

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект центру сертифікації для
корпоративної Windows-мережі організації»

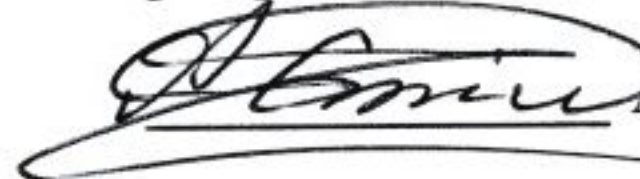
Виконала студентка 4-го курсу групи КІ-19-1
спеціальності 123 «Комп'ютерна інженерія»

 Анастасія Гальчин

Керівник к. п. н., доцент каф. КІ та КБ

 Олена Головня

Рецензент завідувач кафедри КІ та КБ, к. т. н., доцент

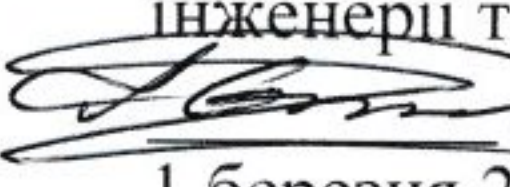
 Андрій Єфіменко

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Гальчин Анастасія Вікторівна

Тема роботи: «Проект центру сертифікації для корпоративної Windows-мережі організації»

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 24 червня 2023 р.

Вихідні дані роботи: об'єктом дослідження є підсистеми сертифікації для Windows-мережі організації, що використовуються для автентифікації користувачів, забезпечення безпеки даних та забезпечення контролю доступу до ресурсів мережі; предметом дослідження є технології та методи, що використовуються у підсистемах сертифікації для Windows-мережі організації, такі як сертифікати.

Обладнання та програмне забезпечення:

1. GNS3
2. GNS VM
3. Oracle VirtualBox
4. Windows Server 2019 Standart
5. Windows 10

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів,
що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О. С.	01.03.2023	01.03.2023
2	Головня О. С.	01.03.2023	01.03.2023
3	Головня О. С.	01.03.2023	01.03.2023

Студентка Анастасія Гальчин
Керівник Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2023-07.03.2023	
2	Аналіз літературних джерел	08.3.2023-25.03.2023	
3	Аналіз об'єкта дослідження	26.03.2023-04.04.2023	
4	Аналіз аналогічних розробок	05.04.2023-19.04.2023	
5	Вибір обладнання	20.04.2023-26.04.2023	
6	Налаштування Active Directory	27.04.2023-6.05.2023	
7	Налаштування Server Certification	7.05.2023-23.05.2023	
8	Створення сертифіката	24.05.2023-31.05.2023	
9	Тестування працездатності сертифіката	01.06.2023-04.06.2023	
10	Написання пояснювальної записки	05.06.2023-24.06.2023	
11	Захист	27.06.2023	

Студентка Анастасія Гальчин
Керівник Олена Головня

РЕФЕРАТ

Звіт з курсової роботи складається зі вступу, трьох розділів, висновку та списку використаної літератури.

Текстова частина викладена на 71 сторінках друкованого тексту. Список використаних джерел містить 10 найменувань і займає 2 сторінки. В роботі наведено 100 рисунків та 4 таблиці.

Метою кваліфікаційної роботи є розгортання сервера сертифікації для Windows-мережі організації та його використання для забезпечення безпеки даних та доступу до них у мережевому середовищі.

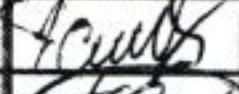
У першому розділі було виконано опис теоретичних відомостей.

У другому розділі описано базові налаштування Windows Server та Active Directory.

У третьому розділі описано налаштування Active Directory Certificate Services та сертифікату.

Висновки містять в собі результати виконаної роботи.

Ключові слова: Active Directory, Certificate Services, Windows Server, сертифікат, сертифікат SSL.

					KKIK.KP.B – 123 – 3 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Гальчин А. В.		20.06.23	Проект центру сертифікації для корпоративної Windows-мережі організації	Літ.	Арк.
Керівник		Головня О. С.		20.06.23			4
Реценз.		Єфіменко А. А.		20.06.23		Аркушів	71
Н. контр.		Головня О. С.		20.06.23		ФІКТ, Гр. КІ-19-1	
Затверд.		Єфіменко А. А.		20.06.23			

ANNOTATION

The explanatory note contains of an introduction, three chapters, a conclusion and a list of references.

The text part is presented on 72 pages of printed text. The list of references includes 10 titles and occupies 2 pages. The paper contains 100 figures and 4 tables.

The purpose of the qualification work is to deploy a certification server for an organization's Windows network and use it to ensure data security and access in a network environment.

The first section describes the theoretical background.

The second section describes the basic settings of Windows Server and Active Directory.

The third section describes the settings of Active Directory Certificate Services and how to create a certificate.

The conclusion contains the results of the work performed.

Keywords: Active Directory, Certificate Services, Windows Server, certificate, SSL certificate.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1. ОСОБЛИВОСТІ РОБОТИ ЦЕНТРІВ СЕРТИФІКАЦІЇ У КОМП'ЮТЕРНИХ МЕРЕЖАХ	9
1.1 Поняття про центр сертифікації	9
1.2 Основні аспекти організації власного центру сертифікації	10
1.3 SSL сертифікати	11
1.4 Реалізації сервера сертифікації.....	14
Висновки до першого розділу	17
РОЗДІЛ 2. НАЛАШТУАННЯ БАЗОВИХ ТА ДОДАТКОВИХ НАЛАШТУВАНЬ ДОМЕНУ	18
2.1 Створення мережі.....	18
2.2 Вибір обладнання для організації роботи мережі	19
2.3 Встановлення Windows Server	21
2.4 Базове налаштування Active Directory	23
Висновки до другого розділу	40
РОЗДІЛ 3. СТВОРЕННЯ ТА НАЛАШТУВАННЯ СЕРВЕРА СЕРТИФІКАЦІЇ	41
3.1 Встановлення та налаштування сервера сертифікації	41
3.2 Створення запиту на сертифікат	54
3.3 Створення сертифікату	59
3.4 Перевірка працездатності.....	65
Висновки до третього розділу.....	69
ВИСНОВКИ.....	70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	71

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПК – персональний комп'ютер.

AC – Active Directory.

CA - Certification Authority

CS - Certification Server

CSR - Certificate Signing Request

SSL - Secure Sockets Layer.

PCA - Private Certificate Authority.

ОС – операційна система.

ЦСК – центр сертифікації ключів.

IIS - Internet Information Services

DNS - Domain Name System

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. Сервер сертифікації є дуже важливою складовою інфраструктури безпеки Інтернету, оскільки він забезпечує можливість перевірки автентичності цифрових сертифікатів та забезпечує їхню безпеку.

З його допомогою можна забезпечити захист від шахрайства та інших атак, які спрямовані на підробку цифрових сертифікатів. Зокрема, за допомогою сервера сертифікації можна перевірити, чи є сертифікат відповідним до публічного ключа, який використовується для шифрування даних та забезпечення їхньої конфіденційності.

Крім того, сервер сертифікації забезпечує можливість встановлення безпечного з'єднання між клієнтом та сервером, що є важливим для забезпечення безпеки відповідності з міжнародними стандартами та законодавством.

Метою кваліфікаційної роботи є розгортання сервера сертифікації для Windows-мережі організації та його використання для забезпечення безпеки даних та доступу до них у мережевому середовищі.

Об'єктом дослідження є підсистеми сертифікації для Windows-мережі організації, що використовуються для автентифікації користувачів, забезпечення безпеки даних та контролю доступу до ресурсів мережі.

Предметом дослідження є технології та методи, що використовуються у підсистемах сертифікації для Windows-мережі організації, такі як сертифікати.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ОСОБЛИВОСТІ РОБОТИ ЦЕНТРІВ СЕРТИФІКАЦІЇ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1 Поняття про центр сертифікації

Центр сертифікації - це установа або організація, яка здійснює процедуру сертифікації продуктів, послуг, систем управління та інших об'єктів відповідно до встановлених вимог та стандартів. Сертифікація передбачає оцінку відповідності об'єкта певним вимогам і підтвердження його відповідності цим вимогам шляхом видачі сертифіката відповідності^[1].

Центри сертифікації можуть бути державними або приватними. Державні центри сертифікації зазвичай функціонують на рівні держави та здійснюють сертифікацію об'єктів, що підлягають обов'язковій сертифікації. Приватні центри сертифікації можуть створюватися різними організаціями та компаніями і проводити сертифікацію об'єктів за добровільною основою.

Центри сертифікації, особливо сторонні, видають сертифікати на основі класів, які визначають надійність сертифіката.

У таблиці 1.1 подано опис класів. Номер класу залежить від суворості процедур перевірки особи власника під час видачі сертифіката. Чим вищий номер класу, тим більш надійний сертифікат. Тому сертифікату класу 5 довіряють набагато більше, ніж сертифікату нижчого класу.

Таблиця 1.1 Опис класів сертифікатів

Клас	Опис
0	Використовується для тестування в ситуаціях, коли перевірки не проводилися.
1	Використовується особами, які потребують підтвердження електронної пошти.
2	Використовується організаціями, для яких потрібне підтвердження особи.
3	Використовується для підпису серверів і програмного забезпечення. Незалежне підтвердження та перевірка ідентичності та повноважень здійснюється центром сертифікації.
4	Використовується для онлайн-ділових операцій між компаніями.
5	Використовується для приватних організацій або державної служби безпеки.

Наприклад, для сертифіката класу 1 може знадобитися відповідь електронною поштою від власника, щоб підтвердити, що він бажає зареєструватися. Таке підтвердження є слабкою автентифікацією власника. Для отримання сертифіката класу 3 або 4 майбутній власник повинен особисто надати принаймні два офіційні документи, що посвідчують особу, і підтвердити відкритий ключ.

1.2 Основні аспекти організації власного центру сертифікації

Власний центр сертифікації (приватний центр сертифікації, Private Certificate Authority, PCA) - це сертифікаційний центр, який відповідає за видання цифрових сертифікатів для внутрішнього використання в організації. PCA може бути створений внутрішньо в організації та дозволяє підписувати сертифікати для внутрішніх потреб без необхідності звертатися до зовнішнього сертифікаційного центру.

Власний центр сертифікації дозволяє забезпечити безпеку та конфіденційність даних, особливо за рахунок шифрування трафіку між клієнтом і сервером. Крім того, він дозволяє забезпечити аутентифікацію користувачів та контролювати доступ до мережеских ресурсів.

Організації можуть використовувати власний центр сертифікації для різноманітних цілей, зокрема для захисту електронної пошти, веб-сайтів, програм та інших систем. Він також дозволяє надавати сертифікати для віртуальних приватних мереж (VPN), які забезпечують безпеку інтернет-з'єднання між різними місцезнаходженнями в організації.

У таблиці 1.2 розглянемо переваги та недоліки власного центру сертифікації^[2].

Таблиця 1.2 Переваги та недоліки власного центру сертифікації

Переваги		Недоліки	
Контроль: Створення власного сервера ЦСК дозволяє зберегти контроль над управлінням сертифікатами, що видаються та відкликаються. Це дозволяє забезпечити вищий рівень безпеки в мережі.		Вартість: Створення власного сервера ЦСК може бути дорогим процесом, оскільки потрібні витрати на апаратне та програмне забезпечення, а також на підготовку технічного персоналу.	

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Продовження таблиці 1.2 Переваги та недоліки власного центру
сертифікації

Гнучкість: Власний сервер ЦСК дає можливість налаштувати вимоги до сертифікатів, які видаються, щоб вони відповідали конкретним потребам організації.	Складність: Створення власного сервера ЦСК може бути складним процесом для неспеціалістів. Необхідно мати високі знання в галузі криптографії та мережної безпеки.
Незалежність: Створення власного сервера ЦСК дозволяє організації бути незалежною від зовнішніх служб сертифікації та захистити себе від можливих атак з боку злоумисників.	Підтримка: Створення власного сервера ЦСК вимагає постійної підтримки та оновлення з метою забезпечення безпеки та надійності сертифікаційної інфраструктури.

Загалом, наявність власного центру сертифікації може бути корисним для компаній та організацій, яким потрібен більший контроль над видачею сертифікатів та управлінням сертифікатами, а також більшої гнучкості у встановленні правил та політик безпеки для своєї мережі. Однак, використання власного центру сертифікації потребує значних зусиль та витрат, тому перед його створенням необхідно ретельно зважити на всі переваги та недоліки цього підходу.

1.3 SSL сертифікати

Сервер сертифікації (Certificate Authority, CA) - це централізований сервер, який відповідає за видачу цифрових сертифікатів, що підтверджують відповідність певної особи, організації або веб-сайту вимогам криптографічного захисту. Його основна мета є забезпечення захищеного з'єднання між клієнтом та сервером, за допомогою цифрового сертифіката. Це дає можливість підтверджувати ідентичність веб-сайту та довіряти передачі конфіденційної інформації, такої як паролі, банківські дані тощо.

