створюємо новий сайт Orchard Core (швидкий старт) шляхом використання шаблону Orchard Core CMS. Це найпростіший і найшвидший спосіб старту, що дозволяє не завантажувати весь репозиторій вручну.

Відкриваємо PowerShell або CMD і виконуємо команду

dotnet new --install OrchardCore.ProjectTemplates::2.1.7

Актуальна версія шаблону Orchard Core CMS уточнюється на сайті

https://www.nuget.org/packages/OrchardCore.ProjectTemplates

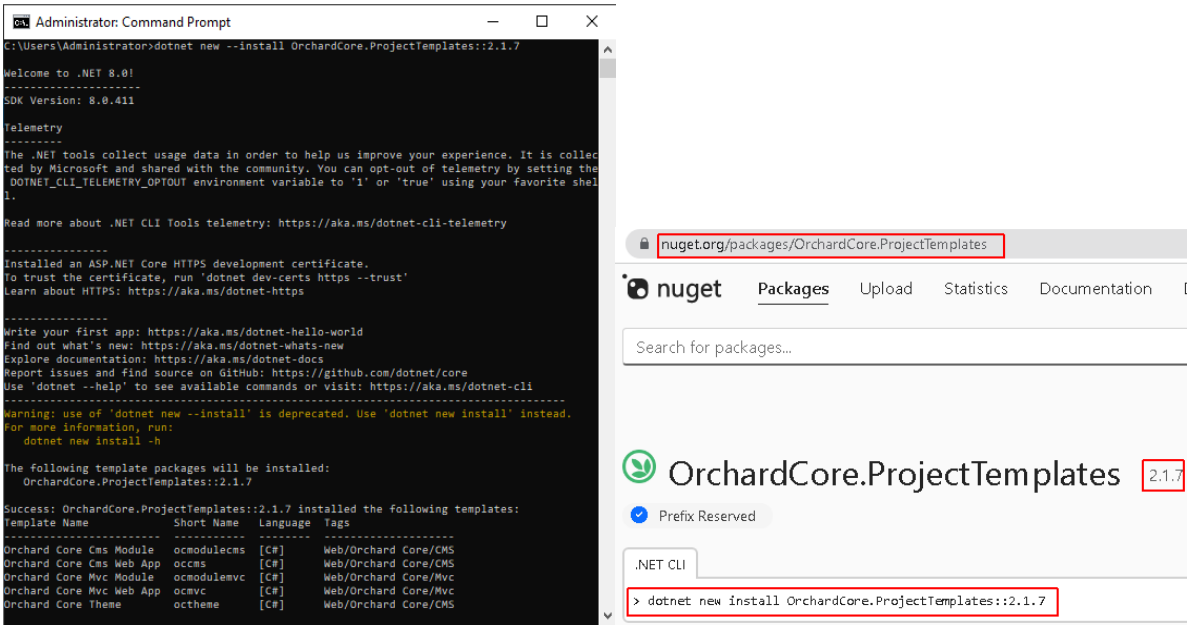


Рис. 12.21

Створюємо новий сайт за допомогою завантаженого шаблону occms. Для розробки нових сайтів за допомогою встановленого інтрументарію створимо каталог ***C:\Orchard.dev***

У PowerShell або CMD у каталозі ***C:\Orchard.dev*** виконуємо:

dotnet new occms -n Site_G_N.local
cd MyOrchardSite

де Site_G_N.local— назва проєкту сайту, згідно технічного завдання

- G – номер групи
- N - варіант

В результаті буде створено директорію C:\Orchard.dev\Site_G_N.local з усім необхідним для запуску сайту Orchard Core.

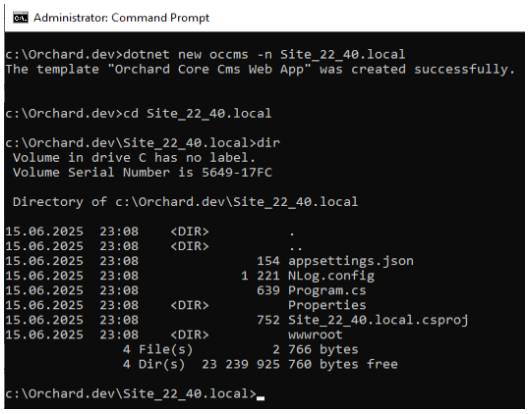


Рис. 12.22

<u>Створення бази даних</u>

Переключаємося у SQL Server Management Studio 21.x.x та створюємо порожню базу даних з довільним іменем. Наприклад Surname.db – Ваше прізвище латиницею. На рис.12.23 показане створення порожньої бази даних з іменем Falkovsky.db

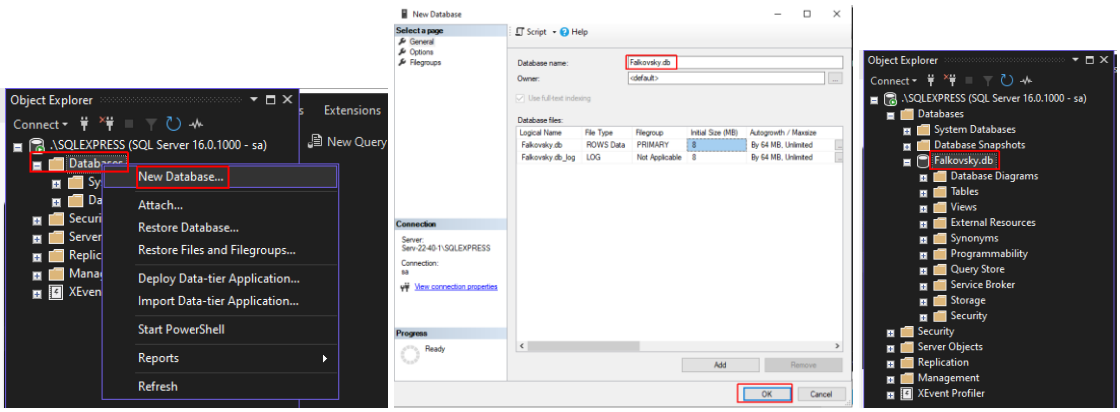


Рис. 12.23

Налаштування сайту та CMS

Переходимо до запуску на налаштування сайту. У командному рядку виконуємо

dotnet run

Якщо все добре, і на попередніх кроках не було помилок, через певний час у консолі з'явиться щось типу: ***Now listening on: http://localhost:5000***

Application started. Press Ctrl+C to shut down.

Сервер Orchard Core зараз слухає на http://localhost:5000 (HTTP) та https://localhost:5001 (HTTPS).

Щоб встановити довіру до сертифікату ASP.NET Core для сторінки https://localhost:5001 виконуємо у Power Shell з правами адміністратора команду

dotnet dev-certs https --trust

Не закриваючи вікно з командою ***dotnet run,*** відкриваємо у браузері ***https://localhost:5001***

На рис.12.24 показаний вигляд командного рядка після успішного запуску dotnet run, встановлення довіри до сертифікату та відкрита у браузері Edge сторінка localhost:5001 "Setup" сторінка Orchard Core. Вікно dotnet run у каталозі поточного сайту утримує активність сторінок сайту у розробці. У даний момент сторінки "Setup"

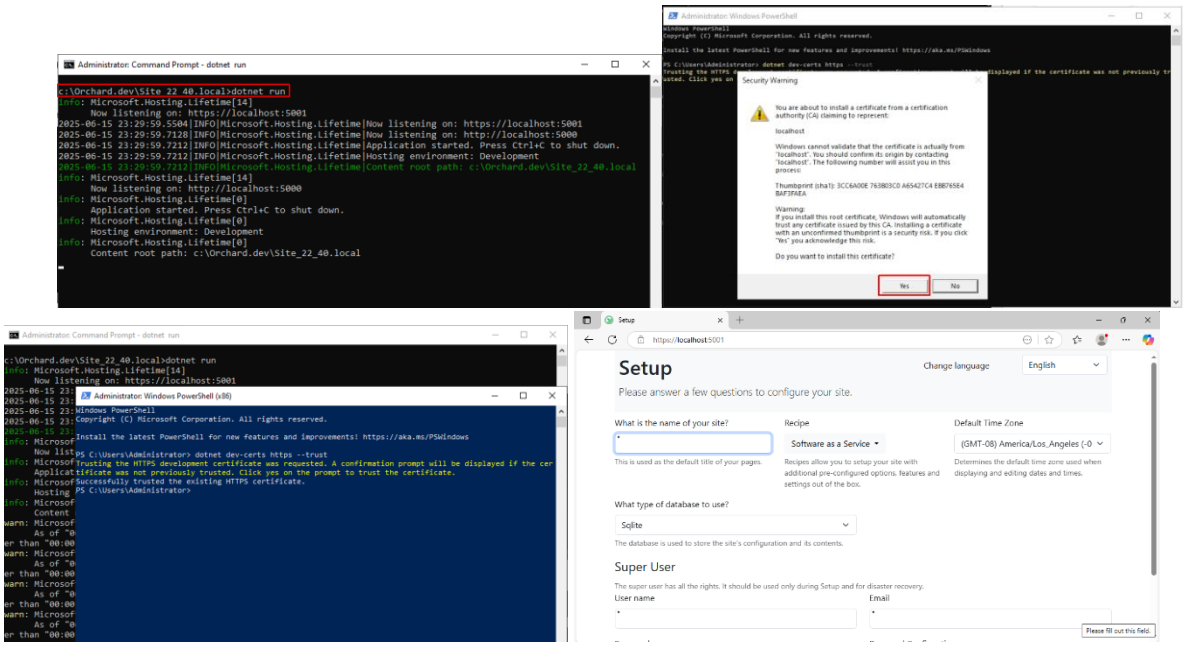


Рис. 12.24

На сторінці "Setup" Orchard Core потрібно вказати назву сайту, обрати «рецепт» (наприклад, "SaaS", "Blog", "Agency" або "Empty"), вказати тип бази даних та деякі інші параметри.

Мова сайту англійська чи українська.
Для назви сайту – використовуйте шаблон найменування

First Name Last Name – Computer Systems & Networks Administration | DevOps

Наприклад

Igor Falkovsky – Computer Systems & Networks Administration | DevOps

У якості «рецепту» обираємо “Blank Site”. Тип бази даних SQL Server
У якості Table Prefix вказуємо щось типу назви індексу orch01 чи залишаємо порожнім. Це поле використовується для підключення кількох сайтів до однієї бази даних.
Параметри підключення до SQL Express. Якщо ми використовуємо для підключення SQL Authentication, то рядок буде мати вигляд:

Server=localhost\SQLEXPRESS;Database=Surname.db;User Id=sa;Password=your_password;TrustServerCertificate=True;

Використання SQL Authentication дає просте налаштування, працює без прив'язки до Windows-облікових записів та зручне для окремих скриптів, інтеграцій, CI/CD тощо. Є і недолік – паролі у відкритому вигляді.

Якщо використовується Windows Authentication (Integrated Security), рядок прийме вигляд:

Server=localhost\SQLEXPRESS;Database=Surname.db;Integrated Security=True;TrustServerCertificate=True;

Використання Windows Authentication (Integrated Security) безпечніше за замовчуванням — немає передачі логінів/паролів у рядку підключення, воно працює з Kerberos або NTLM (залежно від налаштувань), немає пароля, який потрібно зберігати у коді, конфігах, або у веб-інтерфейсі, у Windows-системах (особливо в AD-доменах) — це рекомендований стандарт безпеки. Але є і недоліки. Може бути складніше налаштувати, якщо користувач запускає сайт від імені не того облікового запису та ускладнює розгортання на сервері, якщо IIS запускає застосунок від спеціального облікового запису

Елементи цих рядків:

- Server=localhost\SQLEXPRESS — означає локальний сервер
- Database=Surname.db — назва БД, яка була створена на етапі створення БД (рис.12.23)
- Integrated Security=True — використовується Windows-автентифікація
- TrustServerCertificate=True — необхідно для роботи через HTTPS без довіреного сертифіката SQL

У полі Table Schema можна вказати dbo, або залишити порожнім. Після створення бази даних, буде використовуватись dbo.
У полі User Name вказується ім'я користувача (логін для входу в CMS). Це може бути admin або щось унікальне. У полі Email - пошта для відновлення паролю, сповіщень тощо. Поля Password та Password Confirmation це пароль для входу до CMS

Після заповнення — натискаєте "Finish Setup" (рис.12.25)

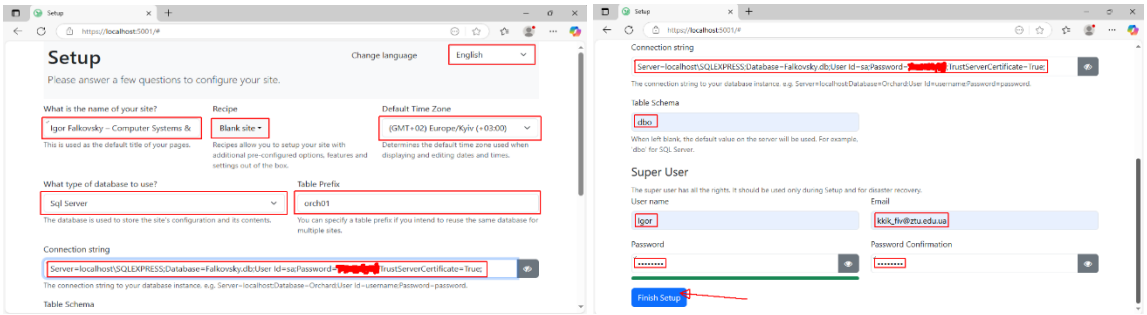


Рис. 12.25

<u>Редагування сайту.</u>

Якщо всі поля вірно заповнено, по натисканню кнопки Finish Setup, Orchard створить всі таблиці у базі даних, заповнить початкові дані та повідомить, що сторінка налаштувань не знайдена: The page could not be found.

