Лабораторна робота №11

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 №3-10.

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. 11.1).

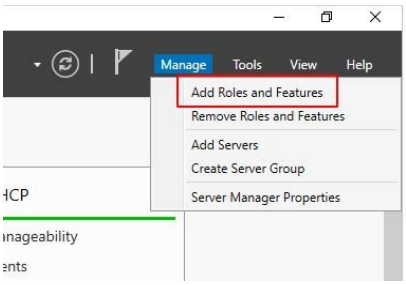


Рис. 11.1

Цього разу знадобиться вибрати другий пункт - *Remote Desktop Services Installation* (рис. 11.2). Надалі він дозволяє налаштувати служби віддаленого робочого столу як на основі сесій віддаленого робочого столу, так і на основі віртуальних машин.

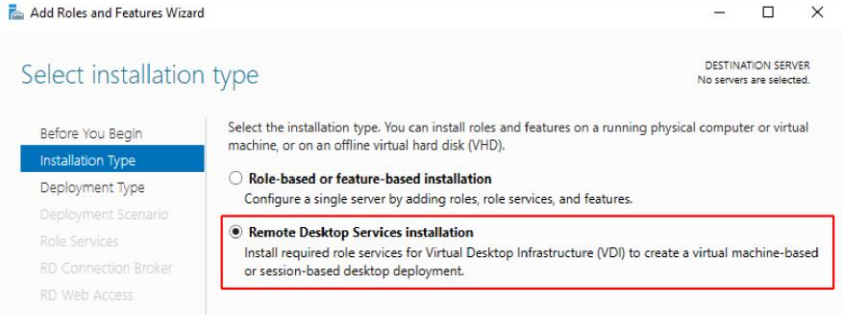


Рис. 11.2

Далі обираємо опцію стандартного розгортання (рис. 11.3).

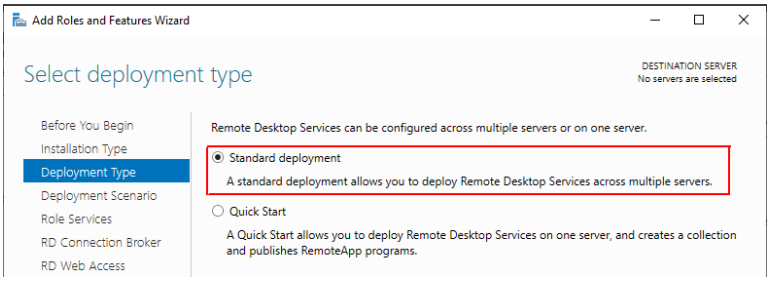


Рис. 11.3

На наступному етапі пропонується обрати сценарій розгортання. Обираємо служби віддаленого столу на основі віддалених сесій – *session-based desktop deployment* (рис. 11.4). Цей сценарій потребує значно менше ресурсів для роботи, що є визначальним фактором для нашої навчальної моделі мережі.

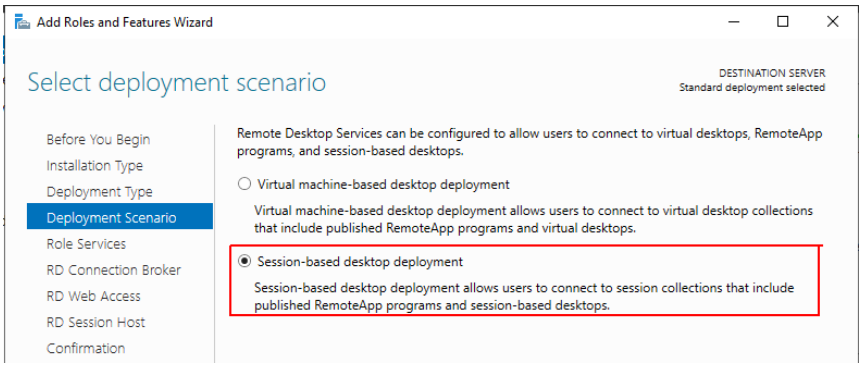


Рис. 11.4

Далі у вікні майстра виводиться перелік служб, які буде встановлено на наступних кроках (рис. 11.5). Ознайомтеся з переліком і натисніть *Next*.

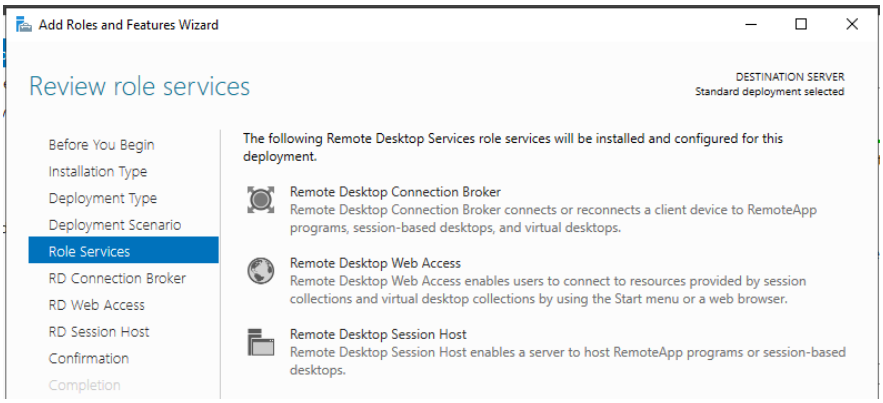


Рис. 11.5

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. 11.6 цей сервер обрано для встановлення RD
Connection Broker (рис. 11.6).

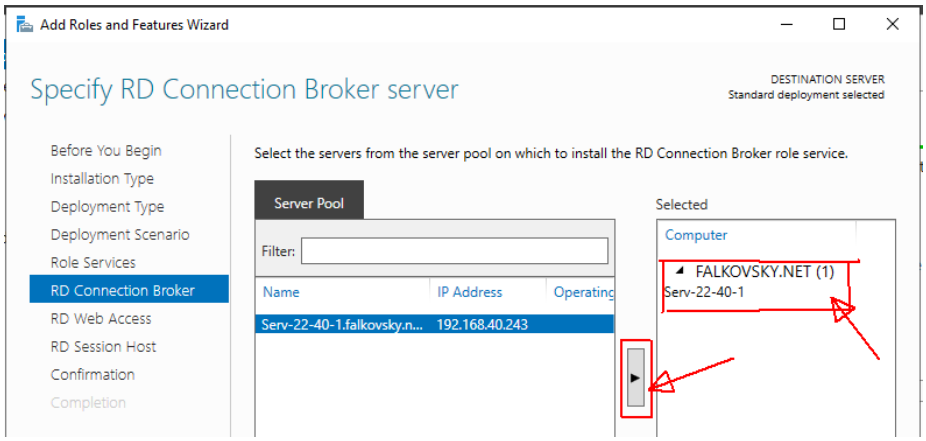


Рис. 11.6

На рис. 11.7 показано, що той самий сервер обрано для компонента RD Web Access.

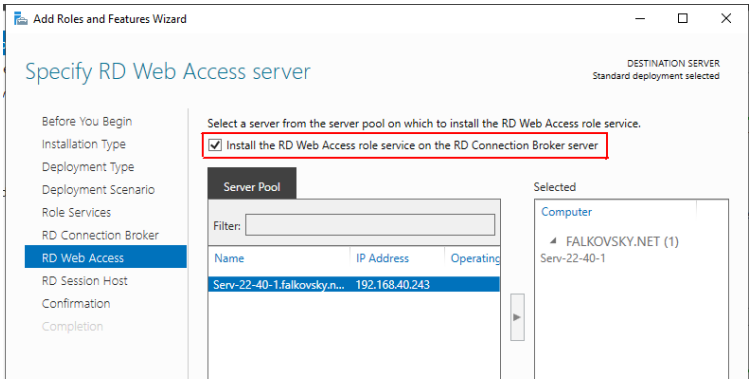


Рис. 11.7

І нарешті, той самий сервер обрано для RD Session Host (рис. 11.8).