CSR (Certificate Signing Request) - це ключ, який генерується при запиті на видачу (підпис) SSL-сертифіката. CSR являє собою шматок зашифрованого тексту, що містить інформацію про компанію та доменне ім'я. CSR - це файл, який містить інформацію для сертифіката, в тому числі відкритий публічний ключ.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

SSL сертифікат (Secure Sockets Layer Certificate) - це електронний документ, який використовується для забезпечення безпеки при передачі даних через Інтернет. SSL сертифікат дозволяє шифрувати дані між сервером та браузером користувача, щоб запобігти несанкціонованому доступу до цих даних.

Типи SSL-сертифікатів^[3].

SSL з перевіркою домену, або DV (Domain Validation) SSL.
Сертифікат із перевіркою домену видається будь-якій людині, яка довела, що вона володіє доменом, для якого запросила SSL. Цей доказ — це унікальний серійний номер, який центр сертифікації бере з вашого вебсервера або з DNS-записів.

SSL з перевіркою організації, або OV (Organization Validation) SSL.
SSL із перевіркою організації означає, що центр сертифікації також перевіряв ім'я компанії та її адресу в публічних базах даних. Інформація вводиться в сертифікат і зазвичай відображається лише тоді, коли користувач натискає на іконку із замочком.

SSL із розширеною перевіркою, або EV (Extended Validation) SSL.
Розширена перевірка більш ретельна, ніж перевірка домену чи організації. При видачі EV сертифікатів перевіряються права на домен, існування та місцезнаходження компанії.

SSL сертифікат видається Сервером сертифікації (Certificate Authority), який перевіряє, що власник домену, для якого виданий сертифікат, дійсно має право на його використання. Після цього Сервер сертифікації видає електронний SSL сертифікат, який містить інформацію про домен, для якого він виданий, а також про сертифікат видавця, термін дії сертифікату та публічний ключ для шифрування даних^[4].

Після отримання SSL сертифікату, веб-сайт може встановити захищене з'єднання з користувачем за допомогою протоколу HTTPS. Це забезпечує шифрування даних, які передаються між сервером та браузером користувача,

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

забезпечуючи безпеку під час передачі конфіденційної інформації, такої як паролі, фінансові дані тощо.

Також можна використовувати сертифікат SSL, підписаний власним приватним ключем. Так ви обійдетесь без центру сертифікації. Такий сертифікат називається самопідписаним. Його часто використовують просунуті користувачі, а також під час тестування вебдодатків.

SSL сертифікати є важливою складовою безпеки в Інтернеті та є необхідними для захисту конфіденційної інформації користувачів. Вони використовуються в різних галузях, таких як електронна комерція, банківський сектор та соціальні мережі.

Коли ЦС випускає цифровий сертифікат, він очікує, що сертифікат буде використовуватися протягом всього терміну його служби. Але так не завжди буває. Іноді сертифікати скасовують раніше. Такий процес називають відкликання сертифікатів - це процес, який відрізняє недійсні і недовірені сертифікати від допустимо довірених. Якщо ЦС необхідно відкликати сертифікат для вашого сайту, він змушує Google Chrome відображати попередження для відвідувачів вашого сайту^[5]:

СА може відкликати сертифікат вашого сайту по одній з наступних причин:

- Хтось скомпрометував або підозрюється в компрометації закритого ключа вашого сертифіката. (Це найпоширеніша причина.)
- СА неправильно видав сертифікат і випускає новий, щоб замінити його.
- Сам СА піддався ризику компрометації.
- Деталі вашої організації, зазначені в сертифікаті, наприклад, назва вашої організації, змінилися, і ЦС повинен перевидати сертифікат, щоб відобразити цю зміну.
- Сертифікат є незаконним або був обманним шляхом підписаний з вкраденим ключем.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

1.4 Реалізації сервера сертифікації

Існує декілька служб сертифікації, які можуть бути використані для створення та керування сертифікатами. Найбільш поширеними є Active Directory Certificate Services, Windows Server Certificate Authority, OpenSSL for Windows та XCA.

Active Directory Certificate Services (AD CS). Це служба сертифікації, яка надається в межах ролівої послуги Active Directory на серверах Windows. AD CS дозволяє видачу, відкликання та керування сертифікатами в мережі Windows. Вона підтримує різні типи сертифікатів, включаючи особисті, машини, веб-сервери, кодові підписи тощо (рис. 1.1)^[6].

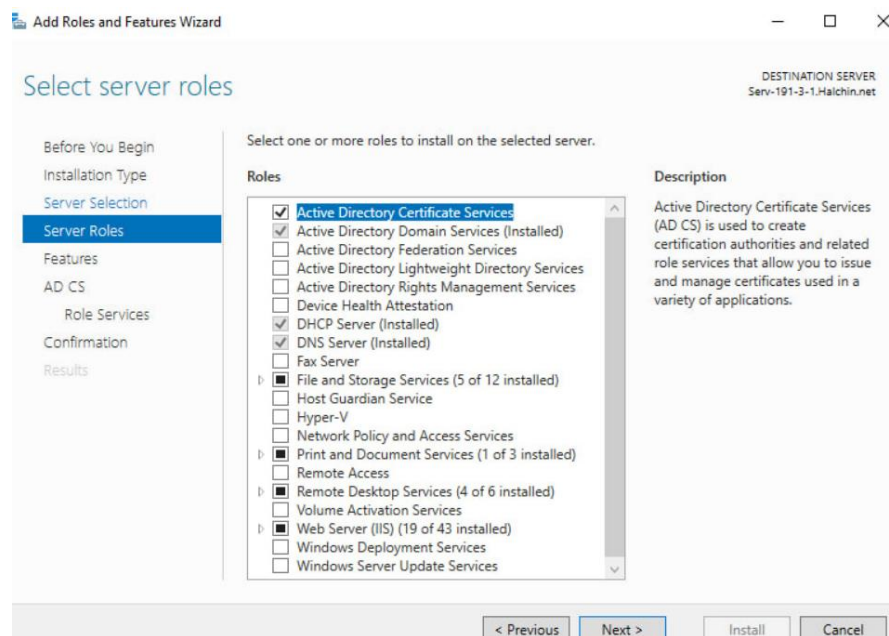


Рис. 1.1 Active Directory Certificate Services

Windows Server Certificate Authority (CA). Це роліова послуга, яка може бути встановлена на серверах Windows для видачі та управління сертифікатами. Вона надає функціонал служби сертифікації, зокрема підтримку CSR, видачу сертифікатів, відкликання та керування (рис. 1.2).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

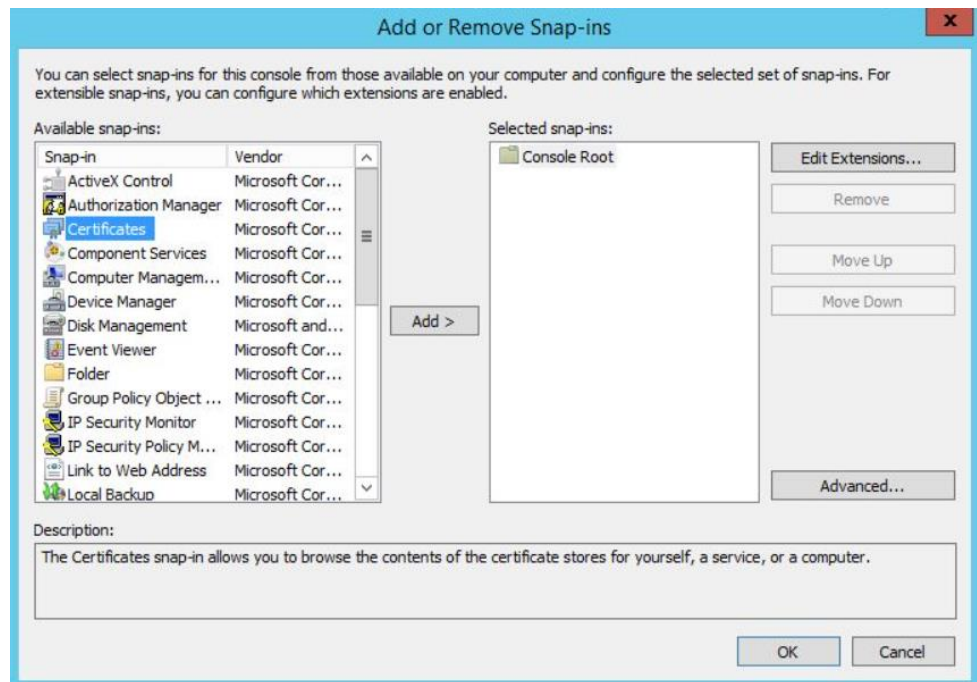


Рис. 1.2 Windows Server Certificate Authority

OpenSSL for Windows. OpenSSL є криптографічною бібліотекою, яка доступна і для платформи Windows. Її можна використовувати для генерації сертифікатів, створення CSR та виконання інших криптографічних операцій. OpenSSL надає командний рядок та програмний інтерфейс, які дозволяють керувати процесом створення та управління сертифікатами (рис. 1.3).