Підключамось до панелі адміністратора по лінку http://localhost:5001/admin (використовуючи логін/пароль, який щойно створили на рис.12.25). Після успішного вводу логіну та паролю завантажується стартова сторінка CMS OrchardCore.

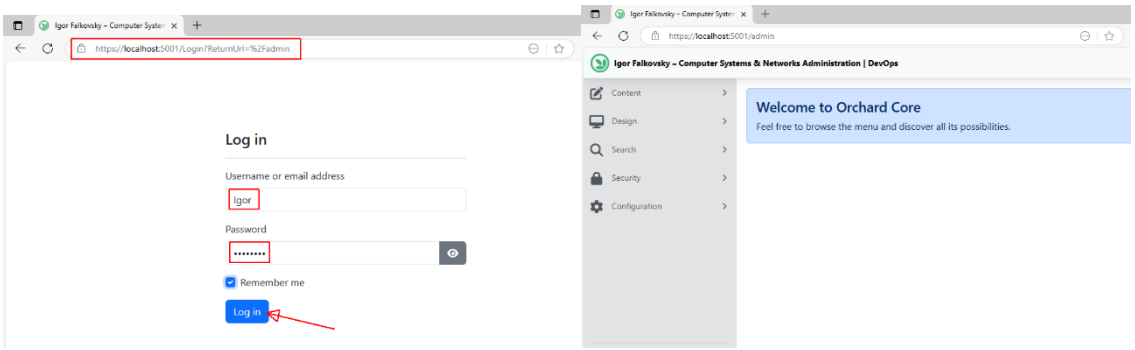


Рис. 12.26

Переходимо до адмін-панелі та приступаємо до налаштування сайту відповідно до вимог завдання. Адміністративне меню дає широкі можливості керування створеним сайтом (рис.12.27).

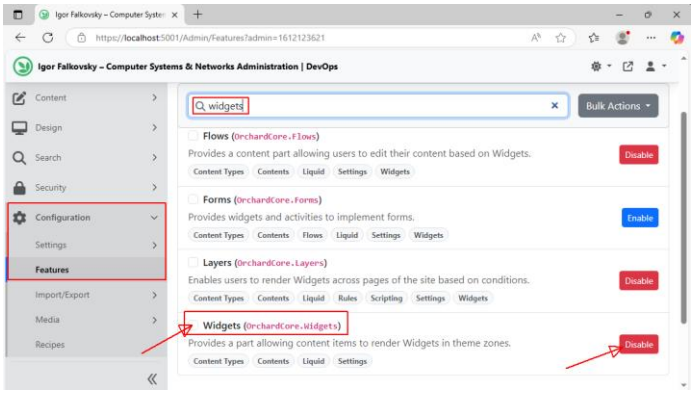


Рис. 12.27

У меню Configuration – Features знаходимо та вмикаємо функцію Widgets (якщо ще не увімкнена).

Так само перевіряємо та вмикаємо базові можливості Autoroute, Custom Settings, Layers, Html, Flow, Title, Contents, Localization.

Переходимо до меню Design – Themes, знаходимо Default Theme та застосовуємо її до поточної сторінки через кнопки Disable/Enable та Make Current. Підпис теми має бути «This is the current Site theme»

Створюємо новий тип контенту через меню Content – Content Definition – Content Type – Create New Type, заповнюємо ім'я нового типу контенту. На рис.12.28 це Page#1. Технічне ім'я заповнюється системою автоматично. Натискаємо кнопку Create і у меню Add Parts to Page#1 додаємо елементи Autoroute та Title, зберігаємо кнопкою Save.

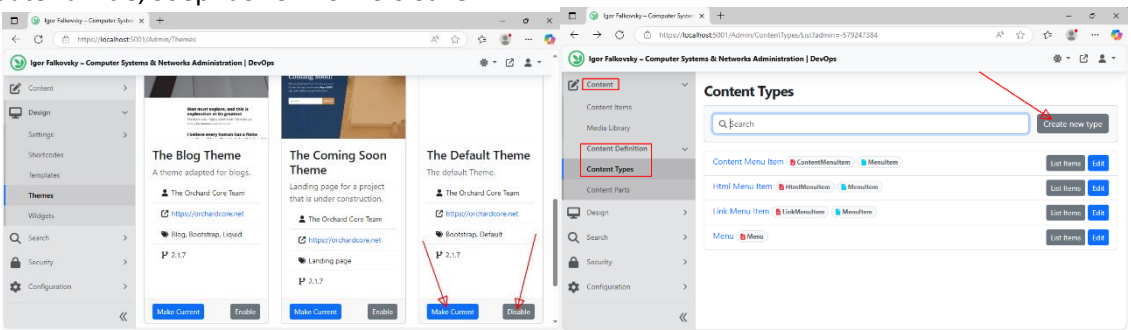


Рис.12.28

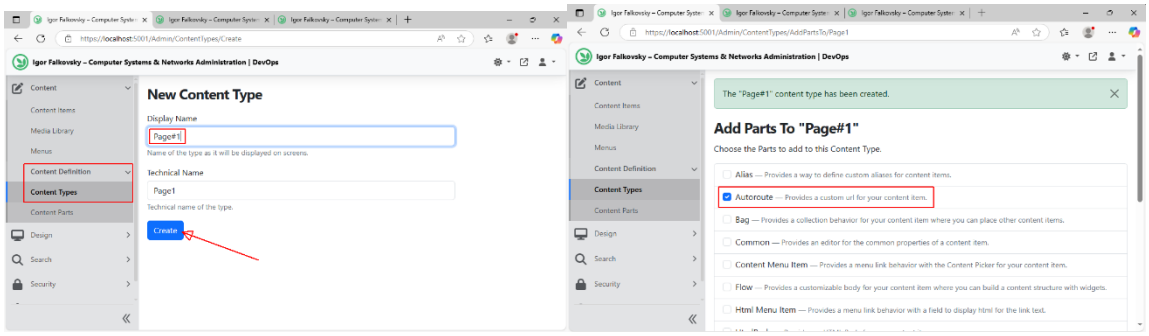


Рис.12.28 (продовження)

Заходимо у редагування елементу Autoroute та дозволяємо редагувати шлях Allow custom path, Allow Path updates та Show homepage options, зберігаємо. Отримуємо повідомлення про успішне додавання елементів та «скролимо» вікно до низу де знову зберігаємо кнопкою Save. Якщо якийсь елемент не додано, або не встановлено у необхідний режим, обираємо редагування кнопкою елементу контенту Page по кнопці Edit (рис.12.29).

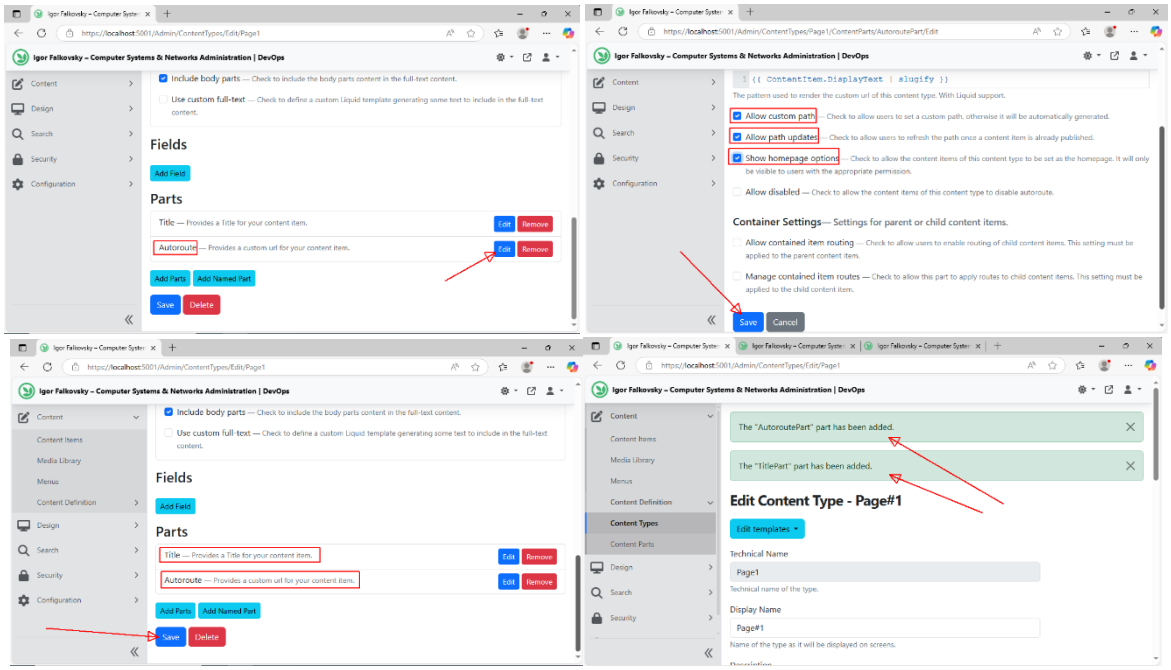


Рис. 12.29

Переходимо у меню Content – Content Items. По кнопці New Page1 викликаємо діалог заповнення нової сторінки по створеному шаблону. На сторінці три поля та два прапорці. Текстовий заголовок Title рекомендовано заповнити по шаблону:

Computer Systems & Networks Administration | DevOps | Lab#12 | Variant#N

Поле Startup – залишаємо порожнім, полю Permalink – надаємо унікальну назву латиницею у нижньому регістрі без спец символів. Наприклад aksm-lab12. Відмічаємо прапорець Set as homepage.

Публікуємо створену сторінку натисканням кнопки Publish. Сторінка з’являється у списку опублікованих і її можливо переглянути по кнопці View, що відкриває додаткову вкладку перегляду контенту (рис.12.30). Після перегляду вкладку рекомендовано закрити.

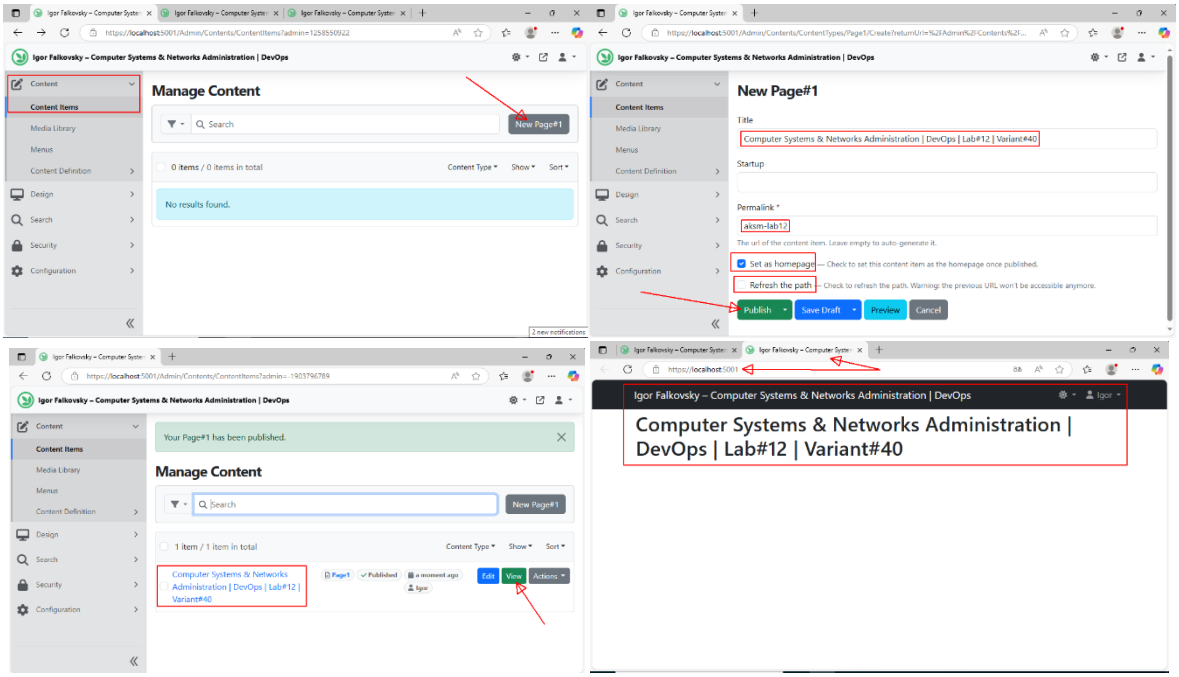


Рис. 12.30

Публікація сайту.

Вважаємо, що розробка сайту завершена і його потрібно опублікувати. За замовчуванням, для серверу IIS, сайти користувачів розташовуються в каталозі C:\inetpub\wwwroot який створює система при розгортанні Web-Server IIS. Перериваємо роботу команди

c:\Orchard.dev\Site_G_N.local>dotnet run

у вікні командного рядка серверу комбінацією клавіш Ctrl+C. Після завершення роботи dotnet у вікні з'являється повідомлення

Application is shutting down...

|INFO|Microsoft.Hosting.Lifetime|Application is shutting down...

У рядку запрошення, не змінюючи поточний каталог, виконуємо команду публікації сайту

dotnet publish "C:\Orchard.dev\Site_22_40.local" -c Release -o "C:\inetpub\wwwroot\Site_22_40.local"

C:\Orchard.dev\Site_22_40.local — це вихідний код сайту (ваш проєкт CMS Orchard Core). dotnet publish створює "збірку" сайту — готову до запуску під IIS чи як standalone app.

-o C:\inetpub\wwwroot\Site_22_40.local означає, що результат буде збережено в цій папці, де з'являться: YourProjectName.dll (основний сайт), wwwroot/ (статичні файли, CSS/JS), appsettings.json, web.config, тощо.