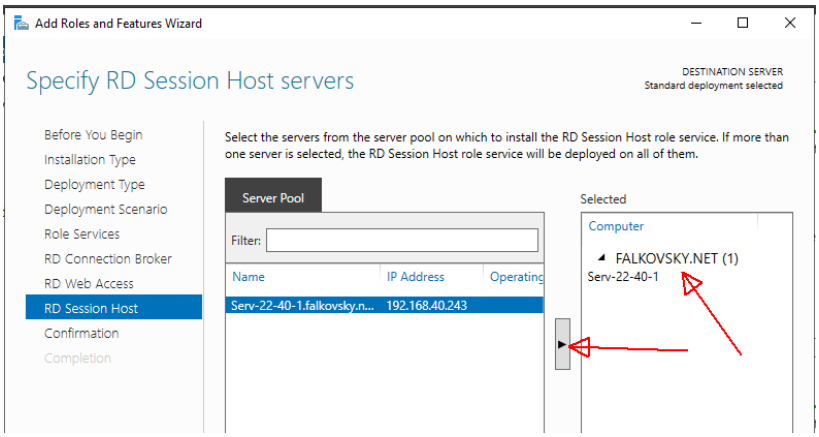


Рис. 11.8

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. 11.9).

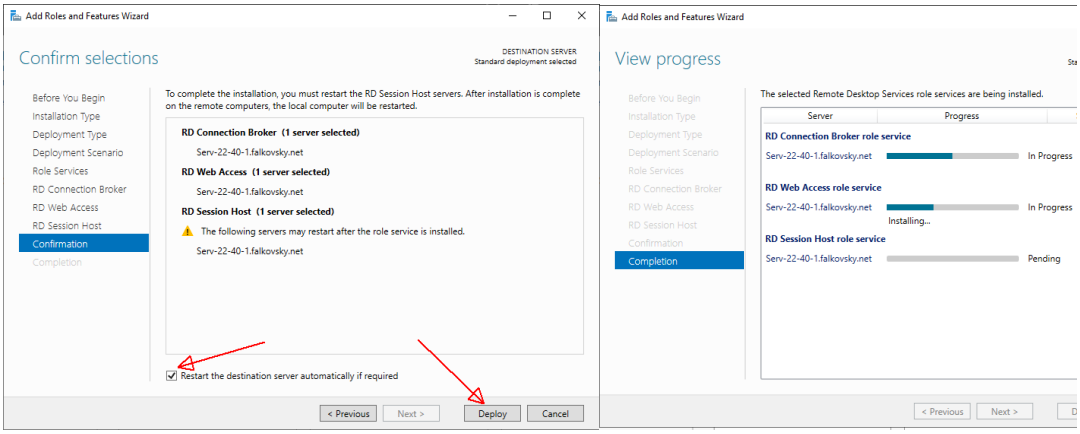


Рис. 11.9

Встановлення необхідних компонентів завершено, а відповідна група опцій з’явилися у вікні Server Manager (рис. 11.10). Тепер треба налаштувати встановлені служби.

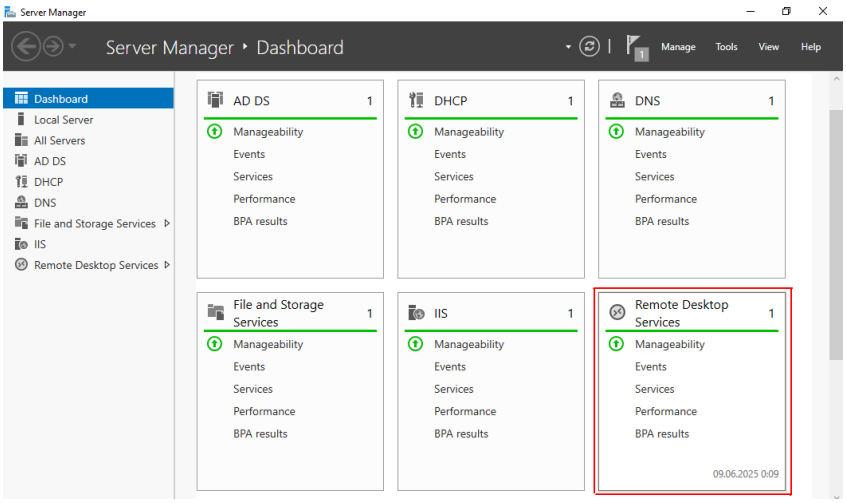


Рис. 11.10

Завдання №11.1

- 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. 11.11). 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. 11.11).

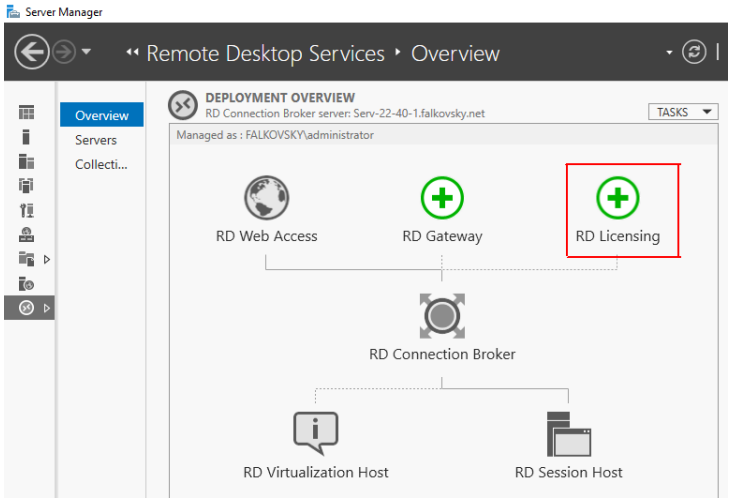


Рис. 11.11

Оберемо у ролі серверу ліцензій перший контролер домену (рис. 11.12).

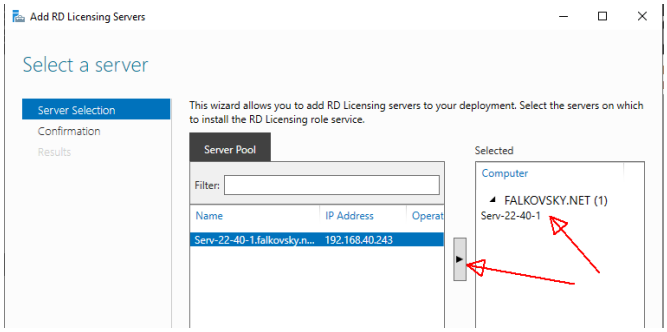


Рис. 11.12

Переконайтеся, що потрібний сервер обрано (рис. 11.13) на натисніть *Add*.

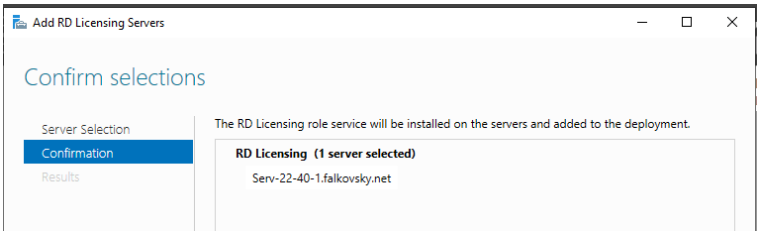


Рис. 11.13

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. 11.14, рис. 11.15).

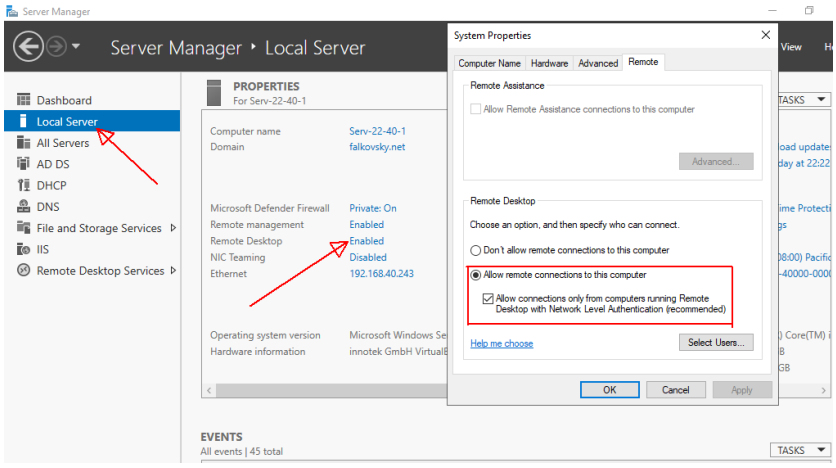


Рис. 11.14

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. 11.15).