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Dina>cd C:\OpenSSL-Win64
C:\OpenSSL-Win64>cd bin
C:\OpenSSL-Win64\bin>openssl req -new -newkey rsa:2048 -nodes -keyout server.key
-out server_csr.txt -subj "/C=US/ST=Arizona/L=Phoenix/O=Namecheap/OU=SSL/CN=nct
est.info"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
C:\OpenSSL-Win64\bin>

```

Рис. 1.3 OpenSSL

ХСА. ХСА є безкоштовною програмою з відкритим вихідним кодом для керування сертифікатами та приватними ключами. Вона підтримує платформу Windows, Linux, FreeBSD, BSD та Mac та надає графічний інтерфейс користувача для створення та керування сертифікатами, включаючи

генерацію CSR, створення самопідписаних сертифікатів та інші операції (рис. 1.4)^[7].

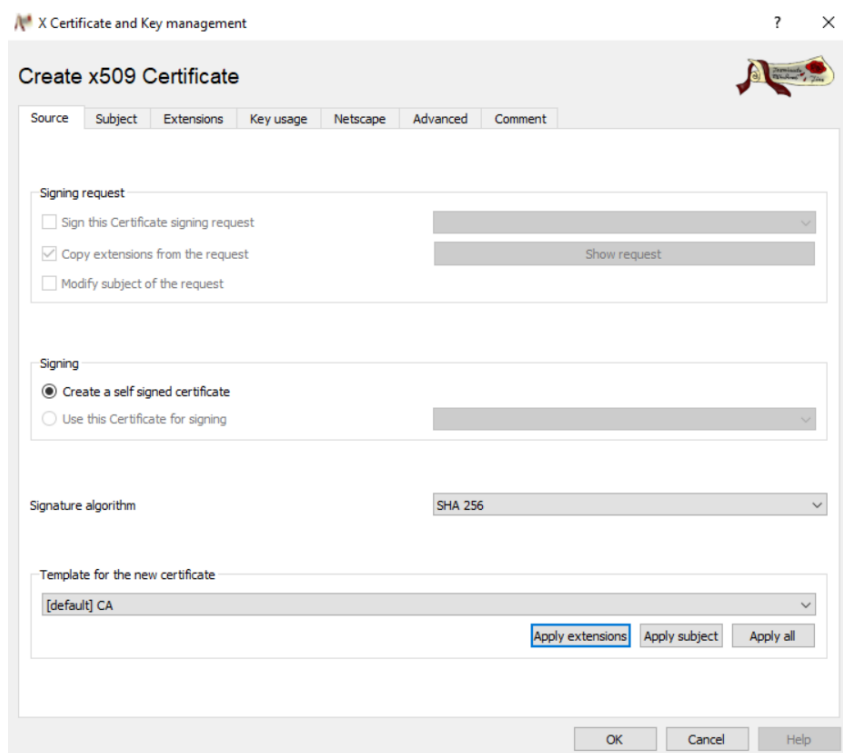


Рис. 1.4 ХСА

В таблиці 1.3 наведено порівняння переваг та недоліків наведених вище служб сертифікації.

Таблиця 1.3 Служби сертифікації

	Переваги	Недоліки
AD CS	- Інтеграція зі структурою Active Directory, що спрощує управління сертифікатами в домені.	- Складність налаштування та конфігурування.
	- Розширена функціональність для різних типів сертифікатів та сертифікаційних політик.	- Вимога до наявності активного домену та ролі AD CS.
	- Підтримка групових політик та спадковості прав доступу.	- Потреба у високопродуктивній та надійній інфраструктурі Active Directory.
Windows Server Certificate Authority	Проста установка та налаштування на серверах Windows.	- Обмежена функціональність порівняно з AD CS.
	- Базова функціональність для видачі сертифікатів та керування ними.	- Не має глибокої інтеграції зі структурою Active Directory.
	- Можливість працювати незалежно від активного домену та AD CS.	- Обмежена підтримка різних типів сертифікатів та політик.

Продовження таблиці 1.3 Служби сертифікації

OpenSSL for Windows	- Криптографічна бібліотека з відкритим вихідним кодом.	- Відсутній графічний інтерфейс, є лише інтерфейс командного рядка.
	- Доступність на платформі Windows та можливість використання для різних криптографічних операцій.	- Вимагає додаткового вивчення та розуміння криптографічних принципів.
	- Гнучкість та можливість налаштування різних аспектів криптографії.	- Відсутність готового веб-інтерфейсу та автоматизованих процесів.
ХСА	- Інтуїтивний графічний інтерфейс для керування сертифікатами.	- Обмежена підтримка розширеної функціональності, порівняно з AD CS або CA.
	- Підтримка різних типів сертифікатів та опцій конфігурування.	- Менш популярне рішення, що може мати обмежену документацію та спільноту.
	- Легке створення та управління сертифікатами на основі власної інфраструктури PKI.	- Вимагає додаткового встановлення та конфігурування.

Отже, порівнявши всі переваги та врахувавши всі недоліки, було обрано Active Directory Certificate Services, так як він має графічний інтерфейс та має найбільшу функціональність.

Висновки до першого розділу

В даному розділі було наведено теоретичні відомості та розглянуто переваги та недоліки власного сервера сертифікації. Також проаналізовано відомості про сертифікат SSL. Порівнювалися декілька методів реалізації служб сертифікації такі як, Active Directory Certificate Services, Windows Server Certificate Authority, OpenSSL for Windows та ХСА. Розглянувши всі переваги та недоліки було обрано Active Directory Certificate Services.