Виконуємо запуск сайту та перевіряємо його стан

Start-Website -Name "Site_22_40.local"

Get-Website

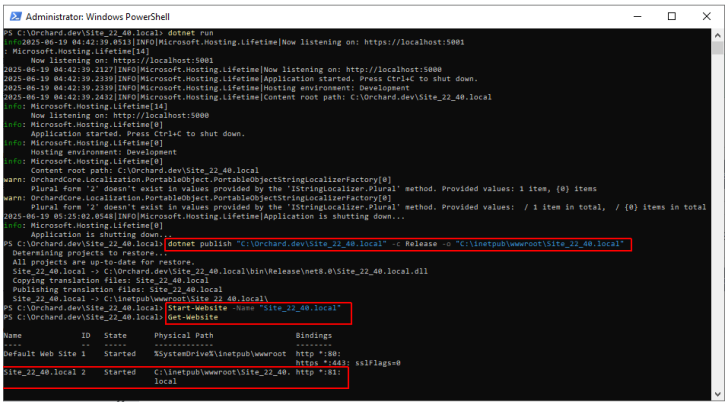


Рис. 12.31

Як показано на скріні (рис.12.31) сайт Site_22_40.local працює на порту 81

Якщо всі налаштування було виконано вірно, відображення сторінки буде аналогічним останньому скріну з рис.12.30. Якщо не відображається текст сторінки, перегляньте встановлення прапорця Set as homepage. Якщо виникають помилки обробки коду, перевстановіть середовище виконання ASP.NET Core для Windows. Файл інсталяції dotnet-hosting-8.0.17-win.exe.

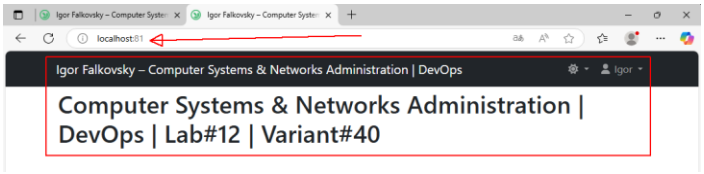


Рис. 12.32

Завдання №12.3

Розгортання Orchard Core CMS-сайту під IIS з використанням MS SQL Express

Завантажте та підготуйте веб-застосунок на базі Orchard Core CMS 2.x, який було попередньо створено у середовищі розробки (локально або на цій же віртуальній машині). Переконайтесь, що сайт коректно працює під командою dotnet run на портах :5000 та :5001. Назва сайту на сторінці стартових налаштувань CMS (Рис. 12.39) буде виводитись у заголовку головної сторінки та у метаданих:

First Name Last Name – Computer Systems & Networks Administration | DevOps

Заголовок сторінки має відповідати шаблону

Computer Systems & Networks Administration | DevOps | Lab#12 | Variant#N

За потреби активуйте необхідні модулі (Features) Orchard Core CMS через панель адміністратора (наприклад, Contents, Widgets, Html, Flow, Autoroute), створіть і опублікуйте тестову сторінку, переконавшись, що вона доступна за прямим посиланням.

Опублікуйте CMS-сайт у режимі Release за допомогою команди:

dotnet publish -c Release -o "C:\inetpub\wwwroot\Site_G_N.local"

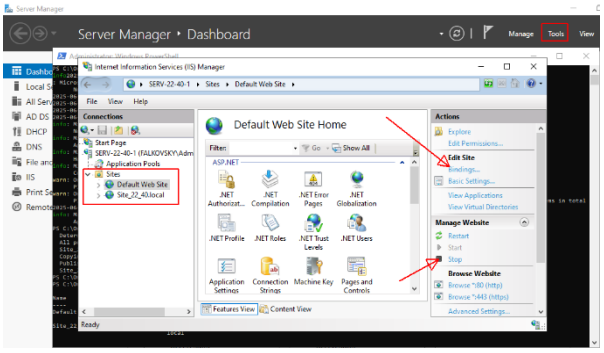
Замініть шлях на актуальний для вашого сайту. G – номер групи, N – варіант. Після публікації перевірте наявність файлу web.config у каталозі — це обов'язково для IIS.

Створіть новий вебсайт в IIS під назвою Site_Orchard.local із фізичним шляхом до опублікованого каталогу та прив'яжіть його до вільного HTTP-порту 81. Увімкніть сайт і перевірте його доступність у браузері за адресою http://localhost:81.

Налаштування автозапуску сайту як дефолтного.

Через меню Tools Server Manager заходимо до Internet Information Services (IIS) Manager. Судячи з виводу Get-Website (рис. 12.31) дефолтним сайтом з закріпленим портом 80 зараз виступає стартова сторінка IIS Manager. Опублікований сайт Site_G_N.local отримав порт 81.

Зупиняємо Default Web Site кнопкою Stop і звільнюємо порти по-замовчуванню через кнопку Binding. Виконуємо заміну HTTP 80 на 82, HTTPS 443 на 445. Алгоритм цих налаштувань показано на рис. 12.32.



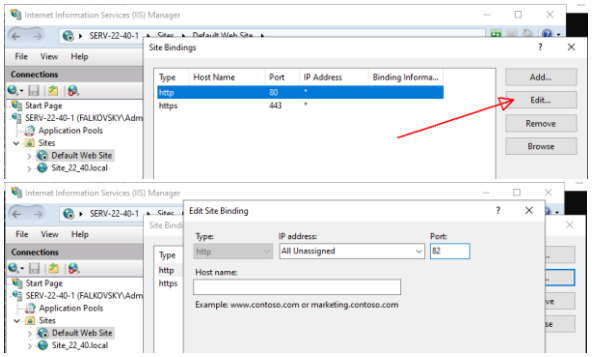


Рис. 12.33

Аналогічно виконуємо налаштування для створеного та опублікованого сайту Site-G-N.local.

Сайт має отримати HTTP ***80*** порт. Якщо для сайту налаштована підтримка HTTPS – 443 порт. У нашому конкретному випадку HTTPS не налаштовується. У IP Address залишаємо ***All Unassigned***, у якості імені хосту – повне ім'я сайту (FQDN) ***Site_G_N.local.Surname.net***

Перевіряємо стан запуску служби серверу World Wide Web Publishing Service (W3SVC). Служба має запускатись автоматично.

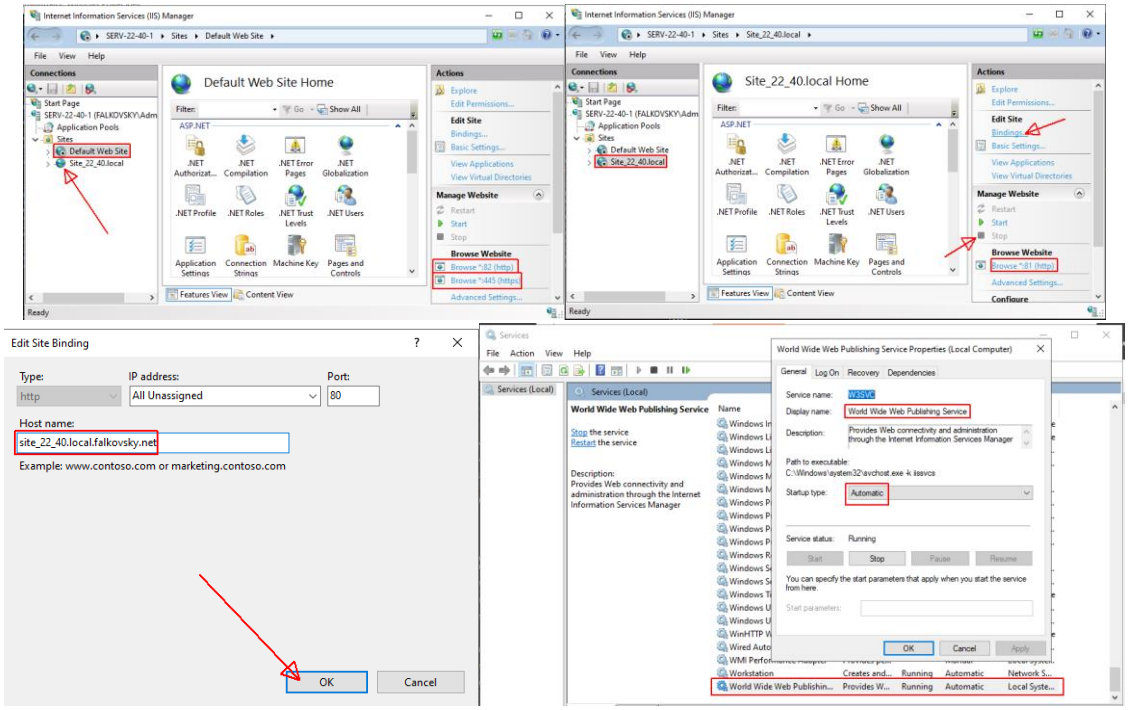


Рис. 12.34

Аналогічно лабораторній роботі №5 «Налаштування DNS-сервера на основному контролері домену Active Directory» додаємо А-запис з ім'ям сайту на DNS-сервер (рис.12.35).

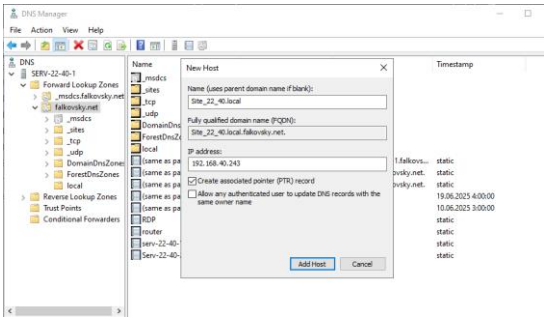


Рис. 12.35

З будь якого хосту мережі перевіряємо роботу виконаних налаштувань.

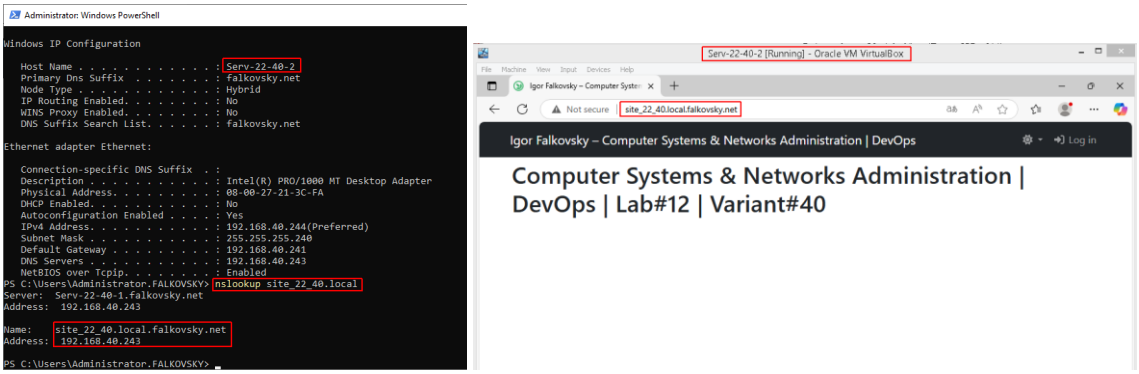


Рис. 12.36

Розгортання WEB-стеку з CMS Orchard Core, SQL Server Express та IIS успішно завершено — Ви офіційно увійшли до лав тих, хто розуміє, що відбувається за кулісами сучасного вебу. Тепер цей сайт готовий до передавання дизайнеру для наповнення, звісно, якщо й це завдання не переклали на ваші плечі.

Завдання №12.4

Вимкніть Default Web Site та замість нього використовуйте Site_G_N.local як головний сайт на порту 80.

Створіть A-запис (forward lookup) у зоні домену для Site_G_N.local з IP-адресою сервера (наприклад, 192.168.V.x).

Перевірте доступність сайту з клієнтської машини за адресою http://Site_G_N.local.local.Surname.net у браузері. За потреби додайте запис до файлу hosts або перевірте кеш DNS.

Загальні зауваження:

- Автозапуск сайту. Після перезавантаження сайту, варто перевірити, що сайт IIS налаштований на автозапуск (Start Automatically = True).
- Логування та налагодження. Orchard Core має лог-файл App_Data/logs. Його можна використовувати як джерело діагностики, якщо сайт не запускається.
- SSL/HTTPS. Поки використовується HTTP:81 — все добре, але варто пам’ятати про потенційні відмови авторизації або редиректи в Orchard при переході на HTTPS (особливо при подальшому вдосконаленні).

Корисні посилання

Configure IIS Web Server on Windows Server 2019
https://computingforgeeks.com/install-and-configure-iis-web-server-on-windows-server/

Install IIS and ASP.NET Modules
https://learn.microsoft.com/en-us/iis/application-frameworks/scenario-build-an-aspnet-website-on-iis/configuring-step-1-install-iis-and-asp-net-modules

Microsoft SQL Server. Download
https://www.microsoft.com/en-us/sql-server/sql-server-downloads

SQL Server® 2016, 2017, 2019 and 2022 Express full download
https://stackoverflow.com/questions/39835986/sql-server-2016-2017-2019-and-2022-express-full-download

Microsoft SQL Server. Вікіпедія.
https://uk.wikipedia.org/wiki/Microsoft_SQL_Server

Orchard online documentation
https://docs.orchardcore.net/en/latest/

Configure the Windows Firewall to allow SQL Server access
https://learn.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver15

Download .NET
https://dotnet.microsoft.com/en-us/download/dotnet5

Робота №13. Встановлення ОС Ubuntu Server

Мета: навчитися здійснювати встановлення ОС Ubuntu 24.04 Server з LVM розбиттям на віртуальну машину.

Інструменти: гіпервізор VirtualBox, інсталяційний образ ОС Ubuntu 24.04 Server.

Завдання до лабораторної роботи

1. Засобами гіпервізора VirtualBox створіть нову віртуальну машину.

   ※ Ім'я віртуальної машини має відповідати наступному формату:

   Srv-*G*-*N*-3

   де *G* - номер вашої групи, *N* - варіант.

   ※ Вказуючи дисковий розділ, на якому зберігатимуться файли віртуальної машини, обов'язково переконайтеся, що на обраному вами розділі достатньо вільного місця.