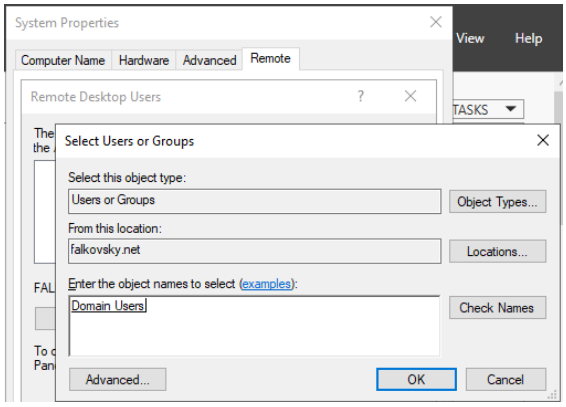


Рис. 11.15

Одержимо вміст вкладки *Members* у властивостях групи *Remote Desktop Users*, подібний до зображеного на рис. 11.16. Натисніть *Apply*.

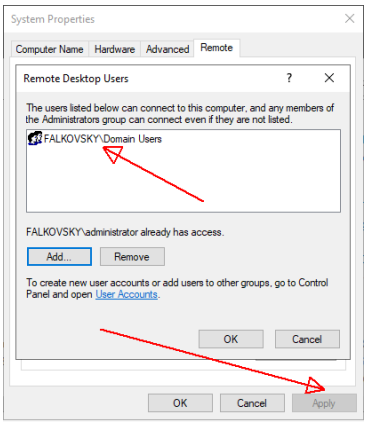


Рис. 11.16

Тепер доналаштуємо компонент RD Licensing. Для цього в області Deployment Overview оберіть *TASKS → Edit Deployment Properties* (рис. 11.17).

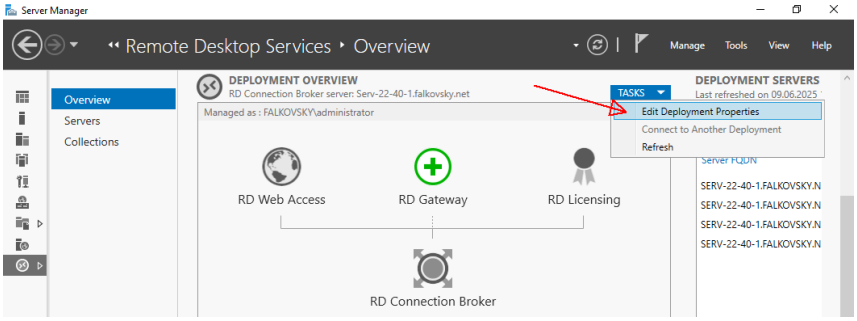


Рис. 11.17

Вкажемо, що ліцензування буде здійснюватися у режимі Per User і переконаймося, що у ролі серверу ліцензування обрано перший контролер домену (рис. 11.18).

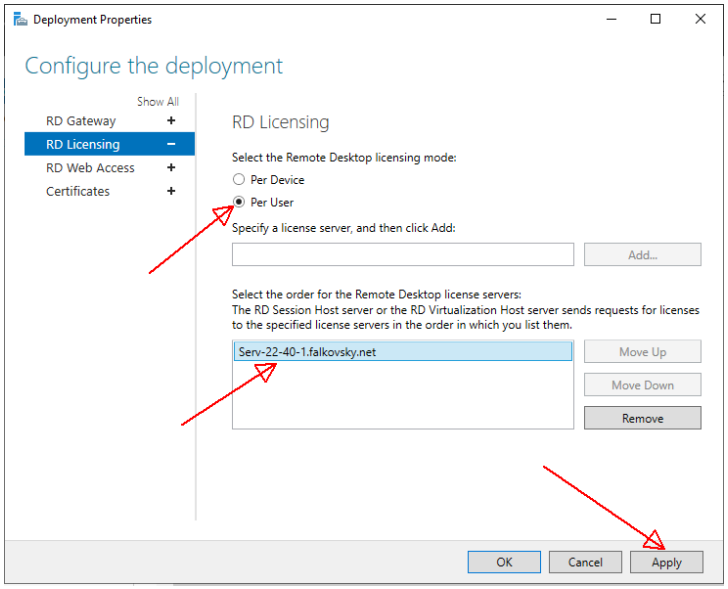


Рис. 11.18

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.11.19):

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

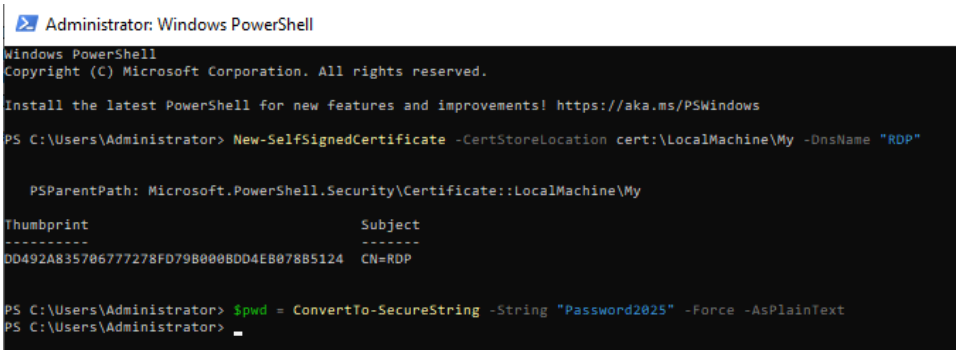


Рис. 11.19

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. 11.20.

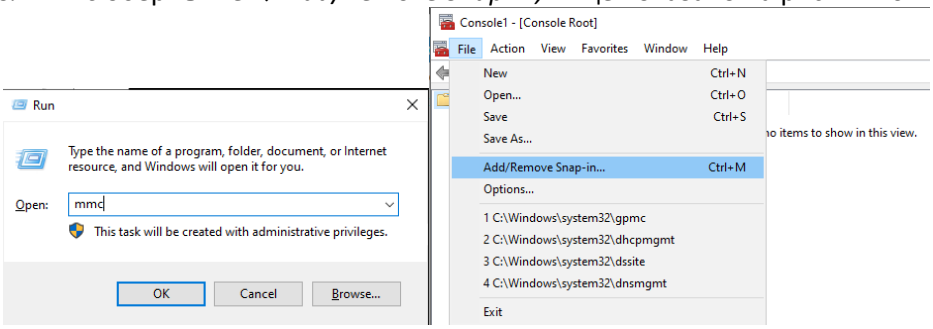


Рис. 11.20

Знайдіть потрібне оснащення та додайте його у вашу новостворену консоль (рис. 11.21).

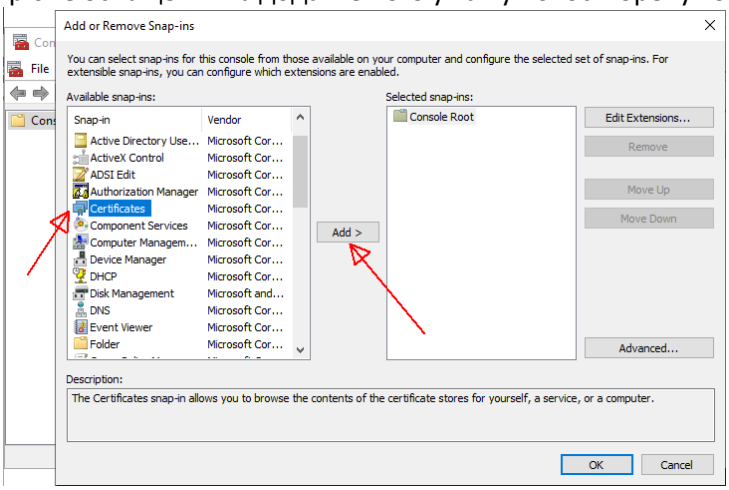


Рис. 11.21

Далі оберемо пункт *Computer Account* (рис. 11.22).

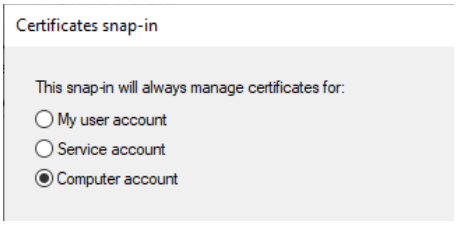


Рис. 11.22

Працювати дане оснащення буде локально, саме на цьому сервері (рис. 11.23).