РОЗДІЛ 2. ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ WINDOWS-МЕРЕЖІ НА БАЗІ ДОМЕНУ ACTIVE DIRECTORY

2.1 Створення мережі.

Для створення мережі було використано маршрутизатор, комутатор, два сервера і два робочі станції (рис. 2.1). В таблиці 2.1 показано схему адресації мережі 193.191.3.0/26.

Таблиця 2.1 – Адресація мережі

Мережа/пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска	Префікс
Підмережа А	-	193.191.3.0	255.255.255.192	/26
Маршрутизатор R_191_3_1	Eth0/0	193.191.3.1	255.255.255.192	/26
Комутатор SW-191-3-2	Vlan 1	193.191.3.2	255.255.255.192	/26
Робоча станція Serv_191_3_1	Мережний адаптер	193.191.3.8	255.255.255.192	/26
	Шлюз за замовч.	193.191.3.1	-	-
Робоча станція WS_191_3_1	Мережний адаптер	193.191.3.9	255.255.255.192	/26
	Шлюз за замовч.	193.191.3.1	-	-

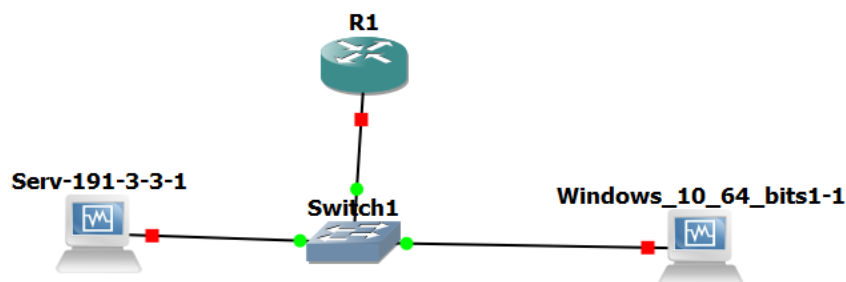


Рис. 2.1 Топологія мережі

У зв'язку ресурсними обмеженнями під час моделювання даної мережі та налаштування у ній сертифікації, у даній кваліфікаційній роботі ми обмежилися моделюванням невеликої частини мережі. За необхідності цю модель може бути розширено для повноцінного використання невеликою організацією за рахунок збільшення кількості проміжних мережних пристроїв та кінцевих вузлів.

2.2 Вибір обладнання для організації роботи мережі

При виборі моделі маршрутизатора потрібно враховувати як він буде працювати в створеній мережі. Маршрутизатор повинен містити достатню кількість портів, забезпечувати легке розширення мережі, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки.

Маршрутизатори Cisco 7200 VXR є найновішими мультисервісними представниками маршрутизаторів серії Cisco 7200 (рис. 2.2). Маршрутизатори Cisco 7200 VXR включають Cisco 7204 VXR (4-слотовий маршрутизатор) і Cisco 7206 VXR (6-слотовий маршрутизатор).



Рис. 2.2 Маршрутизатор Cisco 7200

До переваг модульних маршрутизаторів Cisco 7200 серії можна віднести апаратну підтримку VPN-шифрування (VPN Services Adapter), підтримка інтерфейсів від DS0 до OC-3, а також Fast Ethernet, Gigabit Ethernet, Packet over SONET, надмірність та стійкість до відмов. Також, маршрутизатори Cisco 7200 серії підтримують QoS (quality of service), MPLS, IPSec (до 5000 тунелів на шасі) та передачу голосу, відео та даних.

На рисунку 2.3 показано вид спереду Cisco 7206VXR.

1. Адаптер порту.
2. Адаптери портів
3. Важіль адаптера порту
4. Контролер введення/виведення
5. Слоти ПК Card

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

6. Додатковий інтерфейс Fast Ethernet (порт MII і порт RJ-45)
7. Допоміжний порт
8. Консольний порт

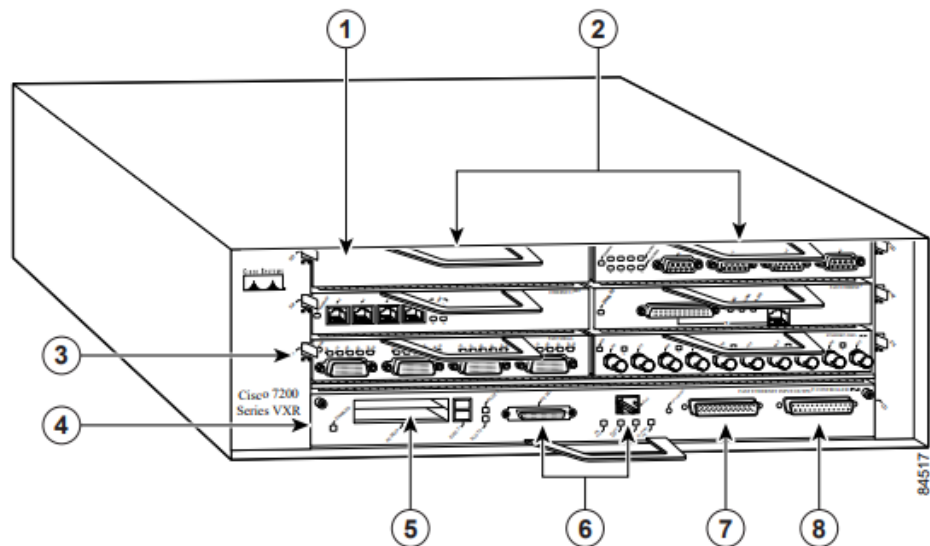


Рис. 2.3 Маршрутизатор Cisco 7200 (вид спереду)

На рисунку 2.4 показано вид ззаду Cisco 7206VXR.

1. Гнізда заземлення шасі
2. Заглушка джерела живлення
3. Вимикач живлення
4. Затиск для кріплення кабелю живлення
5. Внутрішні вентилятори
6. Механізм обробки мережі або механізм мережевих служб
7. Джерело живлення змінного струму
8. Світлодіод PWR OK
9. Гніздо живлення змінного струму

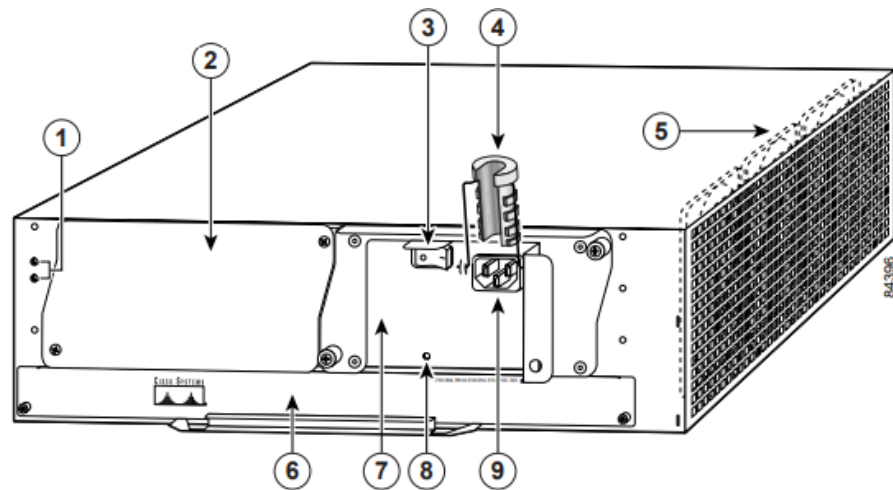


Рис. 2.4 Маршрутизатор Cisco 7200 (вид ззаду)

Ключові особливості:

- Комутатори прості в управлінні і конфігурації;
- Швидкість до 400 к/с при перемиканні CEF;
- Модульність процесора та можливість оновлення;
- Збільшення цінності Cisco 7200.

2.3 Встановлення Windows Server

Засобами гіпервізора VirtualBox створюємо нову віртуальну машину (рис. 2.5).

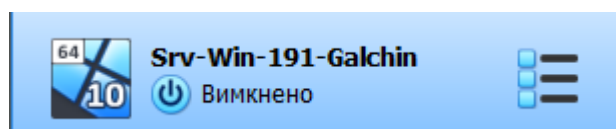


Рис. 2.5. Створення віртуальної машини

Далі підключаємо до створеної віртуальної машини інсталяційний образ ОС Windows Server (iso-файл). Підключення виконуємо на місце віртуального оптичного приводу (рис. 2.6).

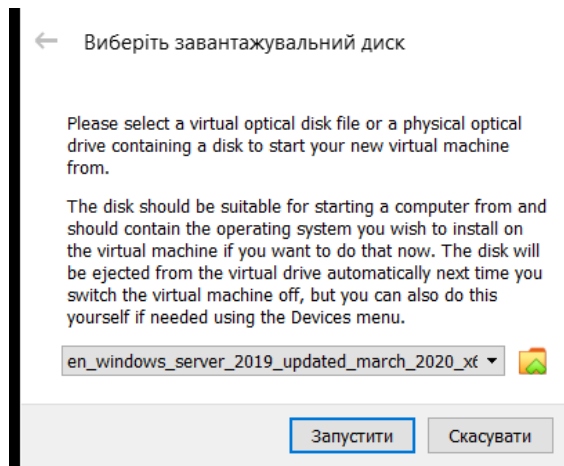


Рис. 2.6. Підключення інсталяційного образу

Виконайте встановлення ОС Windows Server на створену віртуальну машину.

- Редакція - Windows Server 2019 Standard (Desktop Experience)
- Тип інсталяції - Custom
- Пароль для адміністратора – на свій вибір

Від'єднуємо інсталяційний образ (iso-файл) від віртуального оптичного приводу віртуальної машини (рис. 2.7).

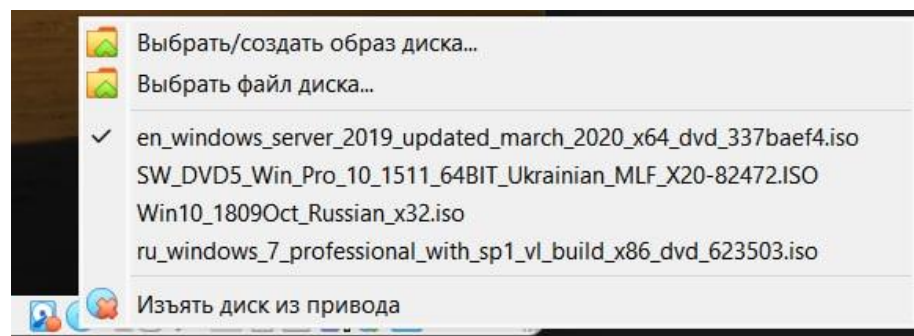


Рис. 2.7 Від'єднання інсталяційного образу

Після завершення встановлення переконаймося у працездатності системи (рис 2.8).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

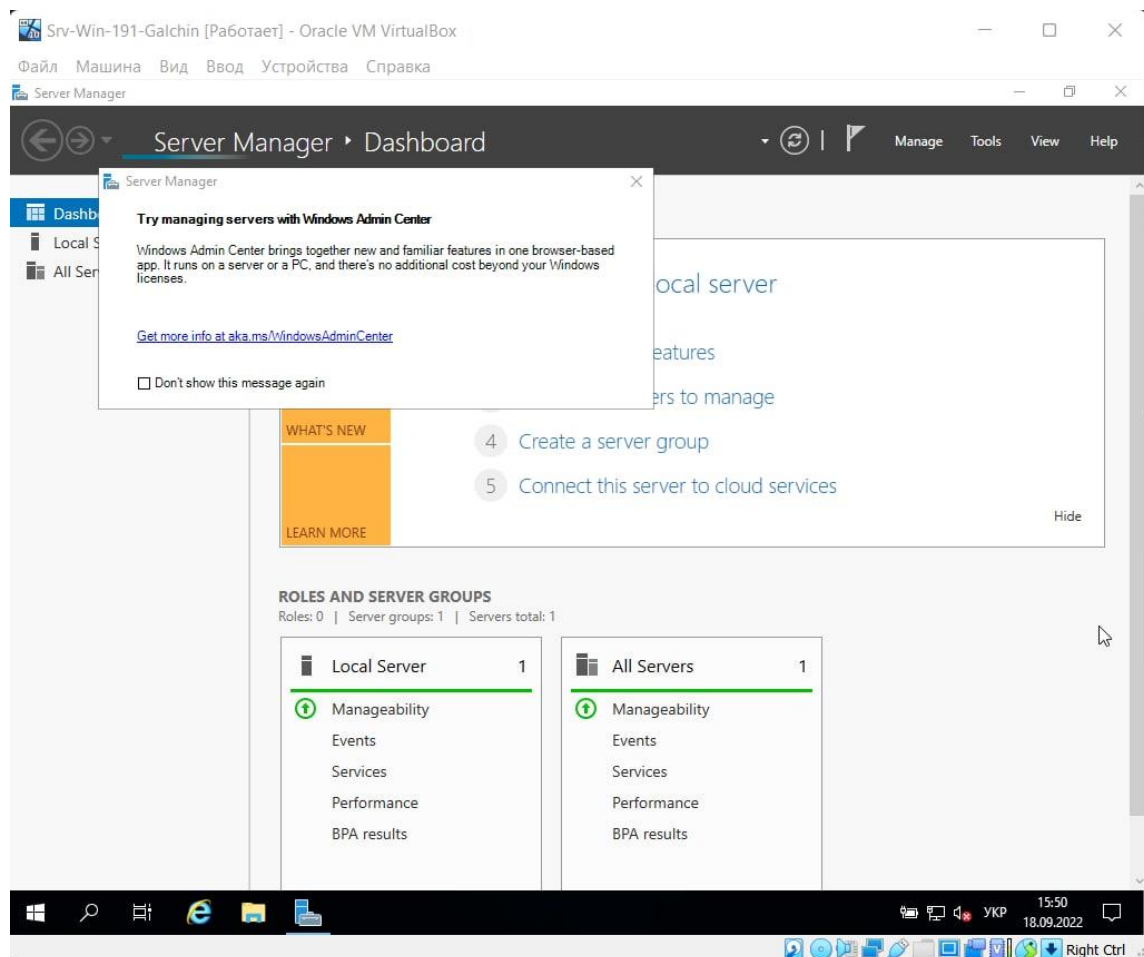


Рис. 2.8 Перевірка роботи

2.4 Базове налаштування Active Directory

Далі виконуємо налаштування Active Directory. Спочатку додаємо ролі служб (рис. 2.9).

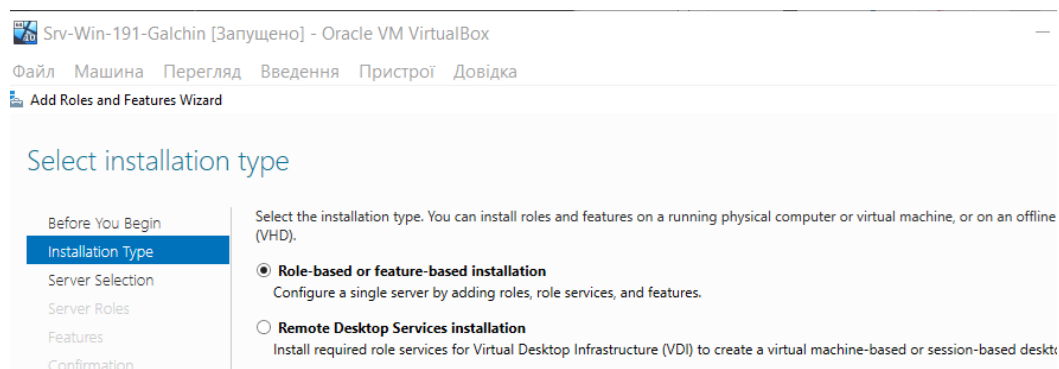


Рис. 2.9 Встановлення на основі ролей або функцій

Потім потрібно обрати сервер, на якому будемо додавати ролі (рис. 2.10).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

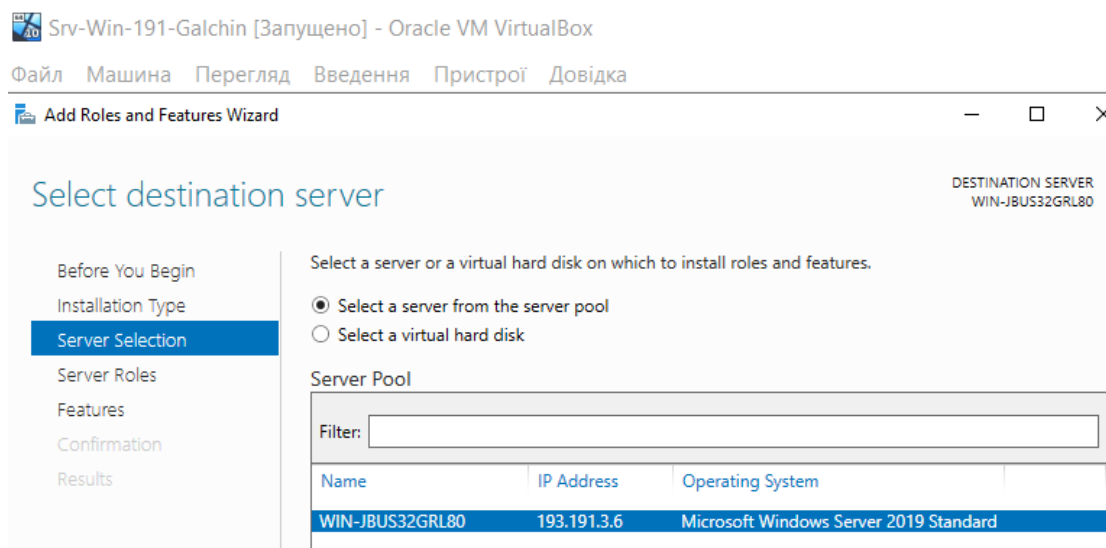


Рис. 2.10 Вибираємо потрібний сервер

Далі вибираємо, які доменні служби потрібно завантажити (рис. 2.11).

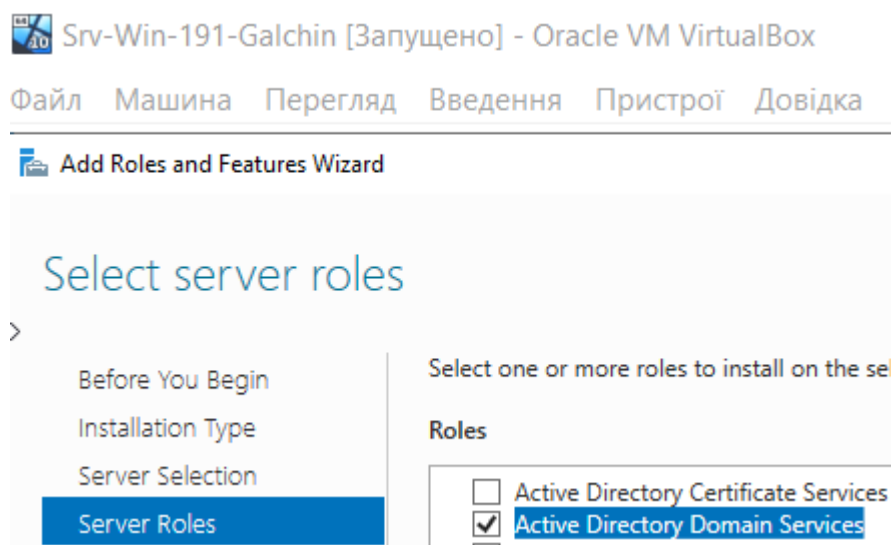


Рис. 2.11 Завантажуємо доменні служби Active Directory

На рис. 2.12 можна спостерігати процес встановлення.

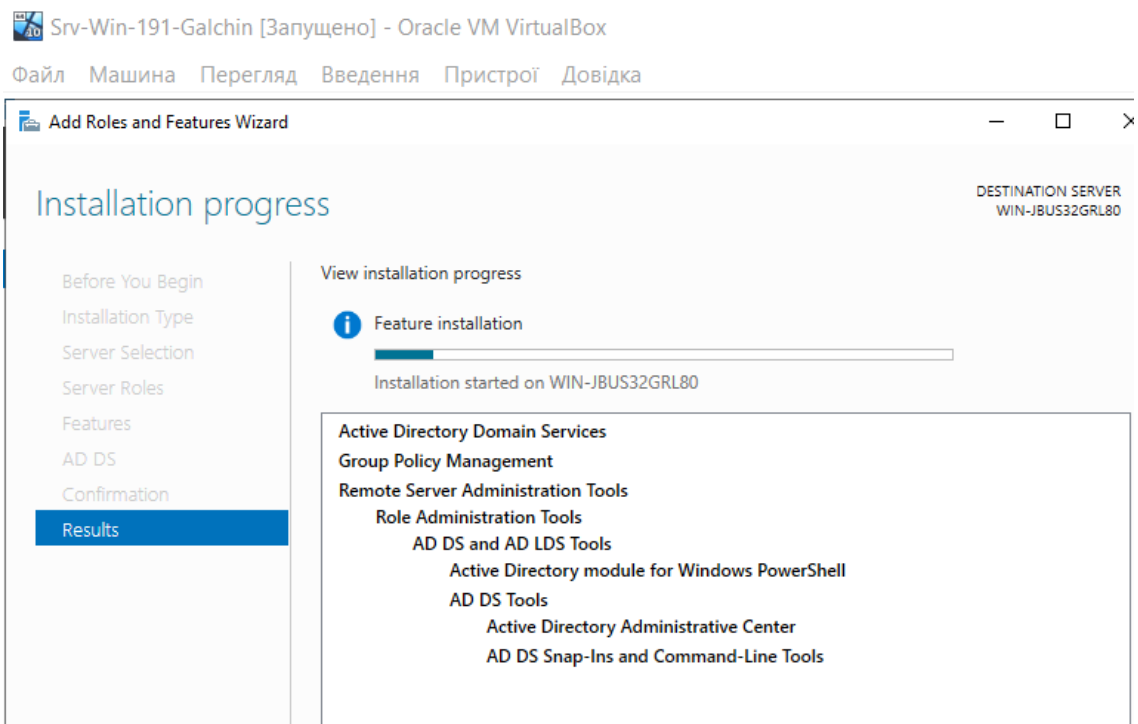


Рис. 2.12 Завантаження

Після встановлення потрібно створити новий ліс та призначити ім'я кореневому домену (рис. 2.13).

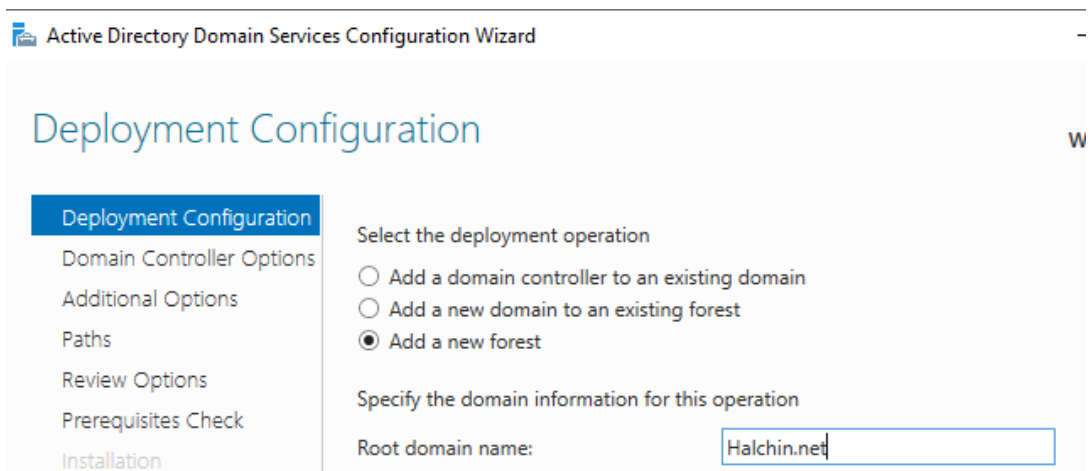


Рис. 2.13 Створення нового лісу та призначаємо ім'я кореневому домену
Далі на (рис. 2.14) показано налаштування паролю для входу до сервера.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

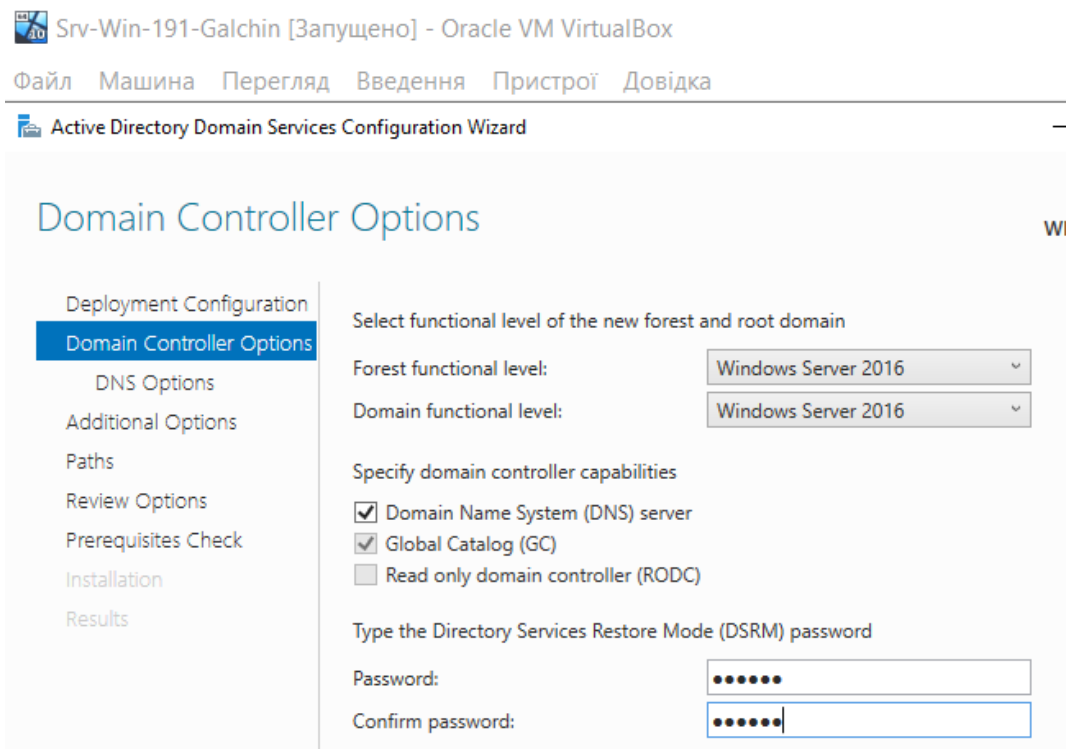


Рис. 2.14 Налаштовуємо пароль для входу в сервер

Продовжуємо налаштування сервера. Для цього призначаємо ім'я кореневому домену (рис. 2.15) та вибираємо шлях папку, де будуть зберігатися база даних Active Directory (рис. 2.16).

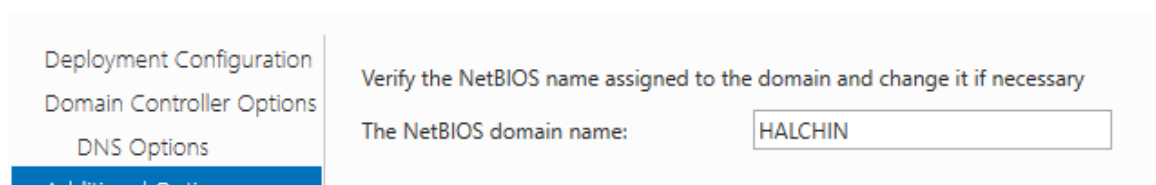


Рисунок 2.15 — Призначаємо ім'я кореневому домену

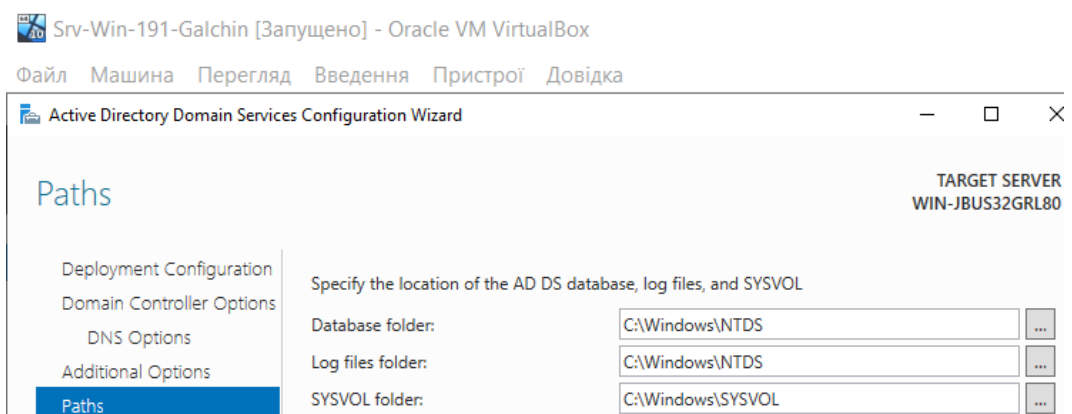


Рис. 2.16 Вибираємо шлях

На цьому базові налаштування сервера завершено. На рис. 2.17 можна побачити успішне встановлення всіх налаштувань.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

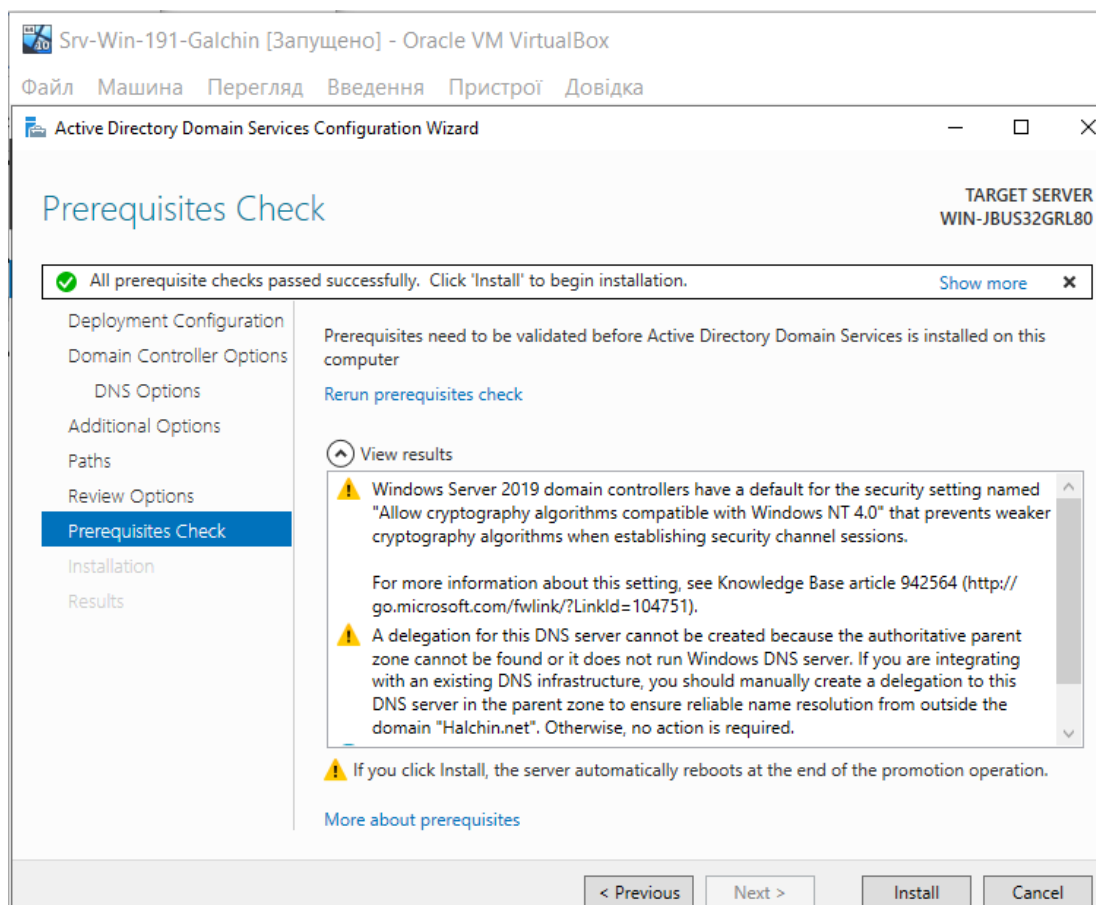


Рис. 2.17 Завершення інсталювання

Далі потрібно виконати встановлення роль DNS-сервера в Active Directory. Зазвичай ця роль вже є встановлена. Для початку у вікні Server Manager на панелі Dashboard обераємо опцію 2 Add roles and features (рис. 2.18).