   ※ Обсяг оперативної пам'яті, виділений віртуальній машині, - 2 Гб (або принаймні 1,5 Гб). Віртуальний диск - 12 Гб (тип віртуального накопичувача - *динамічний*).
2. Підключіть до створеної віртуальної машини інсталяційний образ ОС Ubuntu 24.04 Server (iso-файл). Підключення виконуйте на місце віртуального оптичного приводу.
3. Виконайте встановлення ОС Ubuntu 24.04 Server на створену віртуальну машину.

   ※ Налаштування мережі, дзеркало архіву Ubuntu можна лишити за замовчуванням.

   ※ На етапі розбиття дискового накопичувача створіть окремі розділи /boot, SWAP та LVM-розбиття.

Перш ніж створювати LVM-розбиття, створіть наступні розділи:

Точка монтування	Розмір	Файлова система
/boot	500 Мб	ext4
У налаштуваннях не вказується, але потім у результуючій таблиці відображається як SWAP	2 Гб (зазвичай за обсягом RAM)	swap
У налаштуваннях не вказується	7.5 Гб (або все вільне місце, що лишилося)	Не форматувати (leave unformatted)

Після створення трьох розділів ви побачите таблицю з налаштуваннями, подібну до зображеної на рис. 13.1.

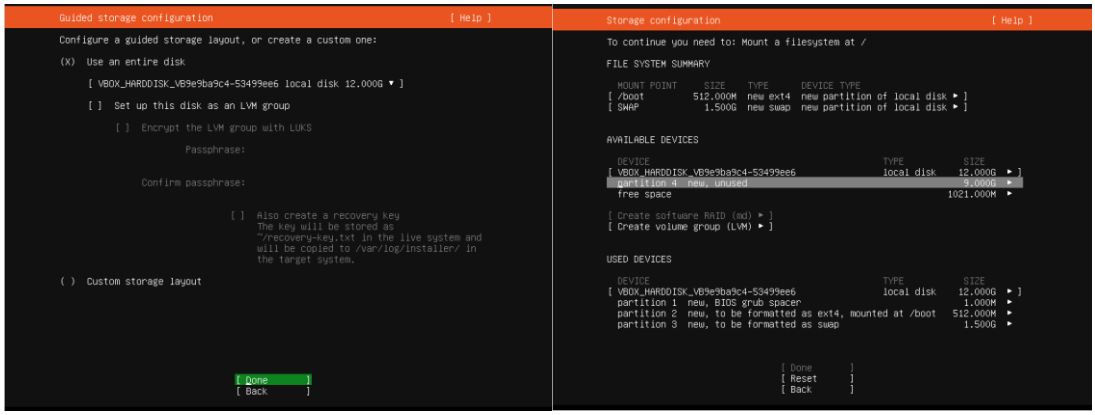


Рис. 13.1

4. У partition 4 (невідформатованому) розділі створіть LVM-розбиття (LVM volume group).

LVM (*Logical Volume Manager*) є однією з систем керування логічними томами. Для логічних томів, створених в LVM, згодом доступна низка корисних опцій, зокрема зручна зміна розмірів дискових

розділів та збереження знімків (snapshots). Також за потреби засобами LVM можна поєднати кілька дисків в один пул.

Ім’я LVM-розбиття - vg0
Пристрій - віртуальний накопичувач VBOX_HARDDISK_*ім’я_диску*, у невикористаному розбитті (partition 4).
Розмір - 8.496 Гб (весь невикористаний обсяг, значення буде вказане автоматично)
Шифрування - відсутнє

5. У межах LVM-розбиття створіть наступні логічні томи:

Ім’я	Точка монтування	Розмір	Файлова система
lv-root	/	4 Гб	ext4
lv-home	/home	2 Гб	ext4
lv-var	/var	2 Гб	ext4

Після створення трьох логічних томів в LVM-розбитті ви побачите таблицю з налаштуваннями, подібну до показаної на рис. 13.2.

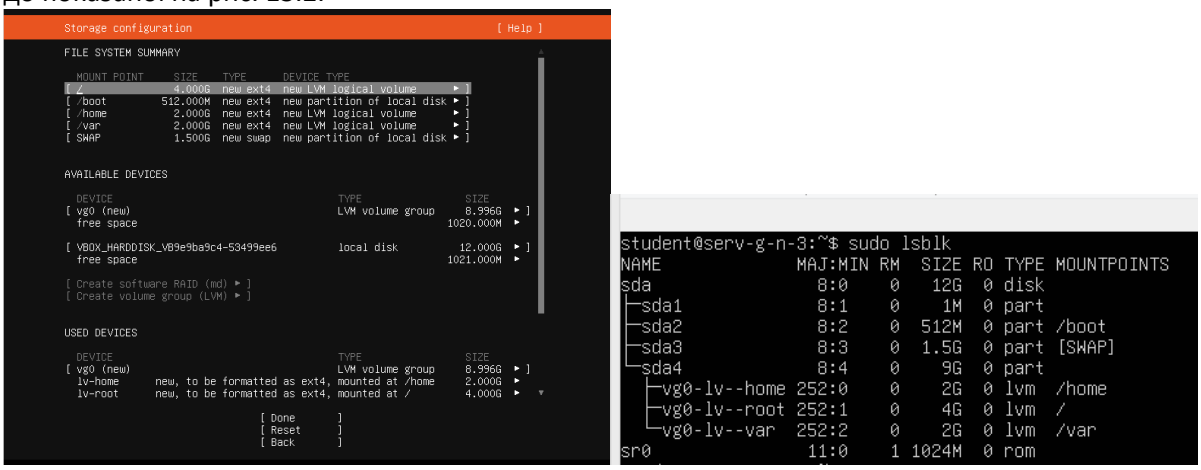


Рис. 13.2

※ Налаштування профілю:

Ваше ім’я - ваші прізвище та ім’я
Назва вашого сервера - srv-*G*-*N*-3, де *G* - номер вашої групи, *N* - варіант.
Ім’я користувача (це буде логін) - *номер-групи-номер-варіанту-з-малої-літери* Пароль - на власний розсуд

※ Встановлення серверу OpenSSH - так.

※ Встановлення додаткових snap-пакунків - ні.

6. Від’єднайте інсталяційний образ (iso-файл) від віртуального оптичного приводу віртуальної машини.

7. Після завершення встановлення переконайтеся у працездатності системи. Виведіть відомості про наявні дискові розділи (командами *fdisk* та *lsblk*) і перевірте, чи відповідають створені розділи та логічні томи тим налаштуванням, які ви робили під час встановлення системи.

Команди діагностики розділів та структури LVM у Linux
sudo fdisk -l показує розділи на фізичних дисках
sudo lsblk показує структуру блочних пристроїв

sudo lvdisplay	інформація про логічні томи
sudo vgdisplay	інформація про групи томів
sudo pvdisplay	інформація про фізичні томи (LVM)

Звіт має містити: скриншоти основних кроків виконання встановлення ОС Ubuntu 24.04 Server **Корисні посилання**

Сторінка завантаження ISO-образу Ubuntu 24.04 LTS
https://ubuntu.com/download/server

Встановлення загалом:
https://ubuntu.com/tutorials/install-ubuntu-server#1overview

Про перерозбиття під час встановлення загалом:
https://ubuntu.com/server/docs/install/storage

Покроковий посібник з встановлення Ubuntu Server 24.04 LTS:
https://blog.psantosh.com.np/step-by-step-guide-to-installing-ubuntu-server-2404-lts

Як керувати логічними томами Ubuntu Server:
https://documentation.ubuntu.com/server/how-to/storage/manage-logical-volumes/

Робота №14. Організація обміну файлами між Linux та Windows на основі протоколу SMB

Мета: організувати файловий сервер на базі Ubuntu Linux та налаштувати доступ до ресурсів цього серверу з домену Active Directory на основі протоколу SMB.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах попередніх лабораторних курсу, а також віртуальна машина з Ubuntu Server, налаштована у межах лабораторної роботи №13.

Теоретичні відомості та завдання до лабораторної роботи

ПРОТОКОЛ SMB ТА ЙОГО РЕАЛІЗАЦІЯ SAMBA

Протокол **SMB** (Server Message Block) – протокол прикладного рівня, який використовується для організації спільного доступу до файлів, принтерів, серійних портів між вузлами мережі. Протокол відомий також під більш загальною назвою **SMB/CIFS**. CIFS є старішою версією цього протоклоу і розшифровується як Common Internet File System).

SMB/CIFS найбільш активно використовувався для Windowsмереж до появи Active Directory. Згодом потокол став основою для інших реалізацій, зокрема для Samba.

Samba – стандартний набір для спільної роботи програм Windows з програмами Linux і Unix, що дає змогу здійснювати взаємну інтеграцію цих систем. Так, на основі Samba можна організовувати спільне використання Windows-системами та Unix/Linuxсистемами каталогів, принтерів. Samba підтримує інтеграцію Unix/Linux-систем в Active Directory, причому не лише як звичайних членів домену (робочих станцій чи серверів), а також за потреби і як контролерів домену.

Проект Samba є членом організації Software Freedom Conservancy, а відповідне програмне забезпечення поширюється під ліцензією GNU GPL.

Завдання №14.1

1. Запустіть віртуальну машину з Ubuntu Server, налаштовану у межах лабораторної роботи №13 та увійдіть у систему під адміністративний обліковим записом, створеним під час встановлення системи.

2. Використовуючи подані нижче теоретичні відомості, встановіть усі необхідні програмні пакунки (п. 1 теоретичних відомостей): samba, cifsutils, smbclient, sssdad, sssd-tools, realmd, adcli, winbind, libpam-winbind, libnss-winbind, krb5-config **Звіт має містити** скриншоти зроблених налаштувань та опис основних дій.

Налаштування Samba -серверу на Ubuntu

Samba дає широкі можливості для спільного доступу до файлів та інших ресурсів (наприклад, принтерів). У цій роботі буде розглянуто випадок файлового сервера з автентифікацією через Active Directory.

1. **Встановлення необхідних пакунків.** Встановимо пакунки, потрібні для функціонування Samba-серверу та його інтеграції в Active Directory. Варто інсталювати всі необхідні пакунки на цьому кроці – потім у вас може не бути доступу до Інтернету з-під цієї віртуальної машини.

```
sudo apt update
sudo apt install samba cifs-utils smbclient
sudo apt install sssd-ad sssd-tools realmd
sudo apt install adcli krb5-user
```

Під час встановлення пакунку krb5-config для параметра realm задайте значення, яке відповідає імені вашого домену. Наприклад:

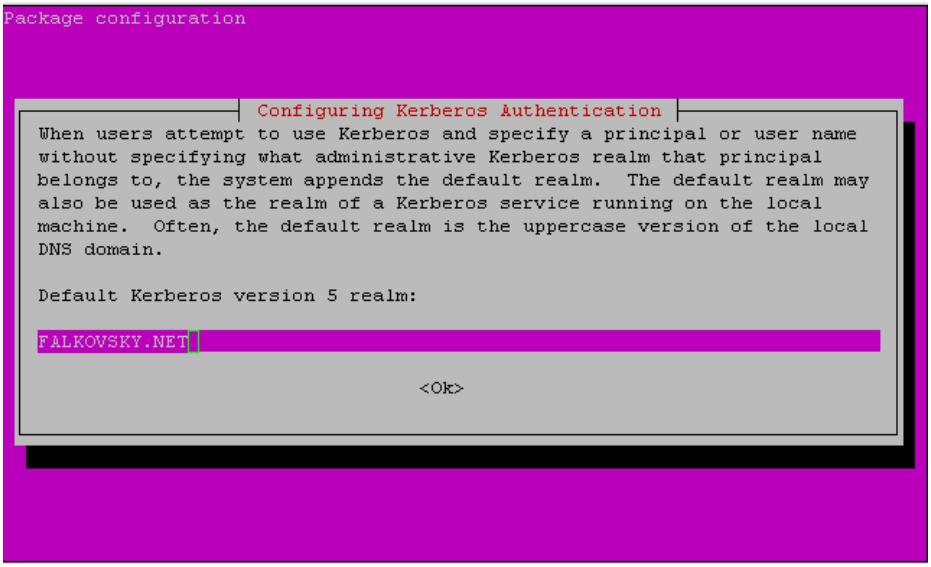


Рис. 14.1.

Для параметрів Kerberos server необхідно відредагувати конфігураційний файл Kerberos /etc/krb5.conf. За потреби можливо зробити резервну копію старого файлу:

sudo cp /etc/krb5.conf /etc/krb5.conf.bak

Відкриваємо /etc/krb5.conf у редакторі. За Вашим бажанням видаліть або закоментуйте всі записи про публічні / сторонні realm'и (MIT, CSAIL тощо), або залиште їх. У секції [realms] додаємо записи про домен surname.net. Різниця між kdc і admin_server: kdc = ... — можна вказувати кілька разів — клієнт сам обере доступний з контролерів домену, admin_server = ... — за специфікацією має бути лише один (Kerberos не підтримує автоматичне перемикання між кількома admin_server):

```
[libdefaults]
        default_realm = SURNAME.NET
        dns_lookup_realm = true
        dns_lookup_kdc = true
[realms]
 SURNAME.NET = {
  kdc = serv-G-N-1.surname.net
  kdc = serv-G-N-2.surname.net
  admin_server = serv-G-N-1.surname.net
  default_domain = surname.net
 }
```

У секції [domain_realm] налаштовуємо відображення імен доменів:

```
[domain_realm]
 .yourdomain.local = SURNAME.NET
 yourdomain.local = SURNAME.NET
```

Перезавантажуємо SSSD:

sudo systemctl restart sssd

Перевірте Kerberos-квиток:

kinit Administrator@SURNAME.NET

klist

Ви повинні побачити дійсний ticket (рис.14.2).