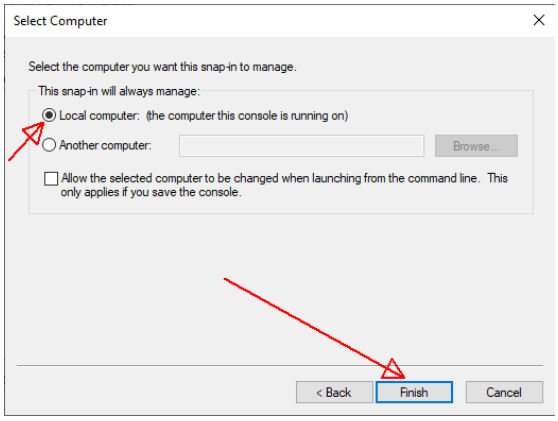


Рис. 11.23

Переконайтеся, що оснащення Certificates справді обране та натисніть OK (рис. 11.24).

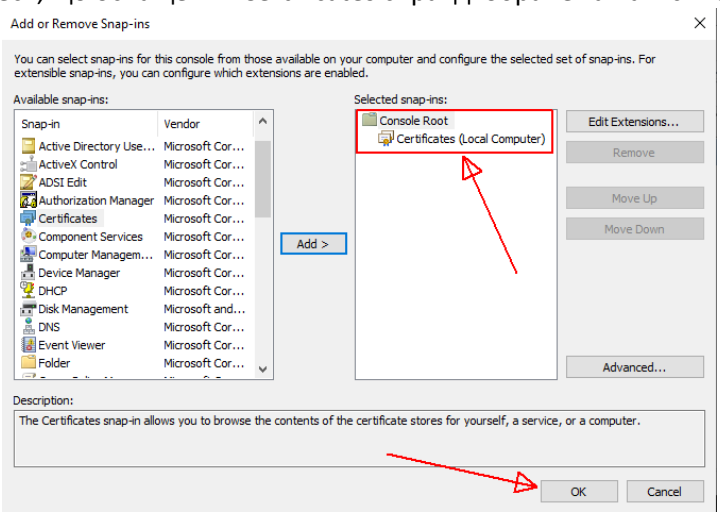


Рис. 11.24

Тепер у новоствореній консолі є перше оснащення - *Certificates* (рис. 11.25). Воно має багато вузлів, однак нас цікавить вузол *Personal* → *Cetificates*. Саме тут має відображатися сертифікат, який раніше було створено за допомогою PowerShell.

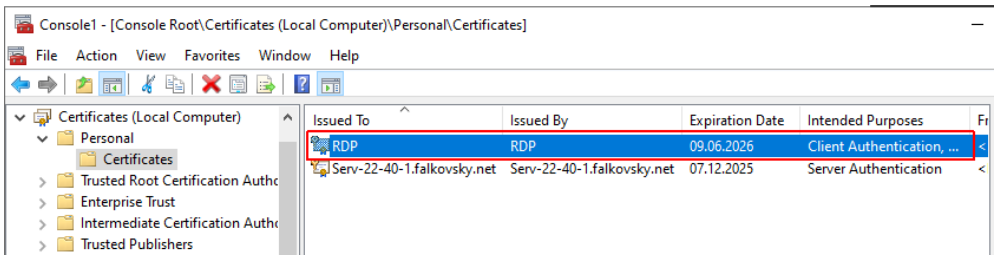


Рис. 11.25

Консоль збережемо на випадок, якщо вона знадобиться у майбутньому (рис. 11.26).

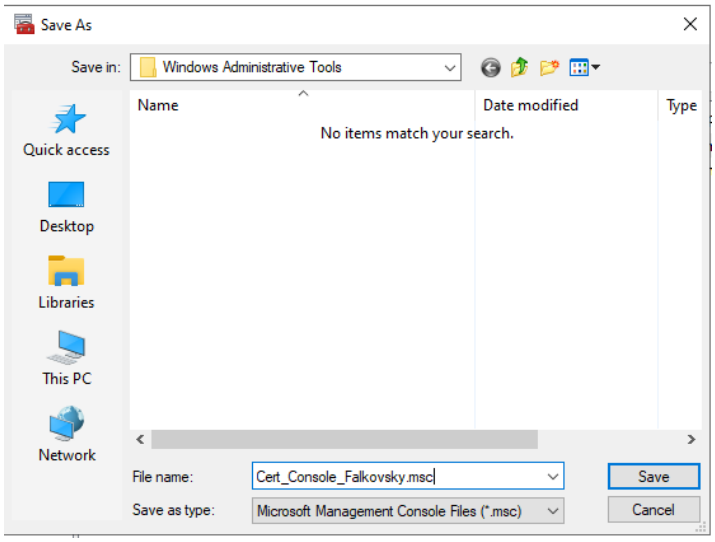


Рис. 11.26

Тепер експортуємо цей сертифікат на сервер у вигляді файлу. Для цього спершу виберемо відповідну опцію у контекстному меню сертифікату (рис. 11.27).

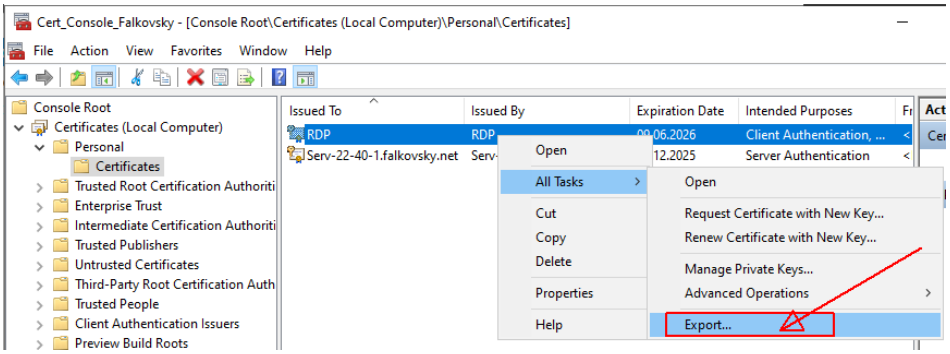


Рис. 11.27

Запуститься майстер експорту сертифікатів (рис. 11.28). Натисніть *Next*.

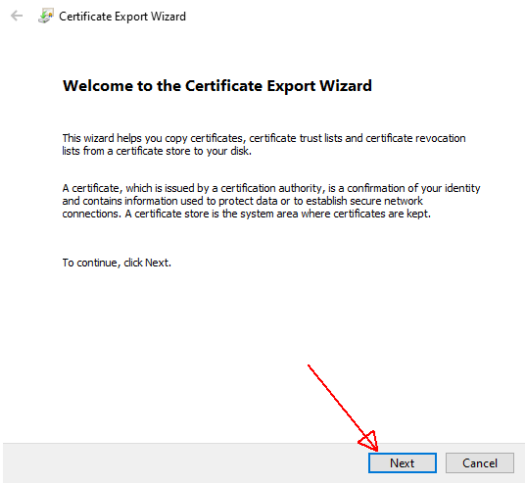


Рис. 11.28

Система попередить нас, що для наступної роботи з експортованим серитфікатом знадобиться пароль (рис. 11.29). Йдеться про пароль, який ми задали за допомогою PowerShell. Натисніть *Next*.

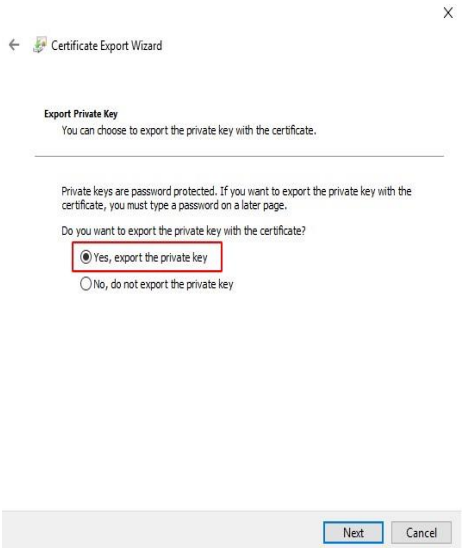


Рис. 11.29

Формат ключа лишаємо без змін (рис. 11.30).