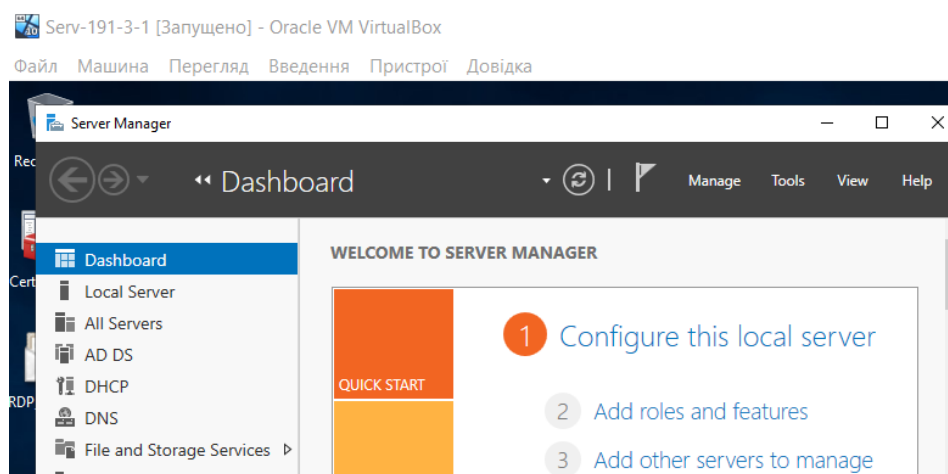


Рис. 2.18 Add roles and features

Потім було обрано опцію Role-based or feature-based installation (рис. 2.19).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

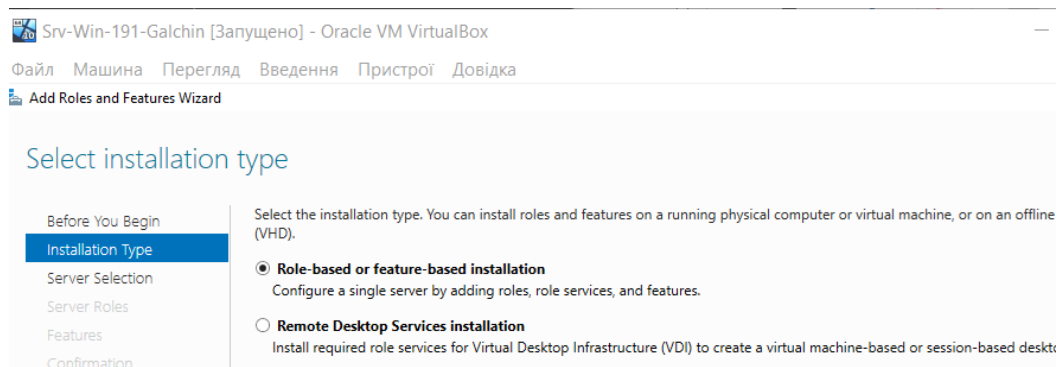


Рис. 2.19 Встановлення на основі ролей або функцій

Вказуємо сервер домену, на якому необхідно встановити роль DNS-сервера. На рис. 2.16 це основний контролер домену.

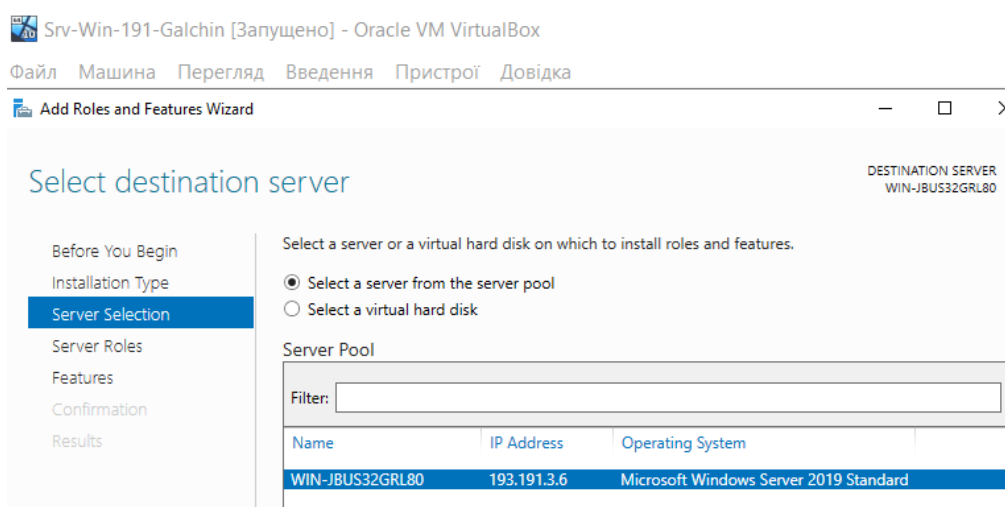


Рис. 2.20 Вибираємо потрібний сервер

Виберемо роль, яку необхідно встановити (у цьому випадку роль DNS Server). Якщо роль вже встановлено, опцію буде вибрано та деактивовано, як на рис. 2.21. В іншому випадку встановіть прапорець поруч з опцією.

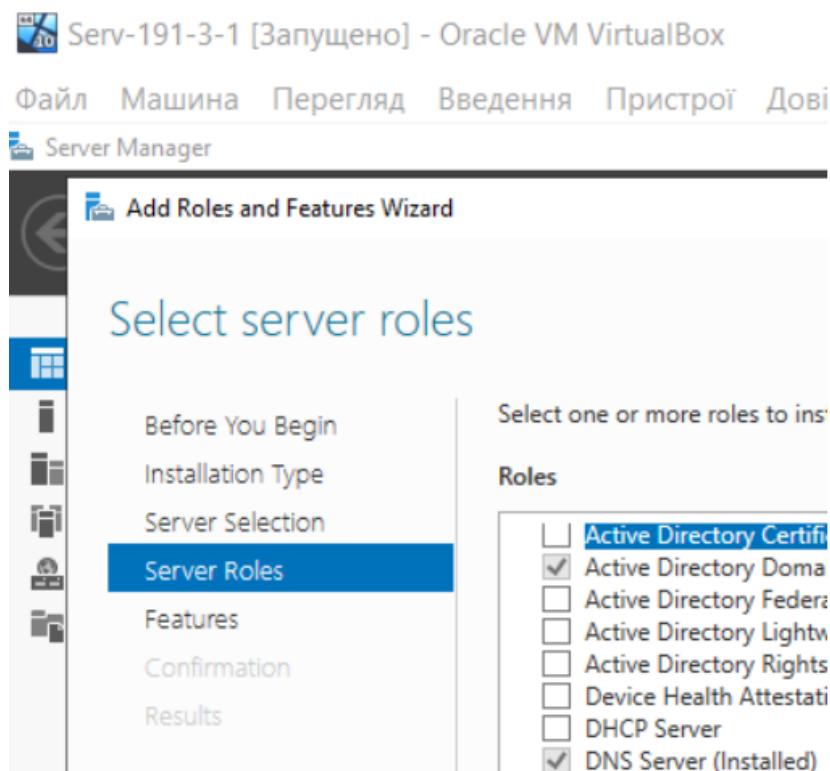


Рис. 2.21 DNS Server

Далі потрібно створити зону зворотного перегляду. Вона використовується для перетворення IP-адреси у доменне ім'я (с IP-адреса - за нею треба одержати доменне ім'я), це може знадобитися для коректної роботи окремих служб. Розглянемо приклад створення зони зворотного перегляду у домені Halchin.net.

За допомогою оснащення DNS Manager переконаймося, що зону зворотного перегляду ще не створено (рис. 2.22).

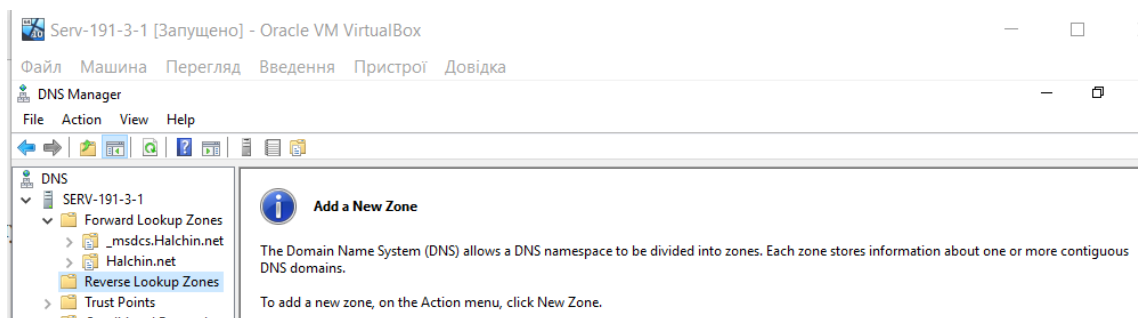


Рис. 2.22 Зона зворотного перегляду

Створюємо зону зворотного перегляду на DNS-сервері, що працює на основному контролері домену. Для цього запускаємо майстер створення нової зони (рис. 2.23).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				29
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 2.23 Майстер створення нової зони

На DNS-сервері основного контролера домену створюємо зону зворотного пошуку.

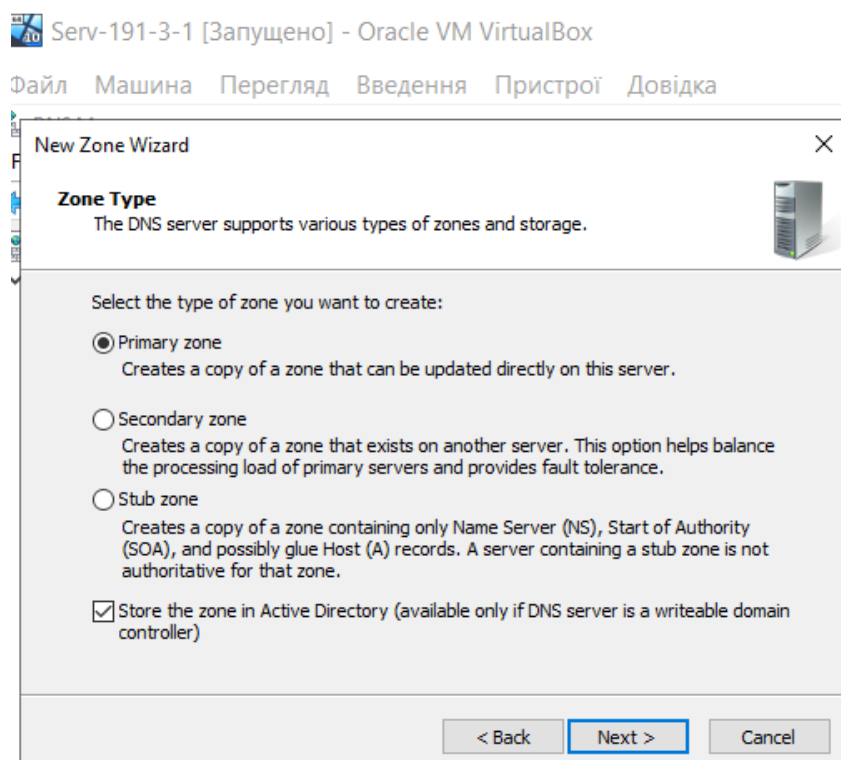


Рис. 2.24 Створення зони зворотного перегляду

Щоб створити зону DNS, спочатку оберемо відповідну зону реплікації. У цьому випадку бажаним варіантом є «До всіх DNS-серверів, які працюють на контролерах домену в цьому домені...». Це означає, що будь-які дані в цій

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

зоні DNS дублюватимуться на всіх DNS-серверах, розташованих на контролерах домену, як показано на малюнку 2.25.

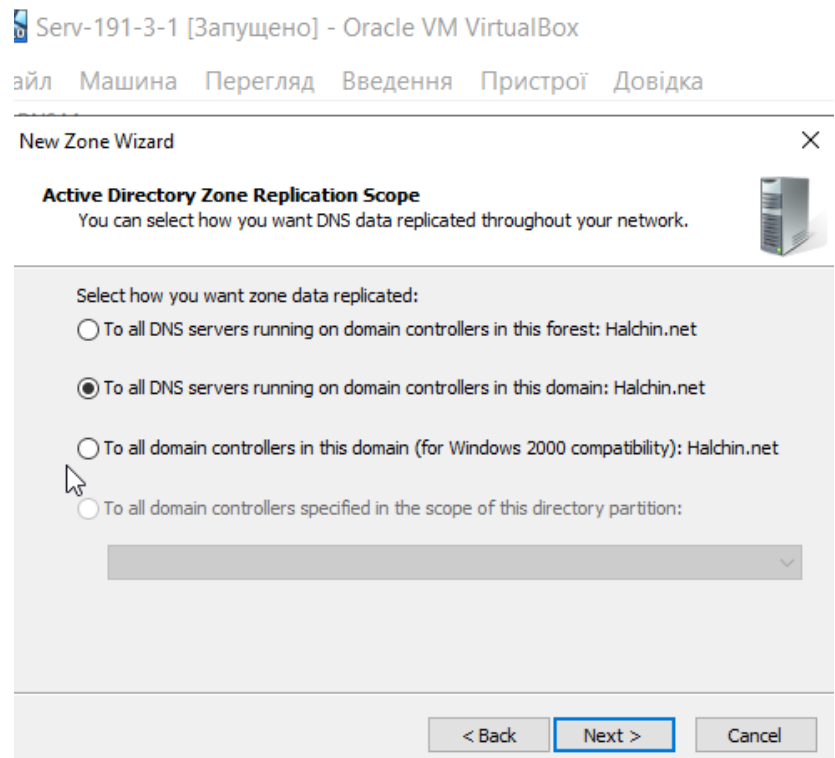


Рис. 2.25 Створення зони зворотного перегляду

Можна призначити область для зворотного перегляду, вказавши мережеву адресу або безпосередньо вказавши назву зони зворотного перегляду. На рис. 2.26, введення адреси мережі призведе до автоматичної генерації назви для зони зворотного огляду. Це ім'я з'явиться в неактивному полі внизу вікна як «3.191.193.in-addr.arpa».

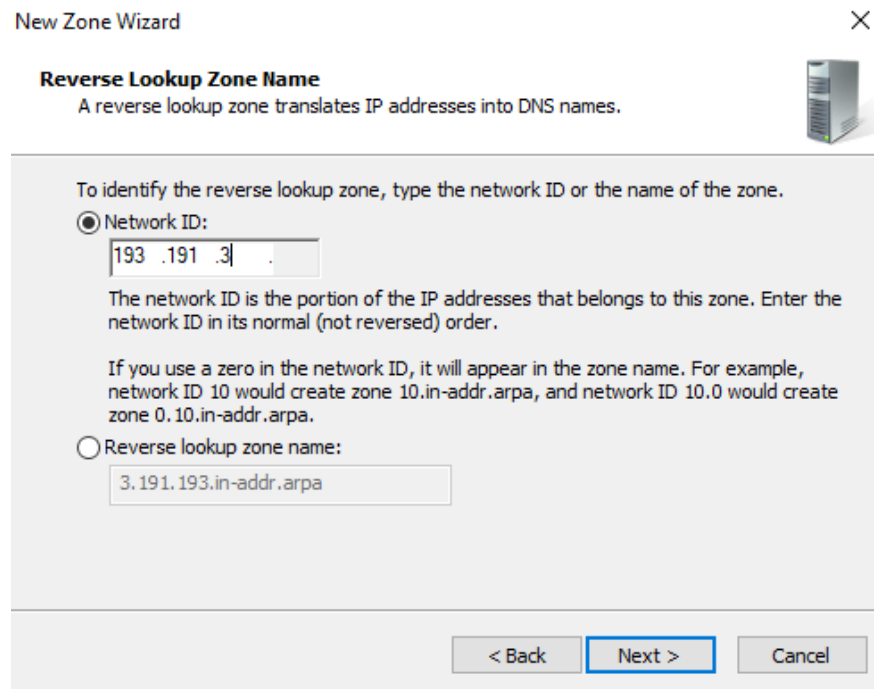


Рис. 2.26 Створення зони зворотного перегляду

На рис. 2.27 показано закінчення створення зворотного перегляду.

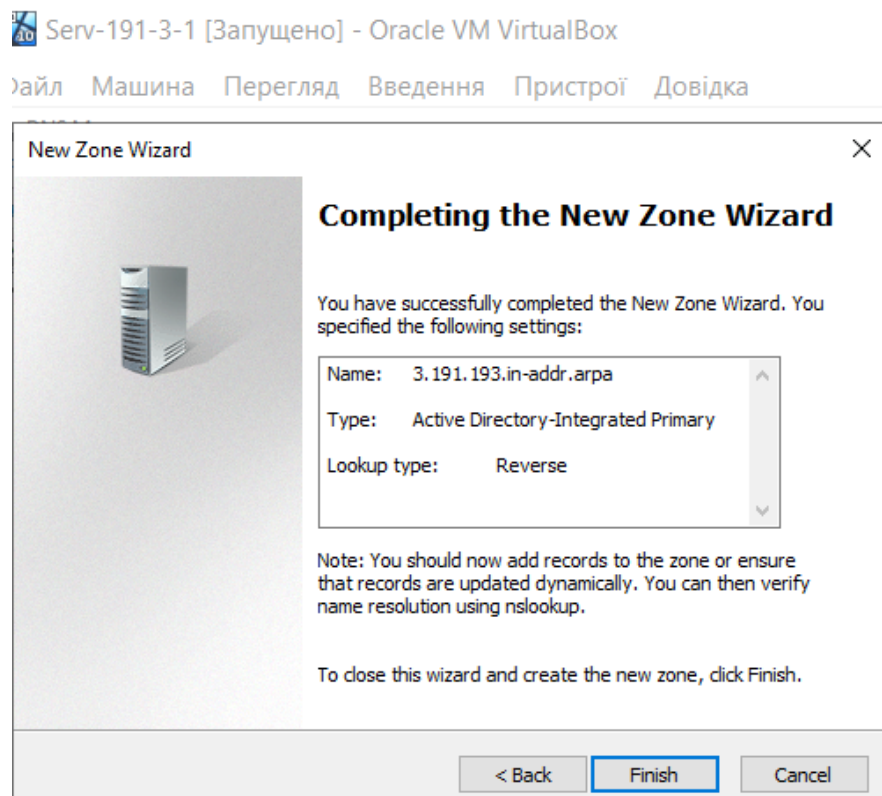


Рис. 2.27 Створення зони зворотного перегляду

Перевіримо ефективність виконаних налаштувань. Для цього ввійдемо в систему на одній з робочих станцій домену і введемо команду nslookup, у ролі аргумента вказавши IP-адресу контролера домена, на якому

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

налаштовували DNS-сервер. Якщо параметри налаштовано правильно, результат команди nslookup має нагадувати приклад на рис. 2.28. Це означає, що сервер DNS надав інформацію про себе.