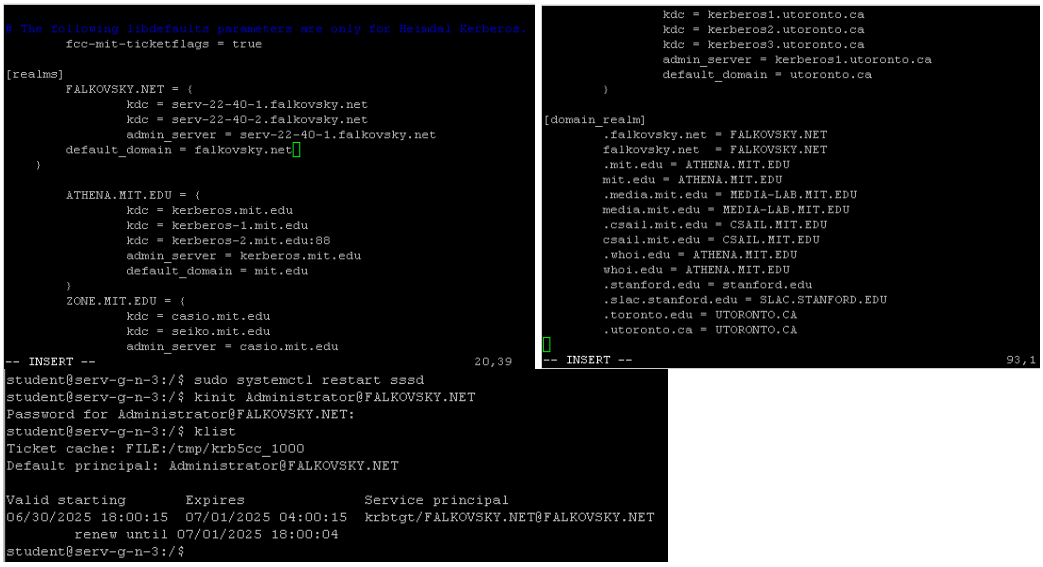


Рис.14.2.

Завдання №14.2

1. Відкорегуйте схему адресації, з якою ви працювали у лабораторній роботі №7, передбачивши статичну адресу для серверу з Ubuntu. **Змінену схему адресації додайте до звіту.**
2. Спираючись на подані нижче теоретичні відомості, змініть мережну конфігурацію серверу з Ubuntu та окремі налаштування Active Directory, щоб сервер з Ubuntu став частиною моделі мережі, з якою ви працювали у лабораторних роботах №1-13

Звіт має містити скриншоти зроблених налаштувань, опис основних дій та змінену схему адресації.

2. Виконання базових мережних налаштувань для серверу з ОС Ubuntu

2.1) **Внесення змін у схему адресації.** Виділимо серверу з ОС Ubuntu це одну статичну адресу у схемі адресації (лабораторна робота №7). У прикладі це буде адреса 192.168.40.246.

2.2) **Виключення адреси сервера з DHCP-пулу.** Цю адресу потрібно додатково виключити з DHCP-пулу на контролері домену. Для цього на контролері домену запустимо оснащення DHCP, оберіть відповідну область
DHCP та в контекстному меню вузла Address Pool виберіть New Exclusion Range (рис. 14.3).

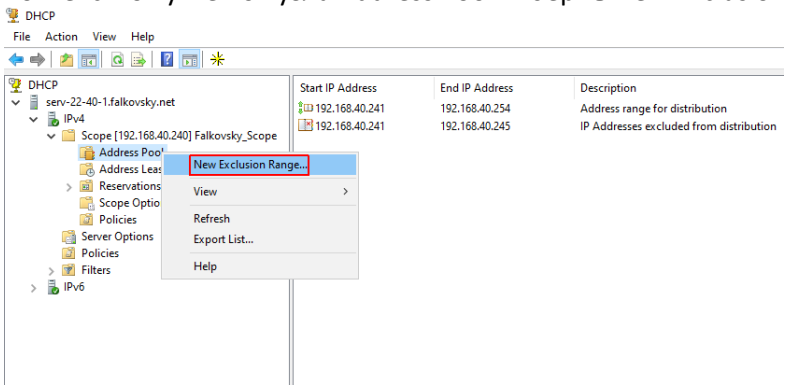


Рис.14.3.

У ролі початкової та кінцевої адреси діапазону, який необхідно виключити, введіть адресу сервера з ОС Ubuntu та натисніть Add (рис. 14.4).

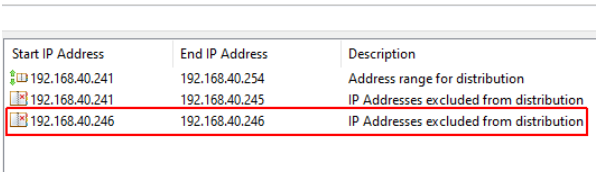


Рис. 14.4

2.3) (за потреби) **Корегування доменного імені серверу.** Для коректної роботи з доменним ім'ям Ubuntu сервера у цій лабораторній роботі переконайтеся, що довжина цього імені не перевищує 15 символів. Якщо символів в імені більше, це можна змінити, відредагувавши файл */etc/hostname* або перейменувавши сервер командою

sudo hostnamectl set-hostname New-Name-Server

Вносимо до файлу */etc/hosts* перелік хостів домену, з якими буде взаємодіяти сервер Ubuntu:

127.0.0.1 localhost

127.0.1.1 serv-G-N-3

192.168.40.246 serv-G-N-3

192.168.40.243 serv-G-N-1.surname.net

192.168.40.244 serv-G-N-2.surname.net

```
127.0.0.1       localhost
127.0.1.1       serv-22-40-3
192.168.40.246  serv-22-40-3
192.168.40.243  serv-22-40-1.falkovsky.net
192.168.40.244  serv-22-40-2.falkovsky.net
```

Рис. 14.5

Починаючи з Ubuntu 22.04+, система використовує systemd-resolved для динамічного керування DNS. Однак це може заважати інтеграції з внутрішнім Active Directory-доменом, оскільки /etc/resolv.conf постійно «скидається».

Щоб це виправити:

sudo systemctl disable systemd-resolved --now

Замінюємо символічне посилання /etc/resolv.conf:

sudo rm /etc/resolv.conf
echo "nameserver 192.168.40.243" | sudo tee /etc/resolv.conf
echo "nameserver 192.168.40.241" | sudo tee -a /etc/resolv.conf
echo "search surmane.net" | sudo tee -a /etc/resolv.conf

Це зробить файл статичним — systemd-resolved вже не перезапише його.

Перевіряємо вміст /etc/resolv.conf:

cat /etc/resolv.conf

```
student@serv-22-40-3:~$ sudo rm /etc/resolv.conf
student@serv-22-40-3:~$ echo "nameserver 192.168.40.243" | sudo tee /etc/reso
conf
nameserver 192.168.40.243
student@serv-22-40-3:~$ echo "nameserver 192.168.40.241" | sudo tee -a /etc/r
lv.conf
nameserver 192.168.40.241
student@serv-22-40-3:~$ echo "search falkovsky.net" | sudo tee -a /etc/resolv
nf
search falkovsky.net
student@serv-22-40-3:~$ cat /etc/resolv.conf
nameserver 192.168.40.243
nameserver 192.168.40.241
search falkovsky.net
student@serv-22-40-3:~$
```

Очікуваний результат - записи nameserver відповідають DNS-серверам, що використовуються у лабораторній роботі.

Перезавантажуємо сервер

sudo reboot

2.4) **Долучення ВМ з Ubuntu до моделі мережі.** Далі за допомогою віртуалізаційного ПЗ, яке ви використовуєте для моделювання мережі (GNS 3 і/або VirtualBox) приєднайте віртуальну машину з Ubuntu Server до моделі мережі, з якою ми працювали у попередніх лабораторних роботах.

2.5) **З'ясування імені віртуального інтерфейсу Ethernet.** Тепер треба дізнатися ім'я мережного інтерфейсу, який використовує мережа нашої моделі. В Ubuntu Server 20.04 мережні налаштування зазвичай здійснюються через Netplan і yaml-файли, тож для перегляду цих налаштувань можна скористатися командою ip:

ip addr show

або скорочено:

ip a

2.6) **Редагування yaml-файлів з налаштуваннями мережі.** Створюємо на сервері з ОС Ubuntu yaml-файл aksm-N.yaml (де N - варіант) у якому прописуємо мережні налаштування, включаючи обробника налаштувань (renderer: networkd), ім'я мережного інтерфейсу (типовий інтерфейс Ethernet зазвичай має ім'я enp0s3), IPадресу та префікс, шлюз за замовчуванням (ключове слово gateway4), ім'я DNSсервера (ключове слово nameservers).

Помилки у файлі Netplan можуть бути локалізовані за допомогою інструменту yamllint. Встановлення та приклад застосування:

sudo apt install yamllint
yamllint /etc/netplan/00-installer-config.yaml

Приклад yaml-файлу:

```
network:
  ethernets:
    enp0s3:
      addresses: [192.168.40.246/28]
      gateway4: 192.168.40.241
      nameservers:
        search: [falkovsky.net]
        addresses: [192.168.40.243, 192.168.40.241]
  version: 2
```

Примітка. У yaml-файлах для Netplan важливі відступи зліва. Йдеться не про кількість пробілів, а про дотримання рівневості. Так, якщо у зразку ключове слово gateway4 має такий самий відступ зліва, як ключове слово address (а не таке, як рядок – 220.19.40.246/28, наприклад) – то так само має бути і у вашому yaml-файлі.

У системі, ймовірно, є й інші yaml-файли. Наприклад, файл *50-cloud-init.yaml*. Закоментуйте рядки цього файлу і збережіть зміни, або перейменуйте його у файл з іншим розширенням. Наприклад *50-cloud-init.yaml.bkp*

2.6) **Застосування та перевірка мережних налаштувань.** Коли yaml-файли готові, застосовуємо мережні налаштування:

sudo netplan apply

Перевіряємо мережні налаштування шляхом пінгування.

2.7) **Приєднання Ubuntu Server 24.04 до домену Active Directory**. Перевіряємо доступність домену (рис.14.6).

realm discover falkovsky.net

Очікуваний результат:

type: kerberos
realm-name: FALKOVSKY.NET
domain-name: falkovsky.net
configured: no
…..

```
student@serv-22-40-3:~$ realm discover falkovsky.net
falkovsky.net
  type: kerberos
  realm-name: FALKOVSKY.NET
  domain-name: falkovsky.net
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
student@serv-22-40-3:~$
```

Рис. 14.6

Годинник Ubuntu має бути синхронізований з DC, різниця не більше ±5 хв, інакше Kerberos не спрацює. Виконуємо (на всяк випадок ☺) примусову синхронізацію часу:

sudo timedatectl set-ntp true

Приєднуємось до домену (рис.14.7):

sudo realm join --user=Administrator surname.net

Вводимо пароль користувача Administrator (або іншого облікового запису з правами додавання комп'ютерів, що використаний у цьому рядку).

Перевіряємо успішність приєднання

realm list

Очікувано побачите щось на кшталт:

falkovsky.net
type: kerberos
realm-name: FALKOVSKY.NET
domain-name: falkovsky.net
configured: kerberos-member
server-software: active-directory
client-software: sssd ...

Рис. 14.7

Як бачимо, сервер повідомляє, що для повноцінної роботи приєднання через sssd необхідні встановлені пакунки (*required-package): sssd-tools, sssd, libnss-sss, libpam-sss, adcli ma samba-common-bin*

Можемо перевірити чи вони встановлені у системі:

dpkg -l sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin

Або одразу виконати спробу встановлення. Якщо щось із них не встановлено, додасться:

sudo apt install sssd-tools sssd libnss-sss libpam-sss adcli samba-common-bin

2.8) **Перевірка наявності серверу з Ubuntu у структурі домену Active Directory**.

На контролері домену запустимо оснащення Active Directory Users and Computers та перевіримо наявність серверу Ubuntu у організаційній одиниці Computers (рис.14.8).

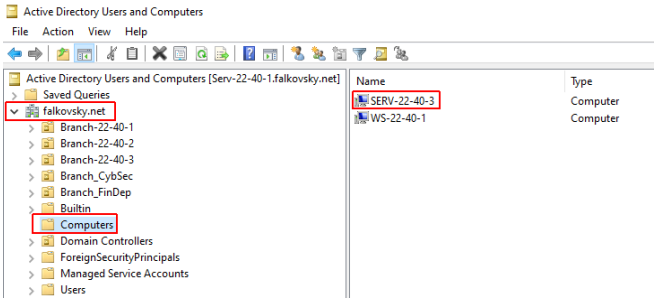


Рис. 14.8.

Якщо сервер відсутній у цій папці, виконуємо пошук у Computers домену (рис. 14.9). Сервер з Ubuntu має бути результатах пошуку.

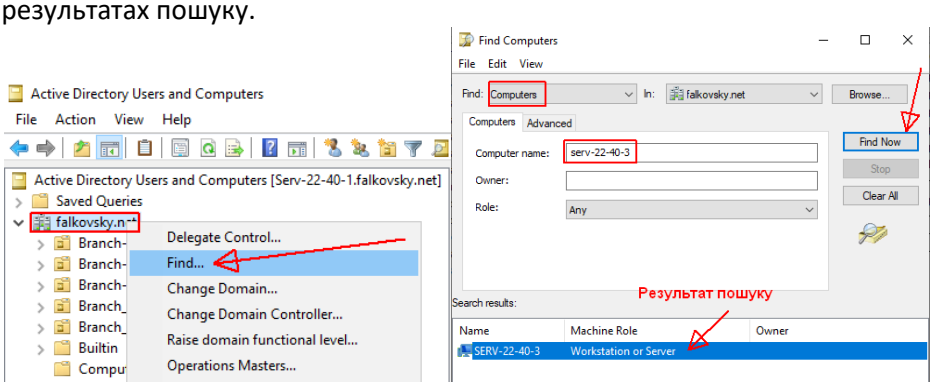


Рис. 14.9.