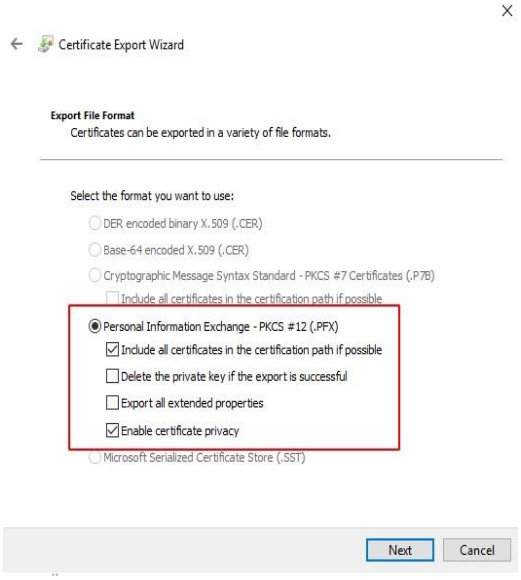
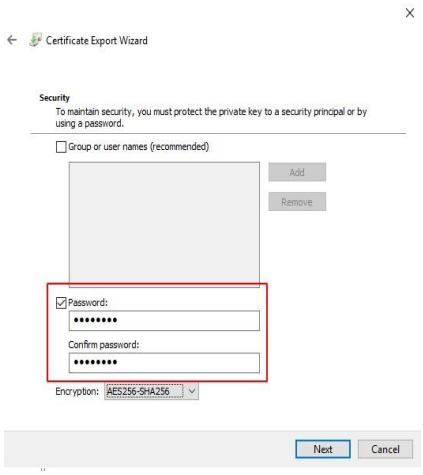


Рис. 11.30

Підтвердимо своє право на завантаження файлу сертифікату, ввівши пароль. Алгоритм шифрування оберіть на власний розсуд. На скриншоті вибрано AES256-SHA256 (рис. 11.31).



Оберіть папку, в яку треба зберегти сертифікат, та його ім’я (рис. 11.32).

Рис. 11.31

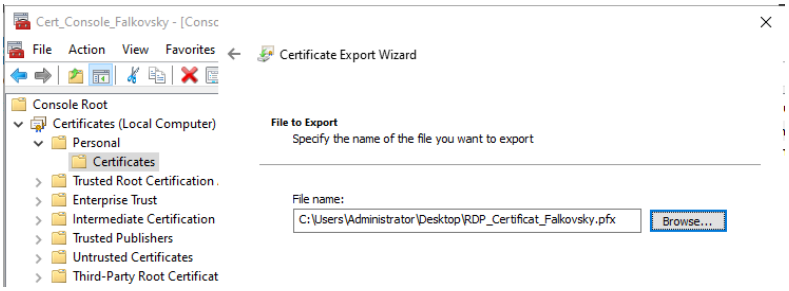


Рис. 11.32

Перевірте, що введено коректні дані (рис. 11.33) й натисніть *Export*.

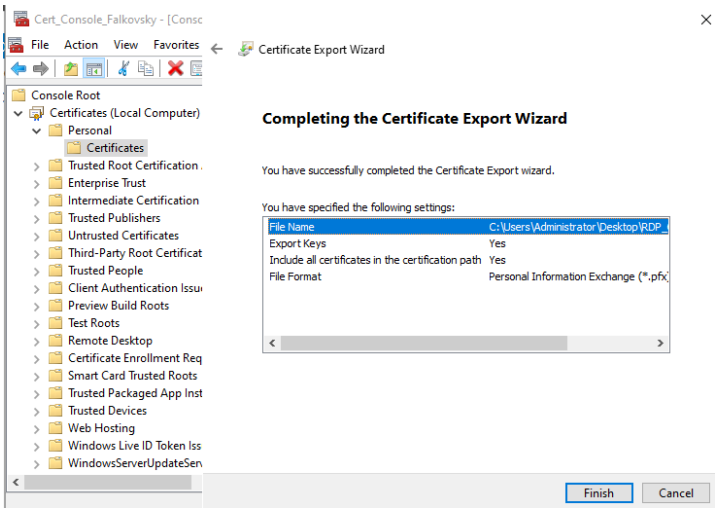


Рис. 11.33 Сертифікат

експортовано (рис. 11.34).

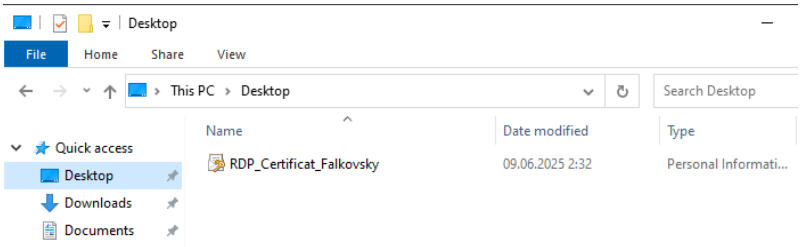


Рис. 11.34

Продовжуємо налаштовувати ліцензування у вікні *Deployment Properties*, крок *Cerificates*. Оберемо першу з трьох служб у списку й натиснемо *Select Existing Certificate* (рис.11.35).

На наступному кроці знадобиться ввести пароль, заданий раніше (рис. 11.36).

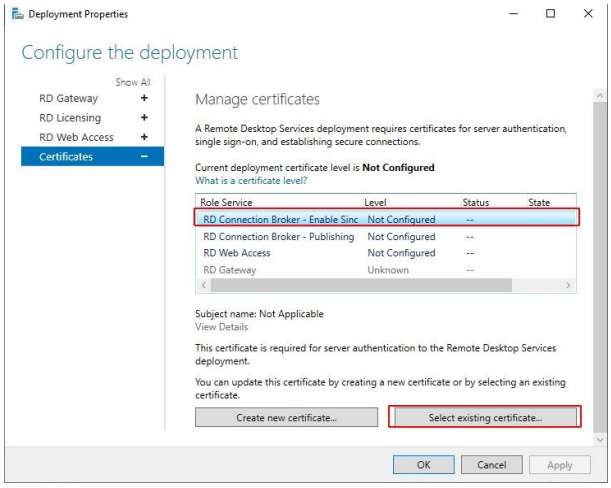


Рис. 11.35

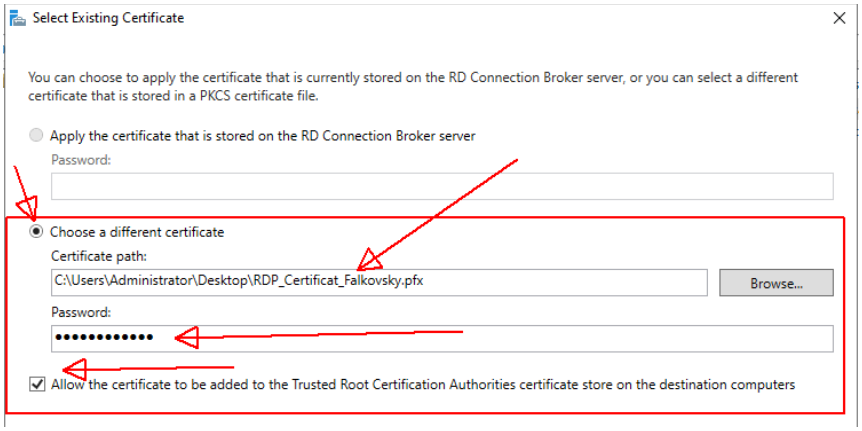


Рис. 11.36

Стан сертифікату першої служби зміниться на Ready to apply. Переконавшись, що цю службу вибрано у переліку, натисніть *Apply* (не *OK*) рис. 11.37. Застосування змін може зайняти деякий час.

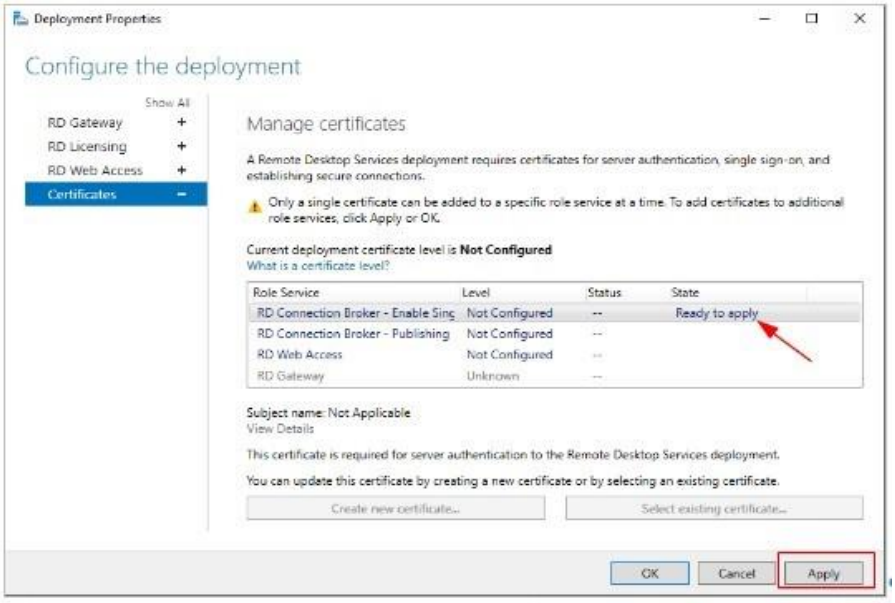


Рис. 11.37

Далі повторимо аналогічні дії з рештою двома службами у списку. У підсумку стан сертифікатів для всіх трьох служб повинен мати стан *Success* (рис. 11.38). 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.