```
C:\Users\dep3-kik>nslookup 193.191.3.6
Name:      Serv-191-3-1.Halchin.net
Address:   193.191.3.6
```

Рис. 2.28 nslookup

Відомості про оренду адреси, виділеної цій робочій станції, мають відображатися на DHCP-сервері в оснащенні DHCP, вузол Address Leases (рис. 2.29).

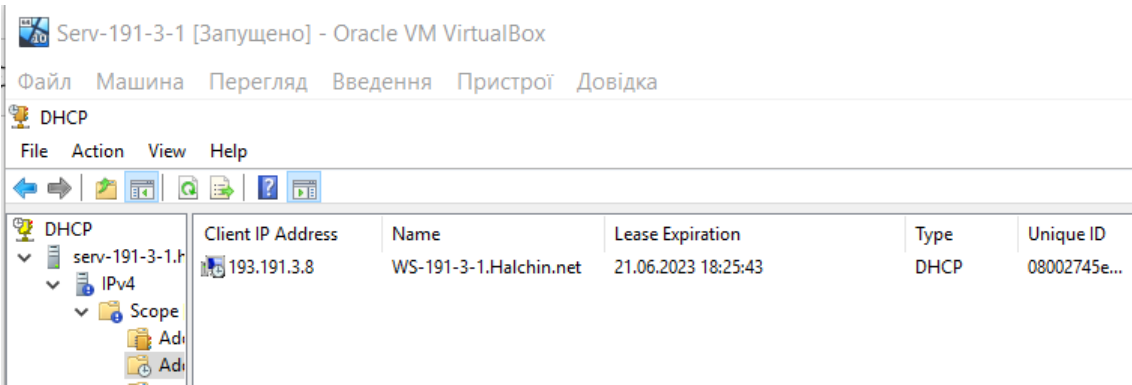


Рис. 2.29 Відомості про оренду адреси

Також потрібно додати ще одну важливу службу віддаленого робочого стола. Для цього у вікні Manage виберемо Add Roles and Features (рис.2.30).

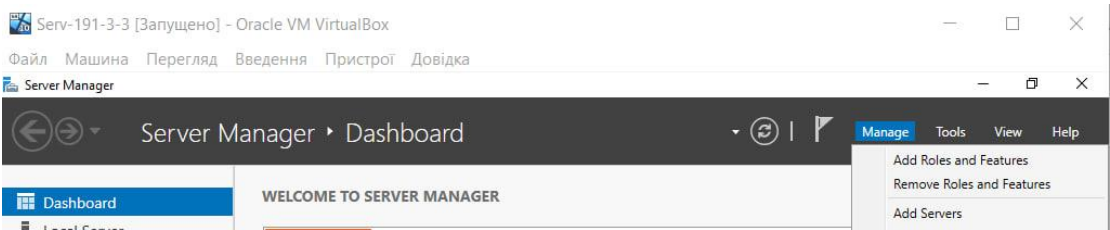


Рис. 2.30 Add Roles and Features

Далі потрібно вибрати Remote Desktop Services Installation оскільки, саме цей пункт дозволяє налаштувати служби віддаленого робочого столу як на основі сесій віддаленого робочого столу, так і на основі віртуальних машин (рис. 2.31).

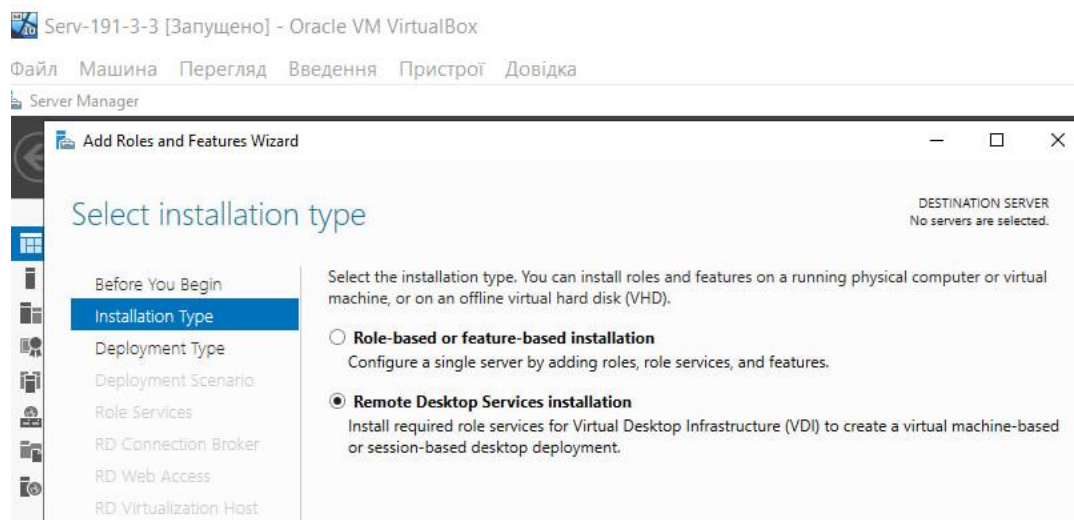


Рис. 2.31 Remote Desktop Services Installation

Далі обираємо опцію стандартного розгортання (рис. 2.32).

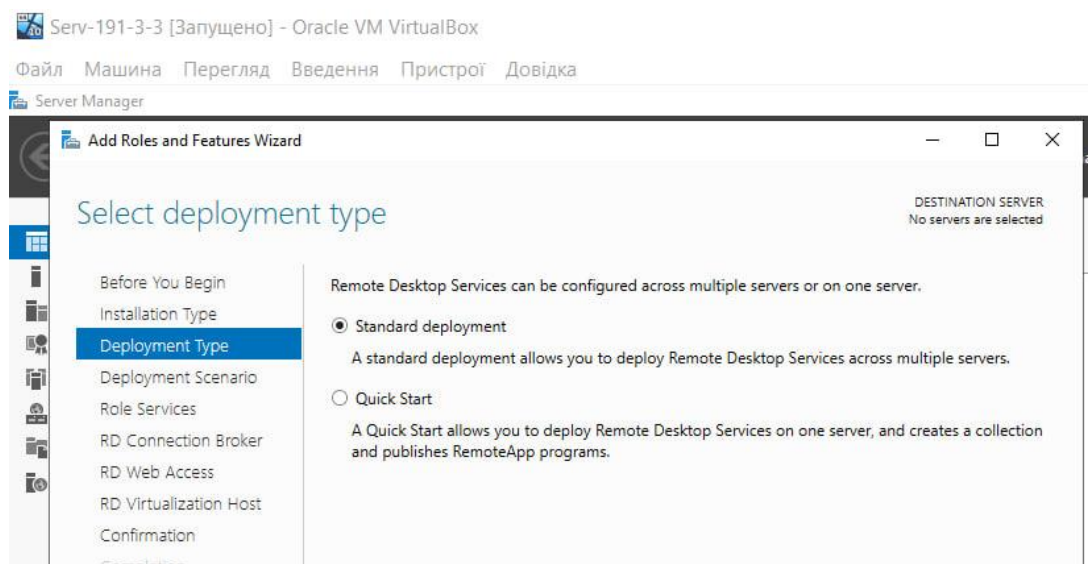


Рис. 2.32 Стандартне розгортання

Для наступного кроку рекомендується вибрати план розгортання. Найкраще обрати є служби віддаленого робочого столу, які базуються на віддалених сесіях, як показано на рис. 2.33. Використовуючи цей метод, ресурси, необхідні для роботи сценарію, помітно зменшуються.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

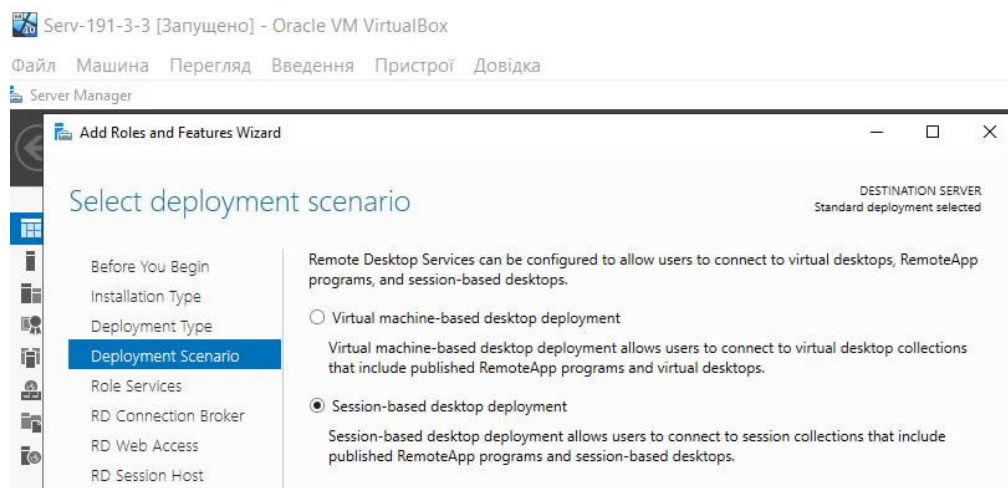


Рис. 2.33 Служби віддаленого столу на основі віддалених сесій

Після цього з'явиться вікно майстра з переліком служб, які будуть встановлені на наступних кроках (рис. 2.34). Преглянемо список, а потім натиснемо «Далі».

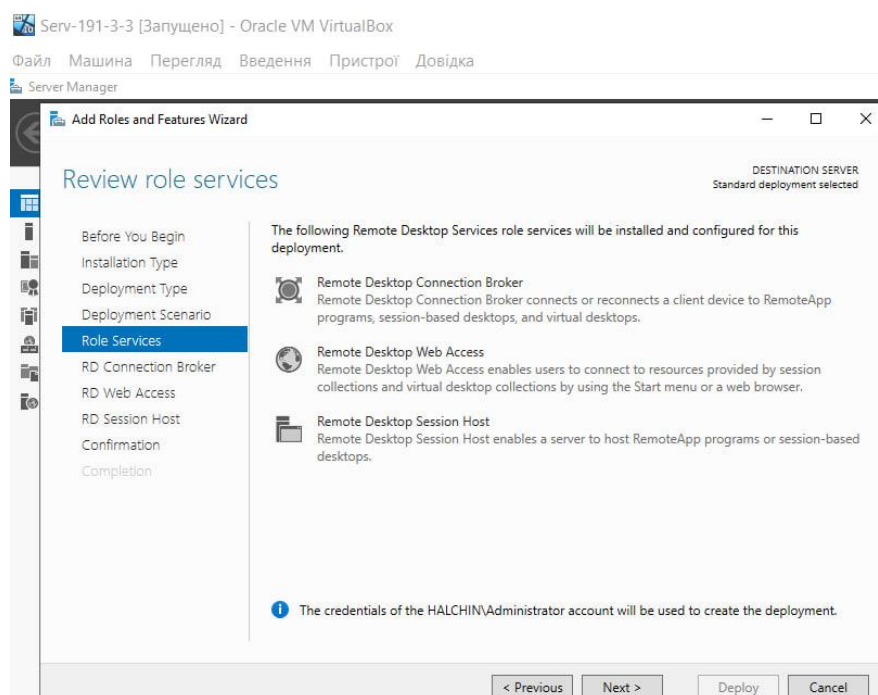