У властивостях серверу з Ubuntu обираємо опцію Trust this computer to delegation to any service (Kerberos only) - рис. 14.10.

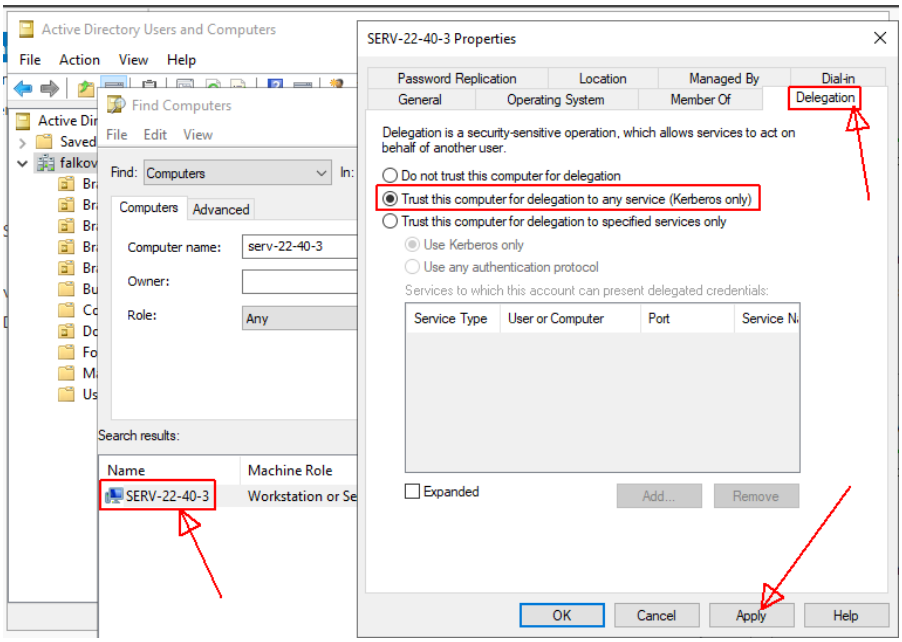


Рис. 14.10

2.8) **Створення DNS-запису для серверу з Ubuntu**. На контролері домену за допомогою оснащення DNS додайте до області прямого перегляду (Forward Lookup Zone) запис типу A для серверу з ОС Ubuntu (рис. 14.11).

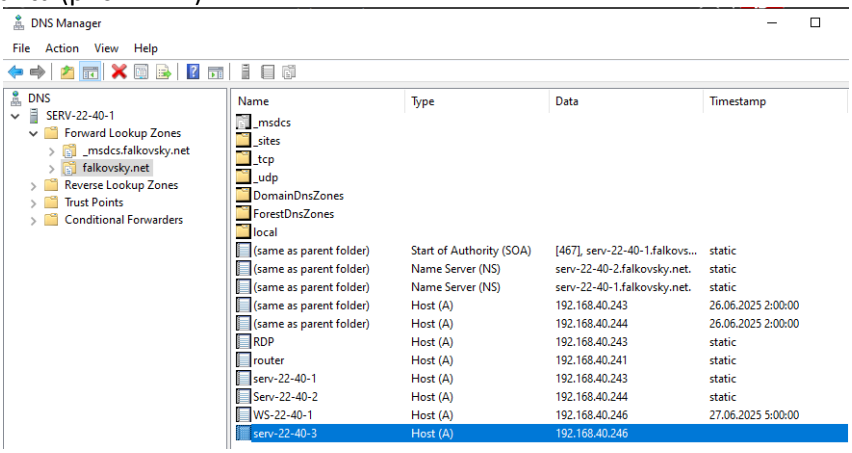


Рис. 14.11

Перевіряємо роботу Kerberos:

kinit administrator@SURNAME.NET

klist

<u>та перевіряємо як SSSD розпізнає користувачів:</u>

id administrator@surname.net

<u>спроба входу під доменним користувачем на сервері:</u>

su - 'administrator@surname.net'

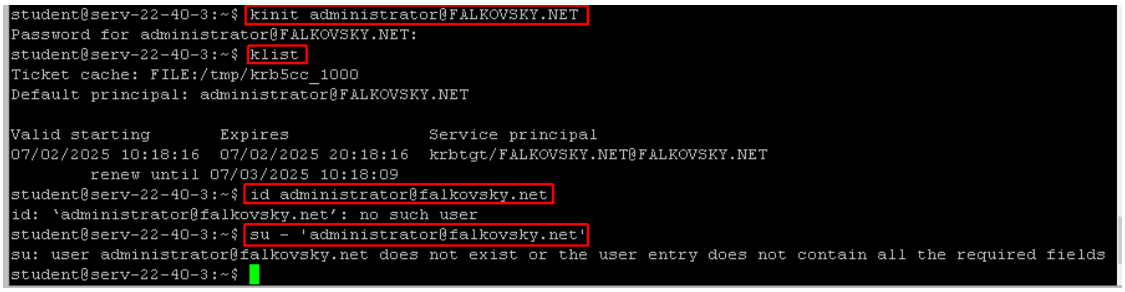


Рис. 14.12

Перевірка налаштувань на рис.14.12 показує успішно отриманий «квиток TGT» (krbtgt/FALKOVSKY.NET@FALKOVSKY.NET), а отже DNS налаштовано правильно (контролери домену знайшлися), час на сервері синхронізовано з контролерами домену (інакше Kerberos видає помилку Clock skew too great), пароль правильний, обліковий запис активний, krb5.conf налаштовано коректно (правильний realm, kdc, admin_server).

Команди id та su SSSD не надають інформацію про користувача, відповідно SSSD не відображає користувачів домену.

Перевіряємо статус SSSD (має бути active (running)

sudo systemctl status sssd

Перевіряємо */etc/sssd/sssd.conf*. У ньому має бути щось на кшталт:

[sssd]
domains = falkovsky.net
config_file_version = 2
services = nss, pam
[domain/falkovsky.net]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = FALKOVSKY.NET
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = falkovsky.net
use_fully_qualified_names = True
ldap_id_mapping = True
access_provider = ad

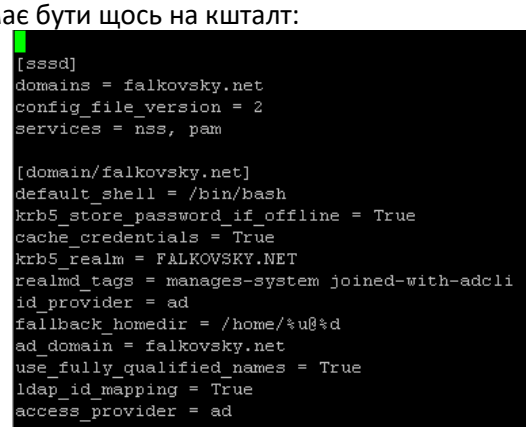


Рис. 14.13

Файл повинен мати права 600:

sudo chmod 600 /etc/sssd/sssd.conf
sudo systemctl restart sssd

Повторно перевіряємо як SSSD розпізнає користувачів:

id administrator@surname.net

та виконуємо спробу входу під доменним користувачем на сервері:

su - 'administrator@surname.net'

Команди працюють – отримана інформація про доменного користувача. Бачимо попередження, що не створено домашній каталог для користувача, хоча вхід під доменним користувачем відбувся успішно (рис.14.14):

su: warning: cannot change directory to /home/administrator@falkovsky.net: No such file or directory

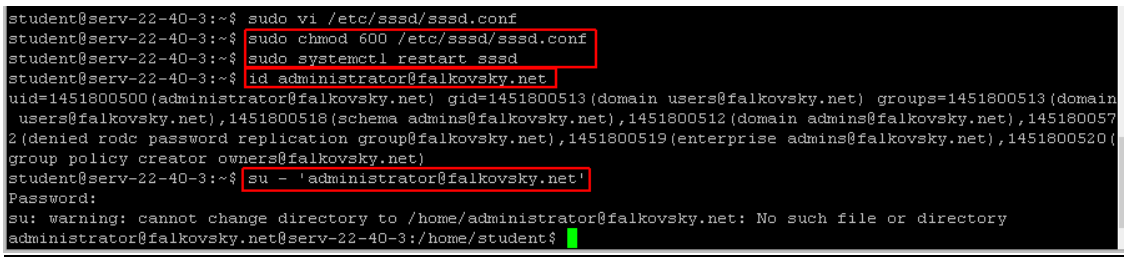
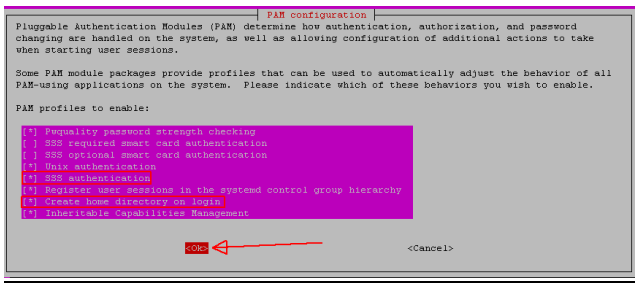


Рис. 14.14

Найпростіше рішення цієї проблеми – активація pam_mkhomedir через майстер

sudo pam-auth-update

Виходимо з сеансу доменного користувача exit. У меню, що з'явиться, необхідно відмітити [*] Create home directory on login переконатися, що також активовано [*] SSS authentication і натиснути Enter (OK)



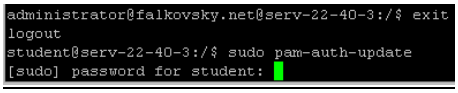


Рис. 14.15

Знову спроба входу під доменним користувачем на сервері:

su - 'administrator@surname.net'

Домашній каталог створився автоматично.

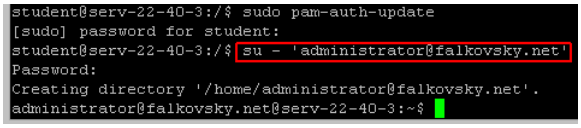


Рис. 14.16

Завдання №14.3

1. Застосовуючи теоретичні відомості, наведені нижче, налаштуйте на сервері з Ubuntu інтеграцію з доменом Active Directory.
2. Переконайтеся, що користувач домену може здійснити вхід на сервері з Ubuntu (команда sudo login). Якщо це не вдається, перевірте зроблені налаштування. Такий вхід для користувача обов'язково має виконуватися успішно.

Звіт має містити скриншоти зроблених налаштувань та опис основних дій.

3. Налаштування інтеграції з Active Directory на сервері з Ubuntu

Щоб користувачі домену Active Directory могли під'єднуватися до ресурсів серверу з ОС Ubuntu, потрібно зробити цей сервер частиною домену та дозволити на ньому вхід користувачів цього домену. В Ubuntu це реалізується на основі сервісу SSSD (System Security Services Daemon), який підтримує автентифікацію через протоколи Kerberos та LDAP. У цій роботі буде використано автентифікацію через Kerberos. Про інші доступні налаштування можна почитати, наприклад, у документації Ubuntu Server [3].

3.1) **Редагування конфігураційних файлів сервісів Samba та Name Service Switch**. Йдеться про файли */etc/samba/smb.conf*, */etc/nsswitch.conf* відповідно. Також за бажанням можна додати створення домашніх каталогів користувачів Active Directory на сервері Ubuntu.
Файл */etc/nsswitch.conf* модифікуємо так, щоб він відповідав поданому нижче зразку. Тим часом файл */etc/samba/smb.conf* доцільно створити заново. У цьому файлі міститься багато варіантів готових налаштувань для різних випадків, і на початковому етапі вони радше заважатимуть, ніж допомагатимуть.

Якщо ви не хочете видаляти початковий варіант файлу */etc/samba/smb.conf*, можна перенести його задля майбутнього використання у домашній каталог:

sudo mv /etc/samba/smb.conf ~/smb.conf.bkp

а основний конфігураційний файл – перестворити:

sudo nano /etc/samba/smb.conf

Зразки конфігураційних файлів

На всіх поданих нижче зразках позначено основні зміни. Ваші зміни у цих файлах мають відповідати даним вашого варіанту та налаштуванням вашого домену.

Вміст файлу */etc/samba/smb.conf* створено наново, у чистому файлі. Відмінності позначено на рис. 14.17.

```
[global]
   workgroup = FALKOVSKY
   realm = FALKOVSKY.NET

   security = ads
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab

   server string = Samba Server with SSSD
   log file = /var/log/samba/%m.log
   log level = 1

   # Використовуємо SSSD, а не winbind ===
   idmap config * : backend = tdb
   idmap config * : range = 3000-7999

   idmap config FALKOVSKY : backend = sss
   idmap config FALKOVSKY : range = 10000-999999

   # winbind повністю не використовується:
   winbind enum users = no
   winbind enum groups = no
   winbind use default domain = no

   # Для підтримки Kerberos-автентифікації:
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab
```

[global]
workgroup = FALKOVSKY
realm = FALKOVSKY.NET
security = ads
kerberos method = secrets and keytab
dedicated keytab file = /etc/krb5.keytab
server string = Samba Server with SSSD
log file = /var/log/samba/%m.log
log level = 1

idmap config * : backend = tdb
idmap config * : range = 3000-7999
idmap config FALKOVSKY : backend = sss
idmap config FALKOVSKY : range = 10000-999999

winbind enum users = no
winbind enum groups = no
winbind use default domain = no

kerberos method = secrets and keytab
dedicated keytab file = /etc/krb5.keytab

Рис. 14.17.

```
student@serv-22-40-3:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
        dedicated keytab file = /etc/krb5.keytab
        kerberos method = secrets and keytab
        log file = /var/log/samba/%m.log
        realm = FALKOVSKY.NET
        security = ADS
        server string = Samba Server with SSSD
        workgroup = FALKOVSKY
        idmap config falkovsky : range = 10000-999999
        idmap config falkovsky : backend = sss
        idmap config * : range = 3000-7999
        idmap config * : backend = tdb
```

Рис.14.18.