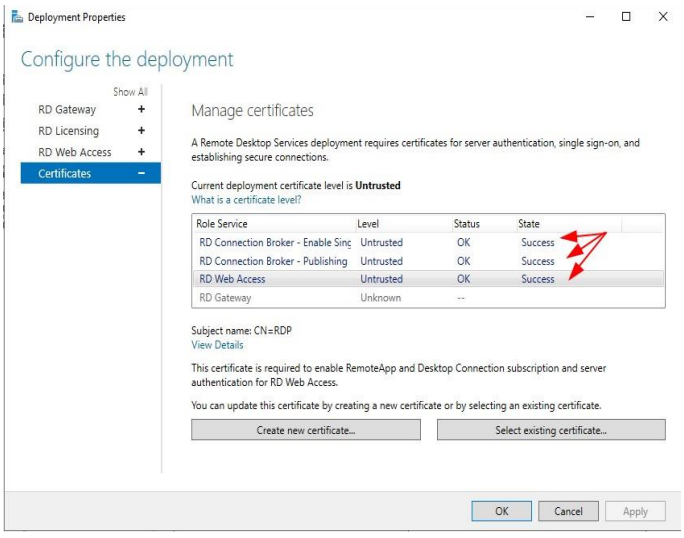


Рис. 11.38

Завдання №11.2

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. 11.39). Створення відповідного PTR-запису у зоні зворотного перегляду - на ваш розсуд.

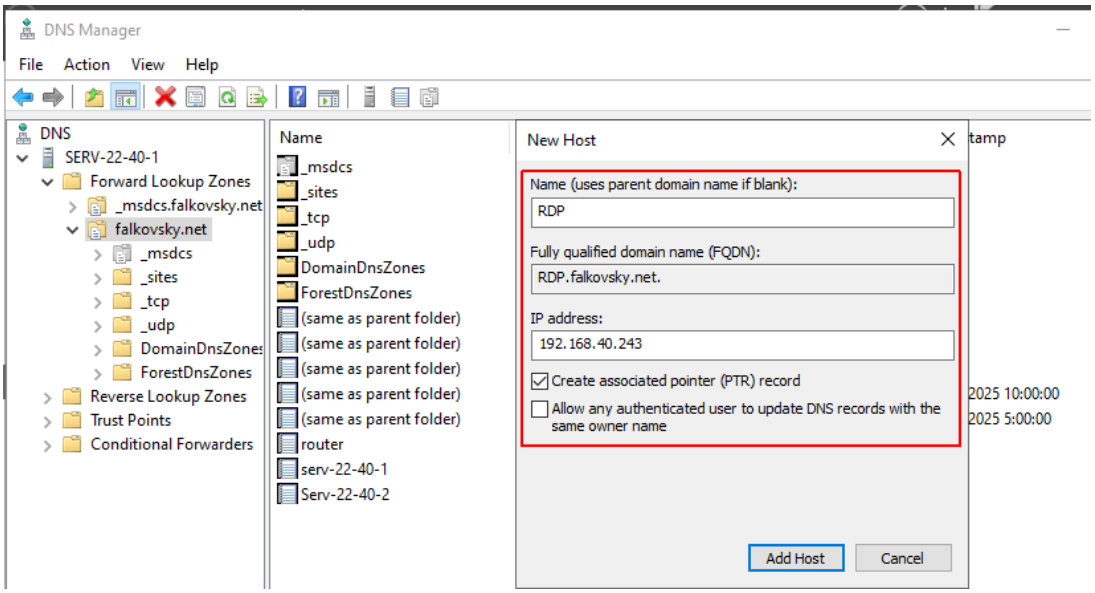


Рис. 11.39

Завдання №11.3

❖ 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.

Надання доступу користувачам 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. 11.40). Це нормально у даній ситуації - натисніть *Перейти на веб-сторінку* чи інше подібне посилання у вашому браузері.

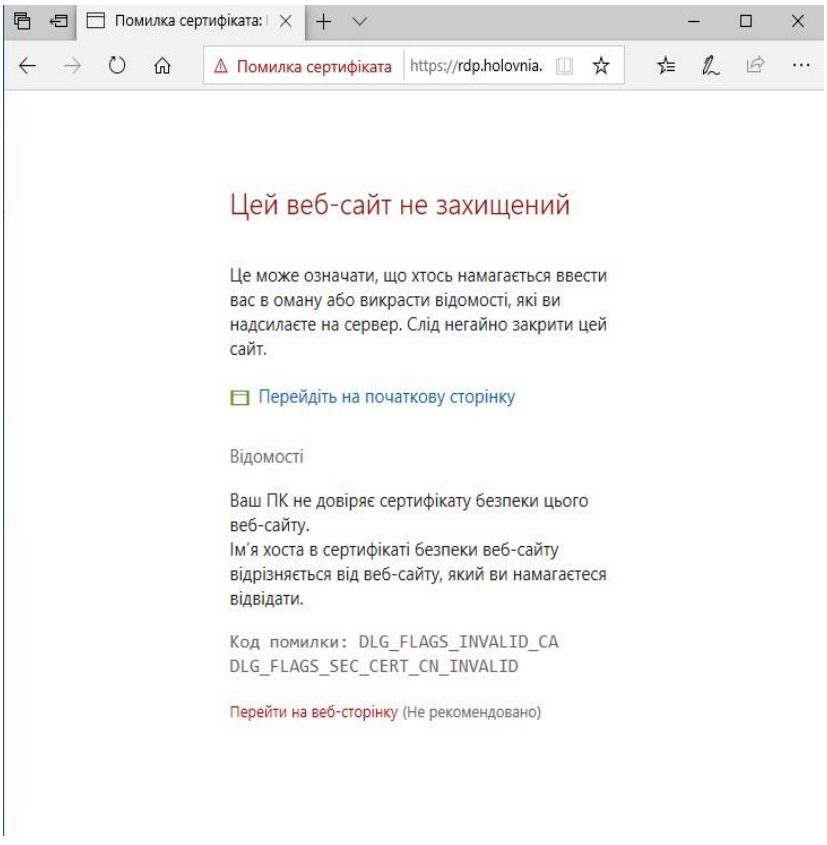


Рис. 11.40

Якщо з'єднання успішне, ви побачите стартову сторінку IIS Windows Server (рис. 11.41).

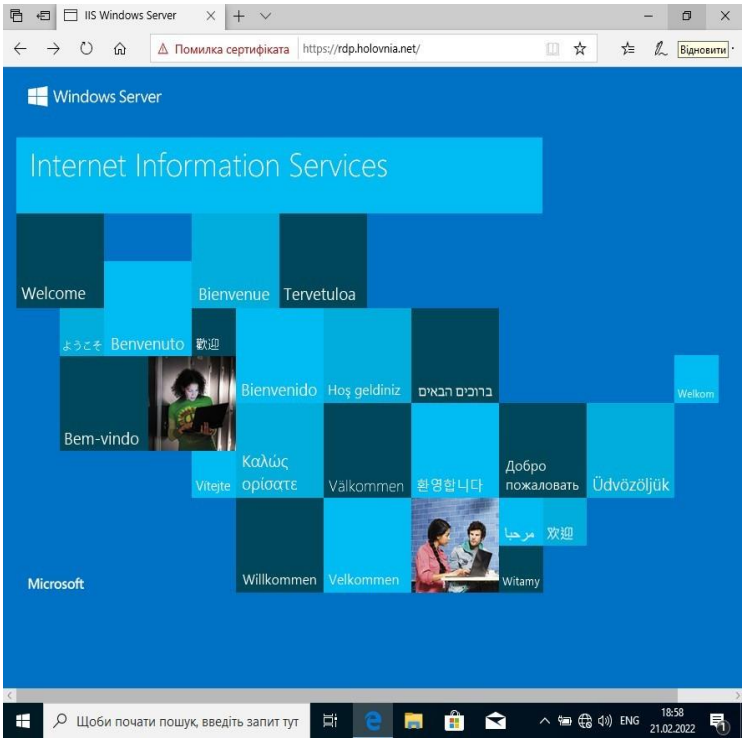
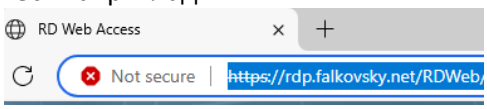


Рис. 11.41

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. 11.42).