Зберігаємо файл */etc/samba/smb.conf.*

Пояснення значень рядків файлу надано у додатку 14.1 цього документу.

У кожному конкретному випадку будуть відрізнятись тільки рядки workgroup, realm та idmap config SURNAME

Виконуємо тестування поточних налаштувань командою *testparm*. Результати наведено на рис.14.18.

Файл /etc/nsswitch.conf.

Вміст цього файлу дещо відредаговано. Ключові зміни – значення рядків passwd: group: та shadow:, що тепер мають бути files sss. Вміст файлу показано на скриншоті (рис.14.19):

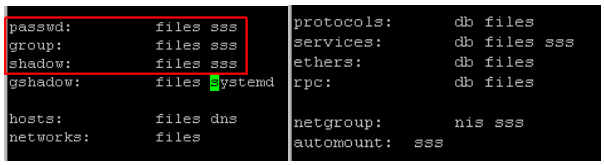


Рис.14.19.

3.2) **Перезавантаження сервісів Samba та Nmbd.**

Для застосування змін у файлі /etc/samba/smb.conf, достатньо перезапустити служби smbd та nmbd:

sudo systemctl restart smbd.service nmbd.service
sudo systemctl status smbd
sudo systemctl status nmbd

У цій конфігурації winbind не використовується, оскільки систему приєднано до домену через sssd (рис. 14.20)

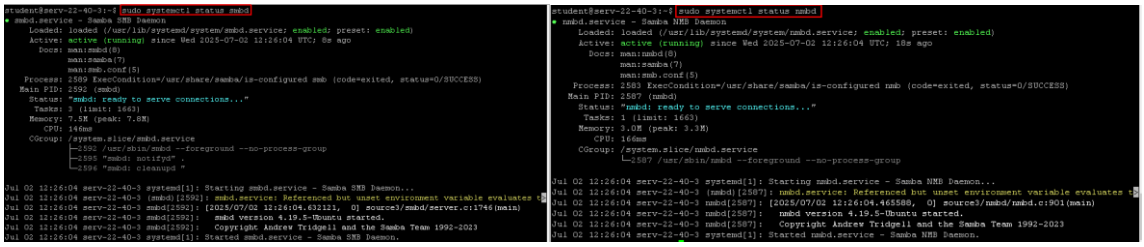


Рис. 14.20.

3.3) **Контроль доступності облікових записів домену Active Directory.** Наприклад, обліковий запис dep-rds-1 з домену falkovsky.net справді доступний на сервері Ubuntu. Також можна бачити, що цей користувач є членом двох груп користувачів домену.

Очистимо кеш SSSD та перезапустимо службу:

sudo sss_cache -E
sudo systemctl restart sssd

Перевіряємо доступ до серверу, членство у групах та входимо під доменним користувачем:

getent passwd dep-rds-1@falkovsky.net
groups dep-rds-1@falkovsky.net

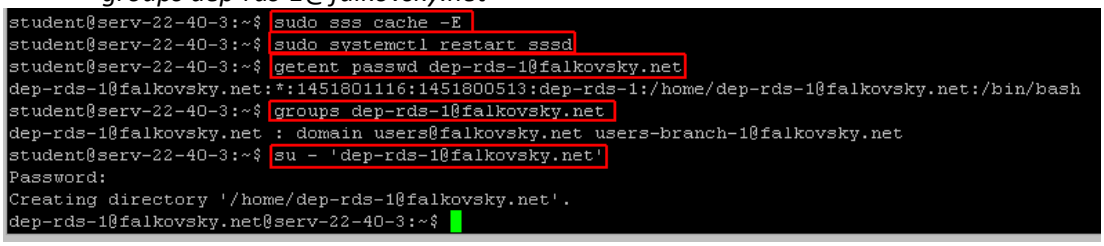


Рис. 14.21.

Увага! Цей етап перевірки (команди getent, groups, su) є критично важливим. Якщо автентифікація доменних користувачів із якихось причин не працює, то і доступ до спільних ресурсів Samba (шер, авторизація у службах тощо) також буде неможливим. Тому у разі будь-яких збоїв на цьому етапі необхідно ретельно перевірити налаштування SSSD, Kerberos, DNS та конфігураційні файли (sssd.conf, nsswitch.conf, smb.conf) перед тим, як переходити до наступних кроків.

Завдання №14.4

1. Користуючись поданими нижче інструкціями, налаштуйте на сервері з Ubuntu спільний каталог на основі Samba.

Вказівка до виконання п. 1. Коментар до спільного ресурсу (поле comment у файлі /etc/samba/smb.conf): Ubuntu File Server Share (Surname Name, Gr. GG, Var. NN), де – ваше прізвище та ім'я, GG – група, NN – варіант.

Звіт має містити скриншоти зроблених налаштувань та опис основних дій.

4. **Налаштування спільного каталогу на основі Samba.** Необхідні компоненти вже встановлено. Сервер з ОС Ubuntu вже приєднаний до домену. Лишилося підготувати майбутній спільний каталог та зробити його спільним ресурсом на основі Samba.

Повторно відкриваємо для редагування файл */etc/samba/smb.conf* і додаємо у кінці цього документа розділ *[share]* з адресою майбутнього спільного каталогу та налаштуваннями доступу до нього. Згідно з FHS (File Hierarchy Standard), для розміщення ресурсів сервера рекомендовано використовувати стандартний каталог */srv*. У каталозі */srv* створимо підкаталог *samba*, а всередині нього – підкаталог *share*:

sudo mkdir /srv/samba
sudo mkdir /srv/samba/share

Зробимо користувачем-власником каталогу системного користувача nobody, а групою-власником – системну групу nogroup:

sudo chown root:"domain users@surname.net" /srv/samba/share

Також дозволимо користувачу-власнику читання, запис і виконання, а групівласнику і решті користувачів – лише читання і виконання:

sudo chmod -R 0770 /srv/samba/share
sudo chgrp -R "domain users@surname.net" /srv/samba/share

Після виконання таких налаштувань для зміни вмісту спільного каталогу знадобляться права адміністратора, тим часом як читання вмісту каталогів та файлів буде дозволене всім користувачам, які пройшли автентифікацію. Налаштування можуть бути й іншими – залежно від потреб.

Приклад конфігураційного файлу */etc/samba/smb.conf* з доданими налаштуваннями спільного каталогу */srv/samba/share*:

```
[global]
   workgroup = FALKOVSKY
   realm = FALKOVSKY.NET
   security = ads
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab
   server string = Samba Server with SSSD
   log file = /var/log/samba/%m.log
   log level = 1
   # Використовуємо SSSD, а не winbind ===
   idmap config * : backend = tdb
   idmap config * : range = 3000-7999
   idmap config FALKOVSKY : backend = sss
   idmap config FALKOVSKY : range = 10000-999999
   # winbind повністю не використовується:
   winbind enum users = no
   winbind enum groups = no
   winbind use default domain = no
   # Для підтримки Kerberos-автентифікації:
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab

[share]
   path = /srv/samba/share
   read only = no
   browsable = yes
   guest ok = no
   valid users = @"FALKOVSKY\Domain Users"
   inherit acls = yes
   inherit permissions = yes
```

```
student@serv-22-40-3:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
        dedicated keytab file = /etc/krb5.keytab
        kerberos method = secrets and keytab
        log file = /var/log/samba/%m.log
        realm = FALKOVSKY.NET
        security = ADS
        server string = Samba Server with SSSD
        workgroup = FALKOVSKY
        idmap config falkovsky : range = 10000-999999
        idmap config falkovsky : backend = sss
        idmap config * : range = 3000-7999
        idmap config * : backend = tdb


[share]
        inherit acls = Yes
        inherit permissions = Yes
        path = /srv/samba/share
        read only = No
        valid users = "@FALKOVSKY\Domain Users"
student@serv-22-40-3:~$
```

У додатку 14.1 наведено текст цього прикладу конфігураційного файлу *smb.conf* з поясненням значень конкретних рядків.

Рис. 14.21.

Виконуємо команду тестування вірності налаштувань *testparm.* У виводі має бути "Loaded services file OK"

Перевіряємо записи krb5.keytab

sudo klist -k /etc/krb5.keytab

Очікувані записи:

host/serv-G-N-3@SURNAME.NET

cifs/serv-G-N-3@SURNAME.NET

Якщо немає cifs/..., додаємо:

sudo net ads keytab add cifs -U administrator

Рис. 14.22.

Для застосування змін у файлі /etc/samba/smb.conf, перезапускаємо служби *sssd,* smbd та nmbd:

sudo systemctl restart sssd smbd nmbd

sudo systemctl status sssd smbd nmbd

Результат цих команд має бути подібним рис.14.20.

У Samba або в більш складних файлових системах часто використовують ACL, щоб точно контролювати доступ до файлів/каталогів не лише для одного власника та групи, а для кількох конкретних користувачів або груп.

Встановлюємо пакети ACL та winbind:

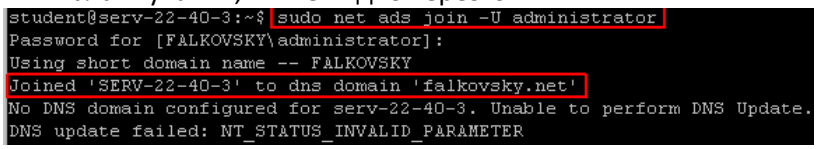
sudo apt update

sudo apt install acl

sudo apt install winbind libnss-winbind libpam-winbind

sudo getfacl /srv/samba/share

Остання команда дозволяє перевірити, хто має доступ до спільної папки, відлагодити проблеми з правами та побачити налаштування, які не видно через ls –l



Для використання winbind з Samba вимагається приєднання до AD-домену. Оскільки вже все налаштовано (SSSD, DNS, SRV записи), достатньо виконати:

sudo net ads join -U administrator

Вводимо пароль адміністратора домену.

Машина успішно приєднана до домену. Попередження DNS update failed не є критичним, DNS-записи вже внесено вручну.

Перевірка доступності домену та отримання інформації про користувача

getent passwd dep-rds-1@falkovsky.net

Перевірка Kerberos - отримання Kerberos-квитка:

sudo kinit dep-rds-1@FALKOVSKY.NET

klist

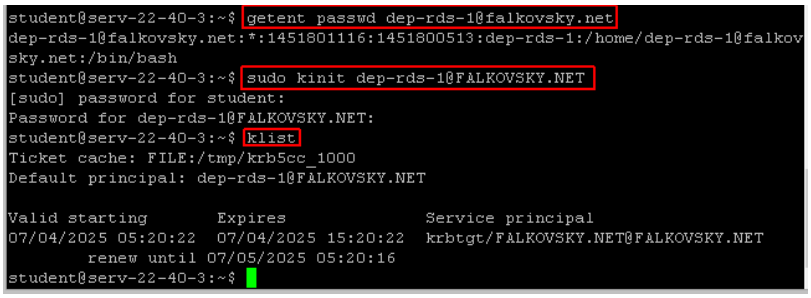


Рис. 14.23.

Знову перезапускаємо усі служби:

sudo systemctl restart sssd smbd nmbd
sudo systemctl restart winbind

winbind обов'язково потрібно запускати після sssd тоді він зможе використовувати бекенд sss для idmap.

Завдання №14.5

1. Спираючись на наведені далі теоретичні відомості, перевірте доступність спільного каталогу /srv/samba/share з довільного комп'ютера з ОС Windows, що належить до вашого домену. У випадку використання контролера домену в якості довільного комп'ютера з ОС Windows для доступу до Samba-ресурсу може знадобитись виконання дій, описаних у додатку 14.2.

Вказівка до виконання п. 1. Імена тестових файлу та каталогу має містити дані про вас: test-dir-ваші-ініціали та test-file-ваші-ініціали.txt **Звіт має містити** скриншоти зроблених налаштувань, опис основних дій.

5. **Перевірка доступу до спільного каталогу на основі Samba.** Аби переконатися, що спільний каталог працює як належне, створимо на сервері Ubuntu у каталозі /srv/samba/share тестові каталог та файл із довільним вмістом.

Створюємо тестовий каталог та тестовий файлу з вмістом:

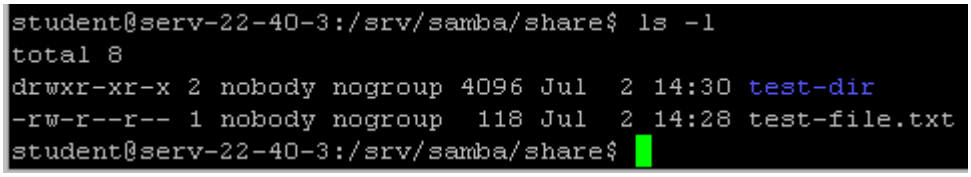
sudo mkdir /srv/samba/share/test-dir

echo "Congratulations!
If you are reading this from a Windows machine, the Samba layer you purchased is working correctly!" | sudo tee /srv/samba/share/test-file.txt

Права повинні відповідати основним налаштуванням спільного каталогу:

sudo chown -R nobody:nogroup /srv/samba/share/test-dir /srv/samba/share/test-file.txt
sudo chmod 0755 /srv/samba/share/test-dir
sudo chmod 0644 /srv/samba/share/test-file.txt

Файл та каталог:



Вміст файлу test-file.txt:

Congratulations!
If you are reading this from a Windows machine, the Samba layer you purchased is working correctly!

```
student@serv-22-40-3:/srv/samba/share$ cat test-file.txt
Congratulations!
If you are reading this from a Windows machine, the Samba layer you purchased is working correctly!
```

Тепер необхідно внести зміни у системний реєстр на комп'ютері домену, з якого планується підключатися до спільного ресурсу на сервері Linux. Заходимо по гілці системного реєстру:

\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows

Шукаємо розділ реєстру **LanmanWorkstation**

Якщо він відсутній, його потрібно його створити.