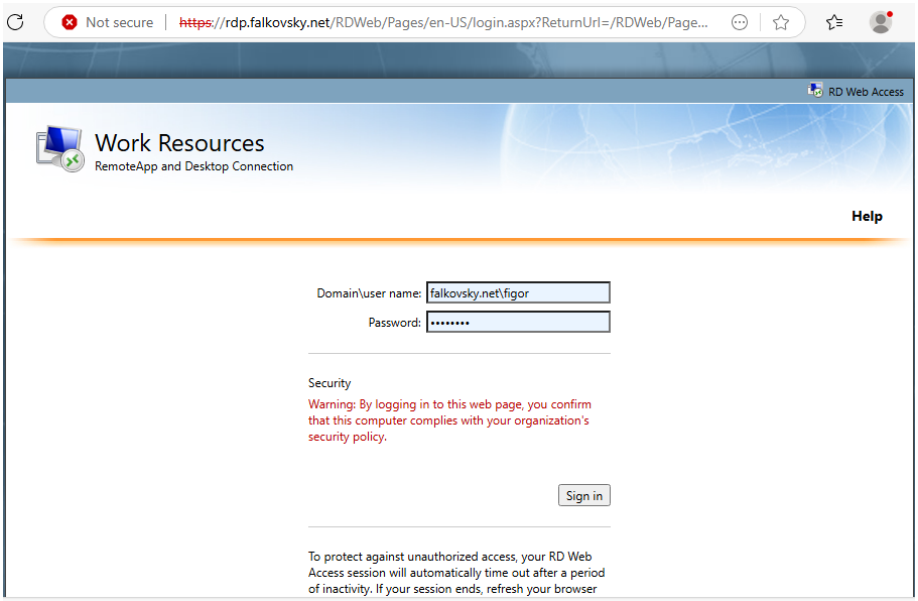


Рис. 11.42

Після успішного входу побачимо область RemoteApp and Desktops - поки що порожню (рис. 11.43).

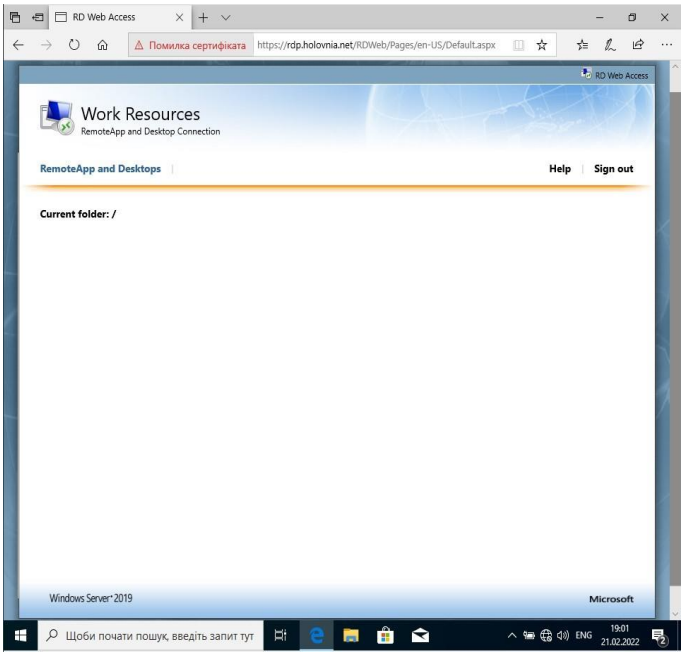


Рис. 11.43

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. 11.44)

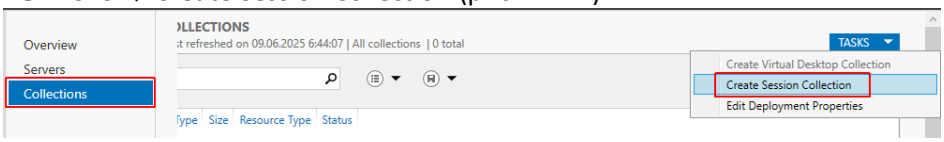


Рис. 11.44

Відкриється вікно майстра створення колекцій (рис. 11.45).

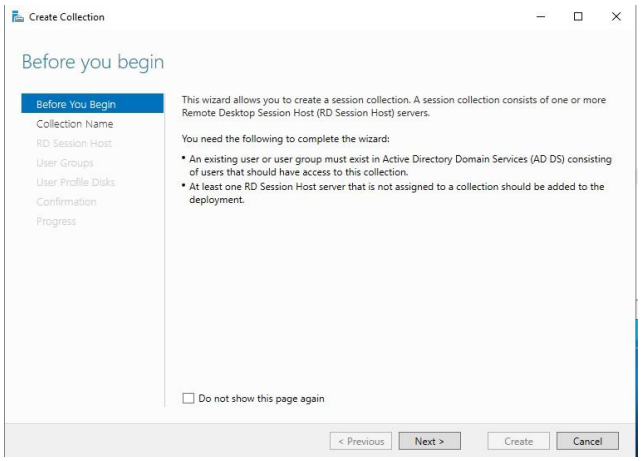


Рис. 11.45

Дамо колекції ім’я (рис. 11.46).

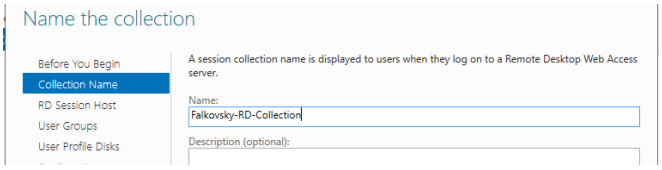


Рис. 11.46

Оберемо сервер, який є водночас першим контролером домену (рис. 11.47).

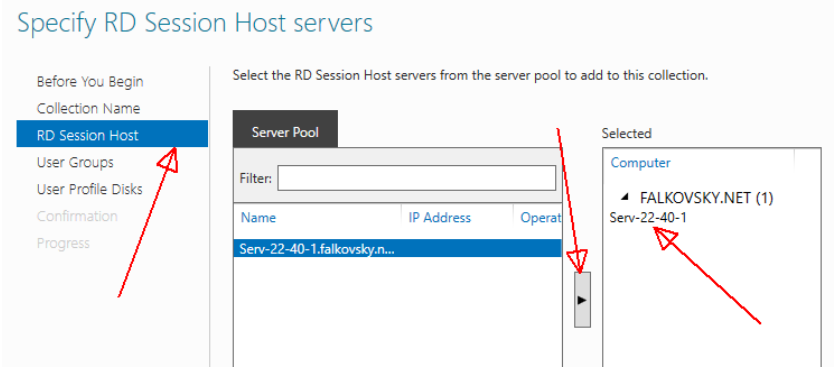


Рис. 11.47

Доступ до колекції за замовчуванням матимуть всі користувачі домену. Нас це влаштовує (рис. 11.48).

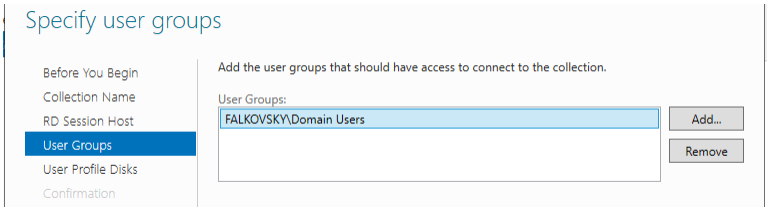


Рис. 11.48

Налаштовувати простір на диску для віддалених користувачів наразі не будемо. Перевірте налаштування (рис. 11.49) і натисніть *Create*. Створення колекції може зайняти деякий час.

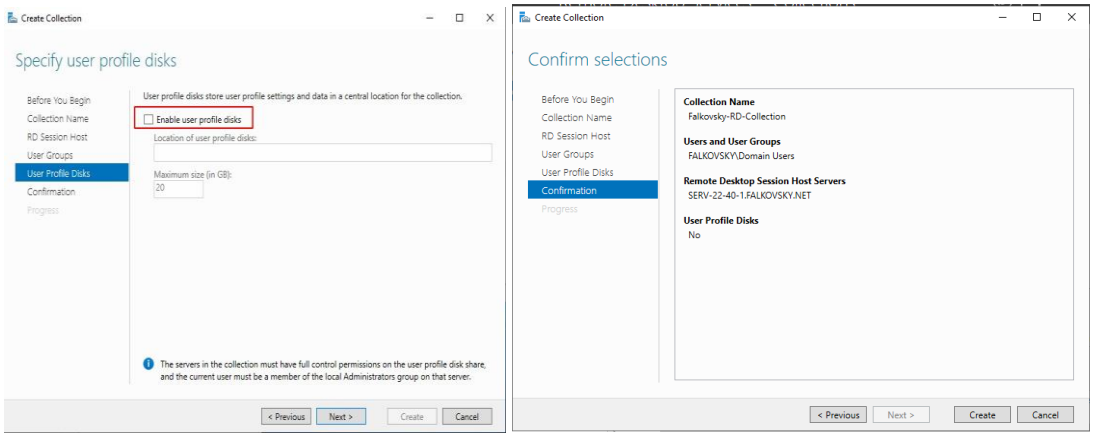


Рис. 11.49

Тепер додамо до новоствореної колекції програми (рис. 11.50).

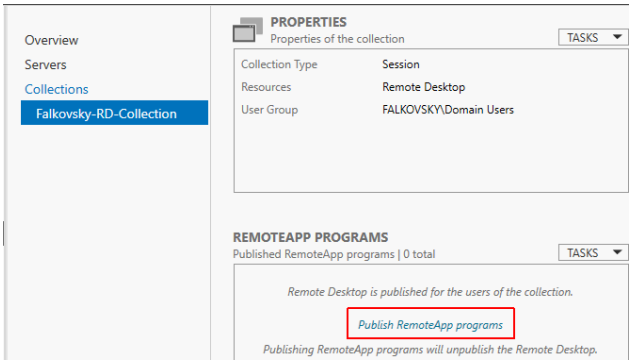


Рис. 11.50

Оберемо кілька програм (рис. 11.51) та натиснемо *Publish*.

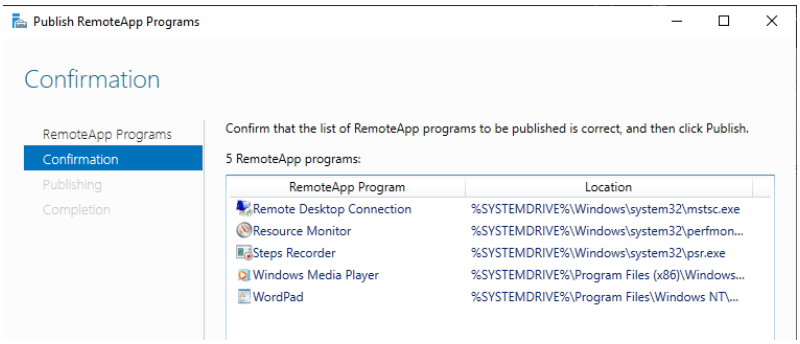


Рис. 11.51

Тепер з робочої станції на оновленій сторінці браузера видно опубліковані програми (рис. 11.52).

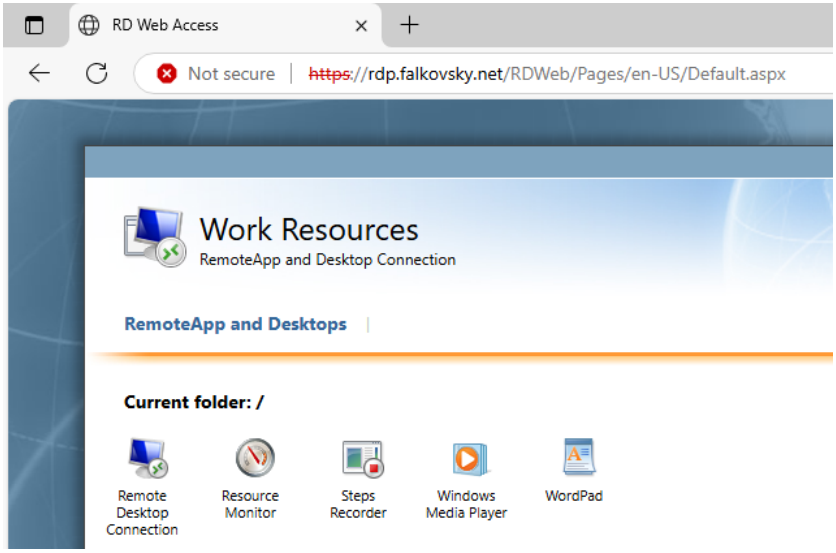


Рис. 11.52

Спробуємо запустити одну з них (рис. 11.53).

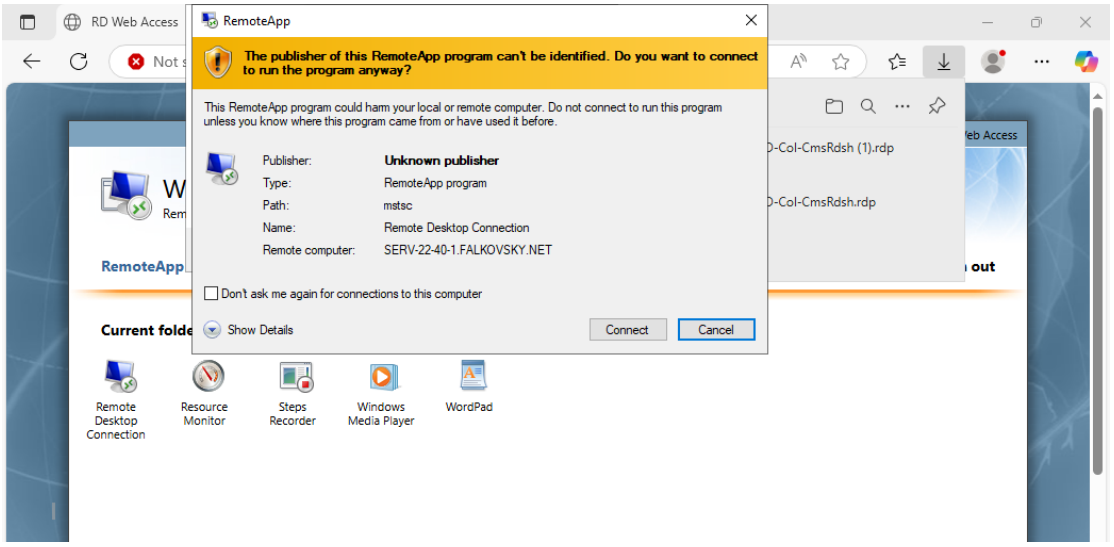


Рис. 11.53

Першого разу треба ввести пароль користувача домену. Після чого програма запуститься. У *Диспетчері завдань* видно, що насправді програма працює віддалено (рис. 11.54).

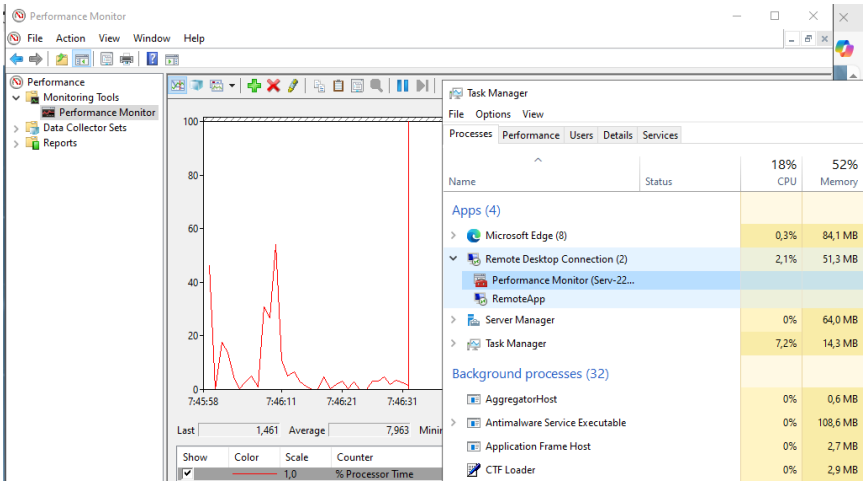


Рис. 11.54

Завдання №11.4

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 11.1 – 11.4.

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.