У розділі **LanmanWorkstation** створюємо запис типу **DWORD 32** bit з назвою **AllowInsecureGuestAuth** та присвоюємо йому значення 1, як на рис.14.24.

Тепер на комп'ютері домену, де ми налаштували дозвіл **LanmanWorkstation**, запустимо Провідник і введемо в адресному рядку адресу серверу з Ubuntu:

\\serv-G-N-3\share

або

\\192.168.40.246\share

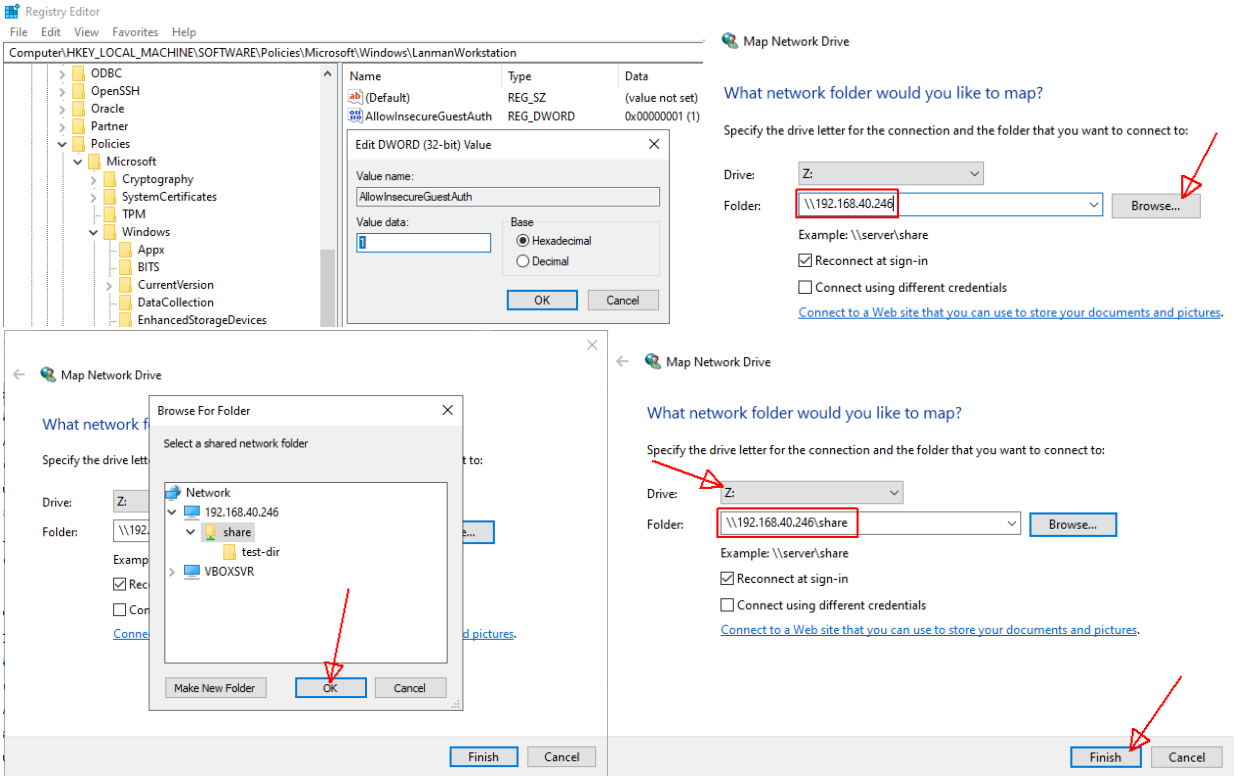


Рис.14.24.

Якщо все було зроблено правильно, має відобразитися спільний каталог (у нашому випадку share), і його вміст повинен бути доступним користувачу для читання.

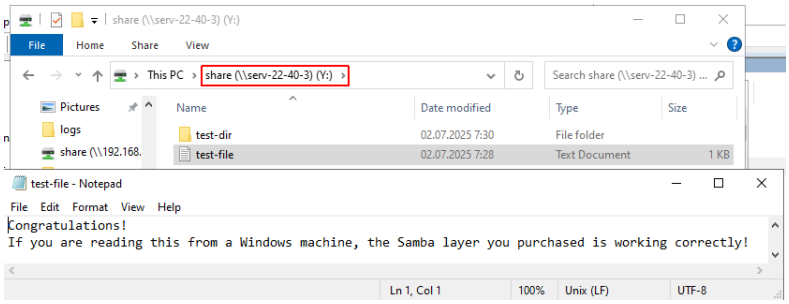


Рис.14.25.

Те ж саме можливо виконати за допомогою командного рядка net use (рис.14.26):

*net use * \\HostNameorIP\share /user:Surname\user-Login **

На рис. 14.26. показане підключення Samba-ресурсу для користувача домену Falkovsky.net dep-rds-1. У першому випадку доступ до Samba-серверу виконується по IP-адресі, у другому – по імені серверу.

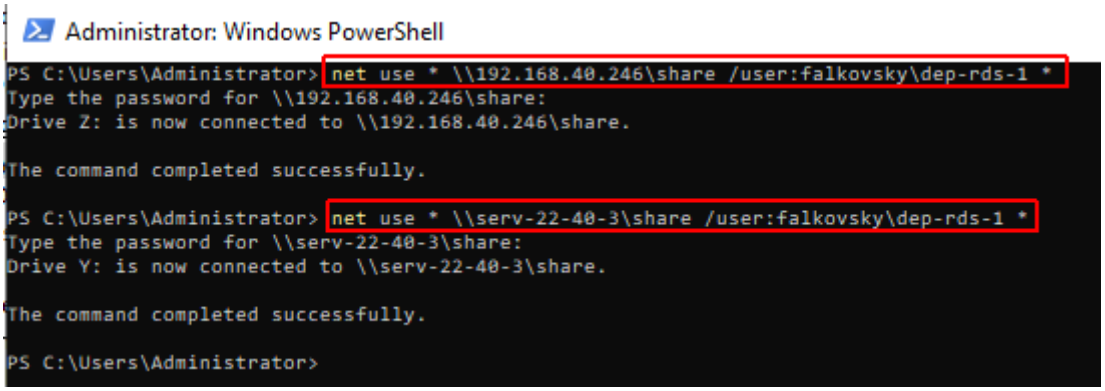


Рис.14.26.

Текст команд:

*net use * \\192.168.40.246\share /user:falkovsky\dep-rds-1 **

*net use * \\serv-22-40-3\share /user:falkovsky\dep-rds-1 **

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 14.1-14.5.

Додаток 14.1.

Пояснення рядків у секціях [global] та [share] конфігураційного файлу /etc/samba/smb.conf

[global] — загальні налаштування сервера

Параметр	Значення	Пояснення
workgroup = SURNAME	NetBIOS-домен	Ім’я робочої групи (NetBIOS). Має відповідати імені домену без суфіксу .NET.
realm = SURNAME.NET	DNS-домен	Повне ім’я Kerberos-домену (REALM), обов’язково у ВЕРХНЬОМУ регістрі.
security = ads	тип автентифікації	Вказує, що сервер є **членом Active Directory-домену**, і використовує AD для автентифікації.
kerberos method = secrets and keytab	спосіб Kerberos	Samba використовує /etc/krb5.keytab для Kerberos-токенів.
dedicated keytab file = /etc/krb5.keytab	шлях до keytab	Вказує Samba, який keytab-файл використовувати.
server string = Samba Server with SSSD	опис сервера	Інформація, що відображається клієнтам у мережі (необов’язково).
log file = /var/log/samba/%m.log	лог-файли	Індивідуальні логи для кожного клієнта (%m — NetBIOS-ім’я клієнта).
log level = 1	рівень логування	Мінімальний рівень логів. Вищі значення — докладніші, але створюють більше шуму.
idmap config * : backend = tdb	резервна база	Мапінг SID↔UID для невідомих доменів (локальний TDB).
idmap config * : range = 3000-7999	діапазон UID	UID/GID для облікових записів **не з домену FALKOVSKY**.
idmap config SURNAME : backend = sss	основний бекенд	Вказує, що Samba повинна брати мапінг із **SSSD**.
idmap config SURNAME : range = 10000-999999	діапазон UID	UID/GID для облікових записів з домену FALKOVSKY.
winbind enum users = no	не перелічувати	Забороняє Samba автоматично перераховувати користувачів через winbind.
winbind enum groups = no	не перелічувати	Те саме для груп.
winbind use default domain = no	без скорочень	Не обрізає доменне ім’я при вході (тобто потрібно user@domain).
passwd backend = sss	бекенд паролів	(Опціональний параметр) каже Samba звертатися до SSSD при перевірці паролів.

[share] — налаштування ресурсу

Параметр	Значення	Пояснення
path = /srv/samba/share	шлях до каталогу	Фізичне розташування расшареного ресурсу.
read only = no	запис дозволено	Користувачі можуть писати.
browsable = yes	видимий	Каталог видно в мережевому оточенні.
guest ok = no	без гостей	Доступ лише для авторизованих користувачів.
valid users = @"SURNAME\Domain Users"	хто має доступ	Доступ лише для членів групи **Domain Users**. Вказано у Windows-форматі (із лапками та зворотними слешами).
inherit acls = yes	наслідування ACL	Нові файли наслідують ACL від батьківського каталогу.
inherit permissions = yes	наслідування прав	Нові файли успадковують права rwx/rw- тощо від каталогу.

Додаток 14.2.

Налаштування доступу до Samba-ресурсу з Windows Server 2022 (роль: DC)

Відкрийте локальну політику безпеки secpol.msc. У дереві зліва перейдіть до:

Local Policies - Security Options

Змініть такі параметри:

Network access: Let Everyone permissions apply to anonymous users → Enabled

Network access: Do not allow anonymous enumeration of SAM accounts → Disabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares → Disabled

Ці параметри дозволяють гостьовим або анонімним обліковим записам взаємодіяти з ресурсами Samba, що особливо важливо при використанні спільних папок з guest ok = yes.

Перевірте групові політики. Введіть gpedit.msc, перейдіть до:

Computer Configuration - Administrative Templates - Network - Lanman Workstation

Установіть

Enable insecure guest logons → Enabled

Цей параметр дозволяє Windows підключатися до SMB-ресурсів, які не потребують автентифікації (тобто гостьовий доступ), що за замовчуванням заборонено в нових версіях Windows через міркування безпеки.

Після змін перезапустіть політики командою:

gpupdate /force

Або перезавантажте сервер для гарантованого застосування налаштувань.

Перевірте доступ до Samba-ресурсу, наприклад через Провідник Windows або команду net use.

Рекомендовані джерела

🎧 Network – Configuration – Ubuntu. URL: https://ubuntu.com/server/docs/network-configuration

🎧 Samba – File Server – Ubuntu. URL: https://ubuntu.com/tutorials/install-and-configure-samba#1-overview

🎧 Service – SSSD – Ubuntu. URL: https://documentation.ubuntu.com/server/how-to/sssd/with-active-directory/

🎧 Samba – Active Directory – Ubuntu. URL: https://ubuntu.com/server/docs/samba-active-directory

Список рекомендованих джерел

1. Active Directory Delegation Tutorial for Beginners. URL: https://corewin.ua/blog/active-directory-delegation-tutorial-for-beginners/
2. ActiveDirectory Module - Microsoft Docs. URL: https://docs.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2019-ps
3. Configure IIS Web Server on Windows Server 2019. URL: https://computingforgeeks.com/install-and-configure-iis-web-server-on-windows-server/
4. Configure the Windows Firewall to allow SQL Server access. URL: https://learn.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver15
5. Enable or Disable Disk Quotas in Windows. Tutorials. URL: https://www.tenforums.com/tutorials/99888-enable-disable-disk-quotas-windows.html
6. File Server Resource Manager (Part 1: Install FRSM - Part 7: File Management Tasks). URL: https://4sysops.com/archives/file-server-resource-manager-fsrm-part-3-quota-management/
7. G. Held. Windows Networking Tools: The Complete Guide to Management, Troubleshooting, and Security. CRC Press, 2013
8. How to Manage Logical Volumes. Ubuntu Server. URL: https://documentation.ubuntu.com/server/how-to/storage/manage-logical-volumes/
9. Install IIS and ASP.NET Modules. URL: https://learn.microsoft.com/en-us/iis/application-frameworks/scenario-build-an-aspnet-website-on-iis/configuring-step-1-install-iis-and-asp-net-modules
10. M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020.
11. Managing Disk Quotas. URL: https://learn.microsoft.com/en-us/windows/win32/fileio/managing-disk-quotas
12. Microsoft Evaluation Center. URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022
13. Module PowerShell GetCimInstance. URL: https://learn.microsoft.com/en-us/powershell/module/cimcmdlets/get-ciminstance?view=powershell-7.3
14. Network – Configuration – Ubuntu. URL: https://ubuntu.com/server/docs/network-configuration
15. O. Thomas. Windows Server 2016 Inside Out. Pearson Education, 2017.
16. Orchard online documentation. URL: https://docs.orchardcore.net/en/latest/
17. PowerShell File Server Resource Manager. URL: https://learn.microsoft.com/en-us/powershell/module/fileserverresourcemanager/?view=windowsserver2022-ps&redirectedfrom=MSDN&viewFallbackFrom=winserverr2-ps
18. Samba – Active Directory – Ubuntu. URL: https://ubuntu.com/server/docs/samba-active-directory
19. Samba – File Server – Ubuntu. URL: https://ubuntu.com/tutorials/install-and-configure-samba#1-overview
20. Service – SSSD – Ubuntu. URL: https://documentation.ubuntu.com/server/how-to/sssd/with-active-directory/

Навчально-методичне видання

АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Підготували
Головня Олена Сергіївна,
Фальковський Ігор Геннадійович

Комп'ютерний дизайн та верстка:
Головня О. С., Фальковський І. Г.

Державний університет «Житомирська політехніка»
вул. Чуднівська, 103, м. Житомир, 10005