Рис. 2.34 Перелік служб

Наступним кроком є вибір серверів з наявного пулу, на які будуть встановлені обрані служби. У цьому випадку ми обираємо перший контролер домену згідно з рис. 2.35 для встановлення RD Connection Broker. Цей сервер виконує ряд важливих функцій для керування підключеннями до віддалених робочих столів.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

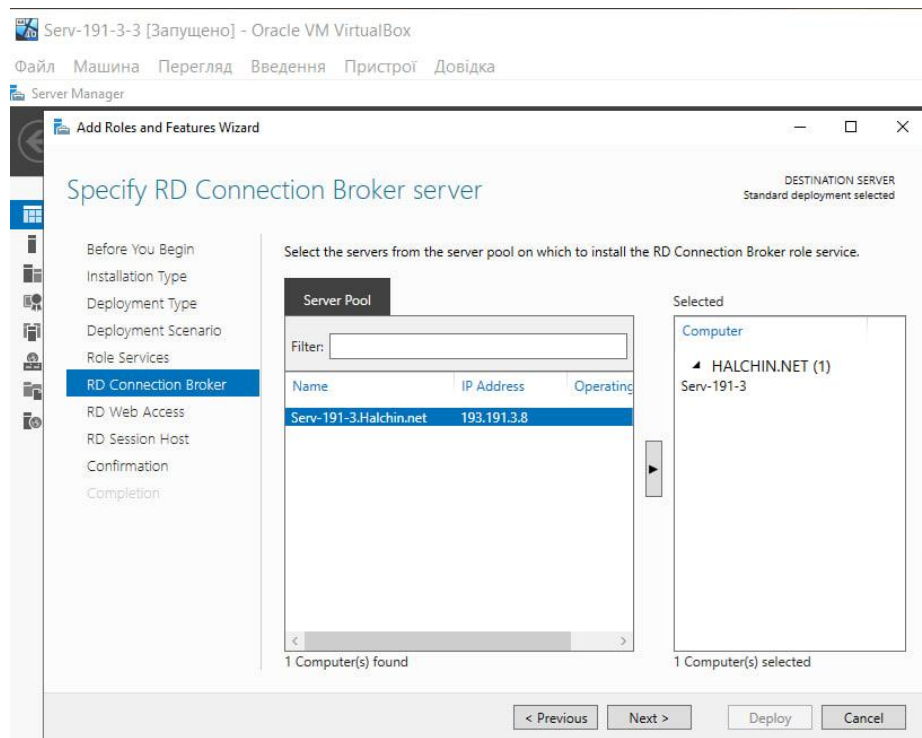


Рис. 2.35 RD Connection Broker

На рис. 2.36 показано, що той самий сервер обрано для компонента RD Web Access (надає можливість користувачам отримувати доступ до віддалених робочих столів та програм через веб-браузер).

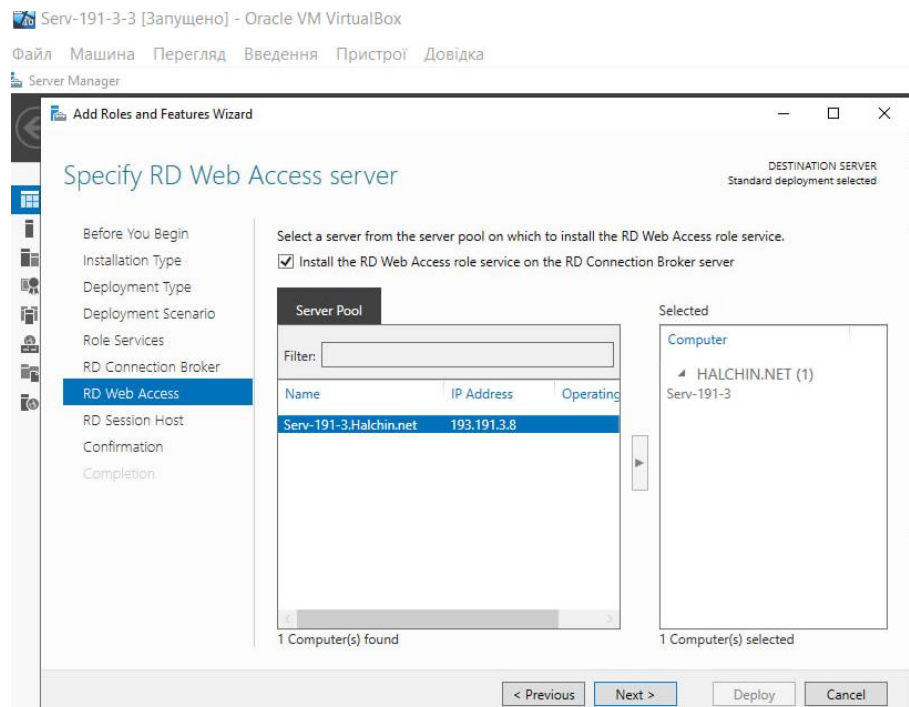


Рис. 2.36 RD Web Access

І нарешті, той самий сервер обрано для RD Session Host (рис.2.37).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

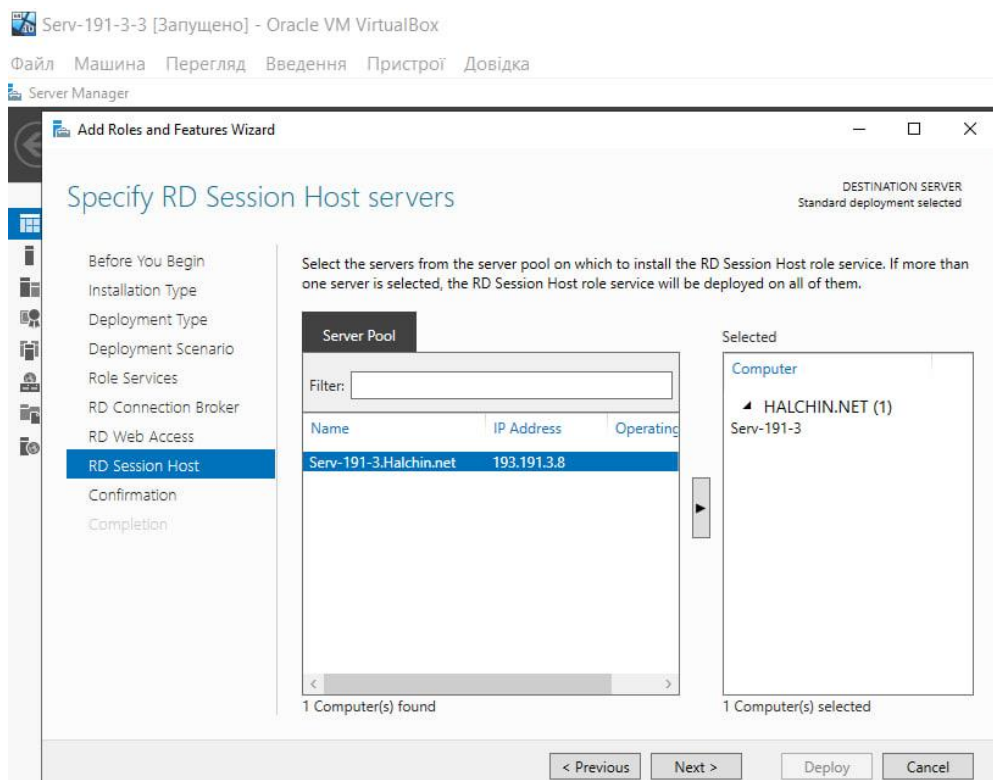


Рис. 2.37 RD Session Host

Підготовку завершено і тепер можна розпочинати процес встановлення. Рекомендується встановити прапорець, який вказує на необхідність перезавантаження системи, згідно з рис. 2.38.

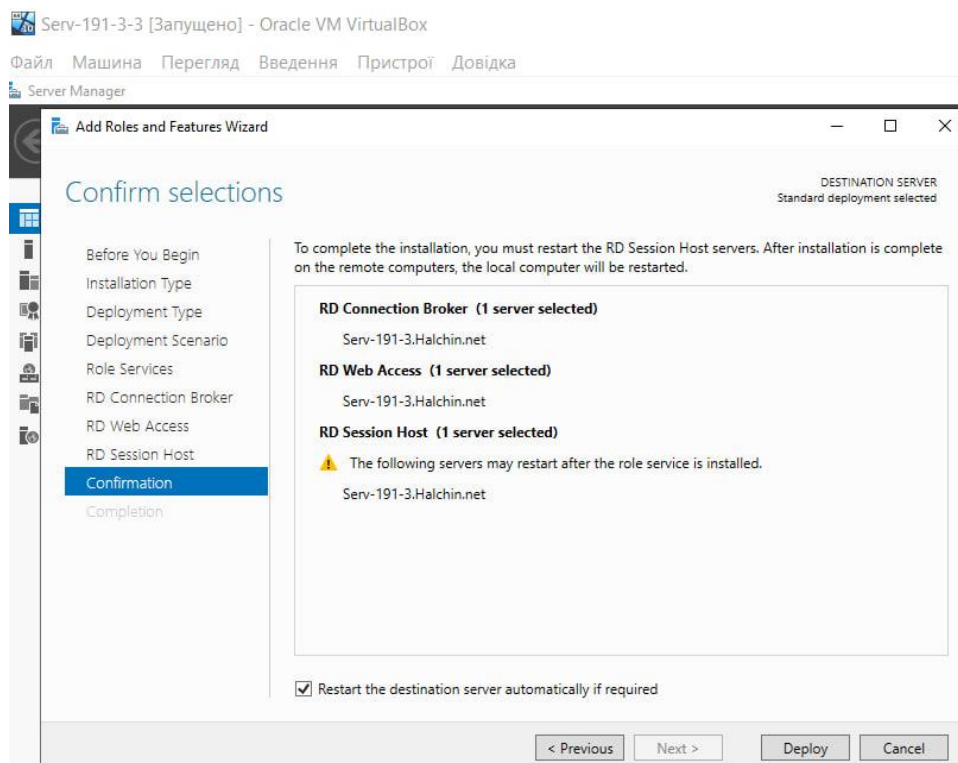


Рис. 2.38 Підготовка встановлення

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Процес встановлення може зайняти деякий час. Після успішного завершення вікно майстра виглядатиме подібно до зображеного (рис. 2.39).

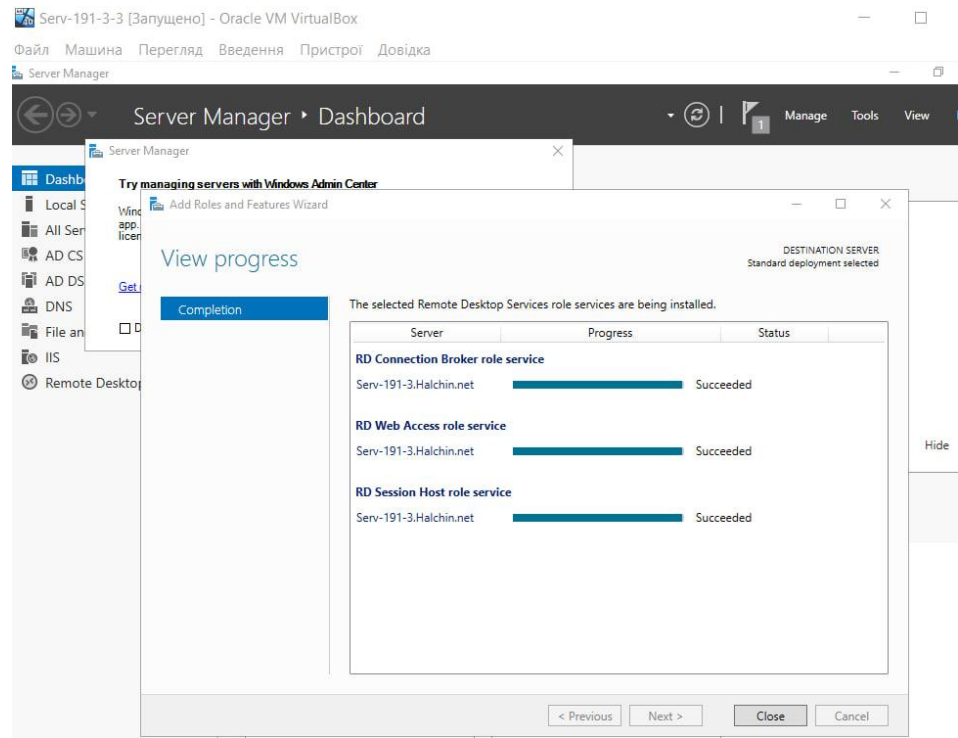


Рис. 2.39 Успішне встановлення

Встановлення необхідних компонентів завершено, а відповідна група опцій з'явилися у вікні Server Manager (рис. 2.40).

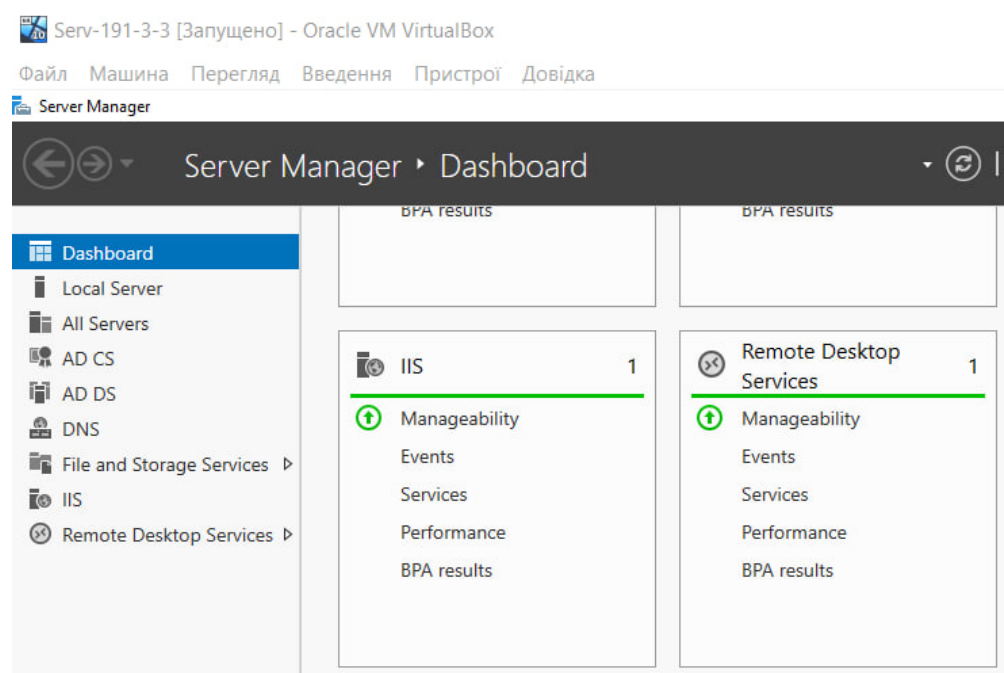


Рис. 2.40 Remote Desktop Services

Тепер додамо до новоствореної колекції програми (рис. 2.41).

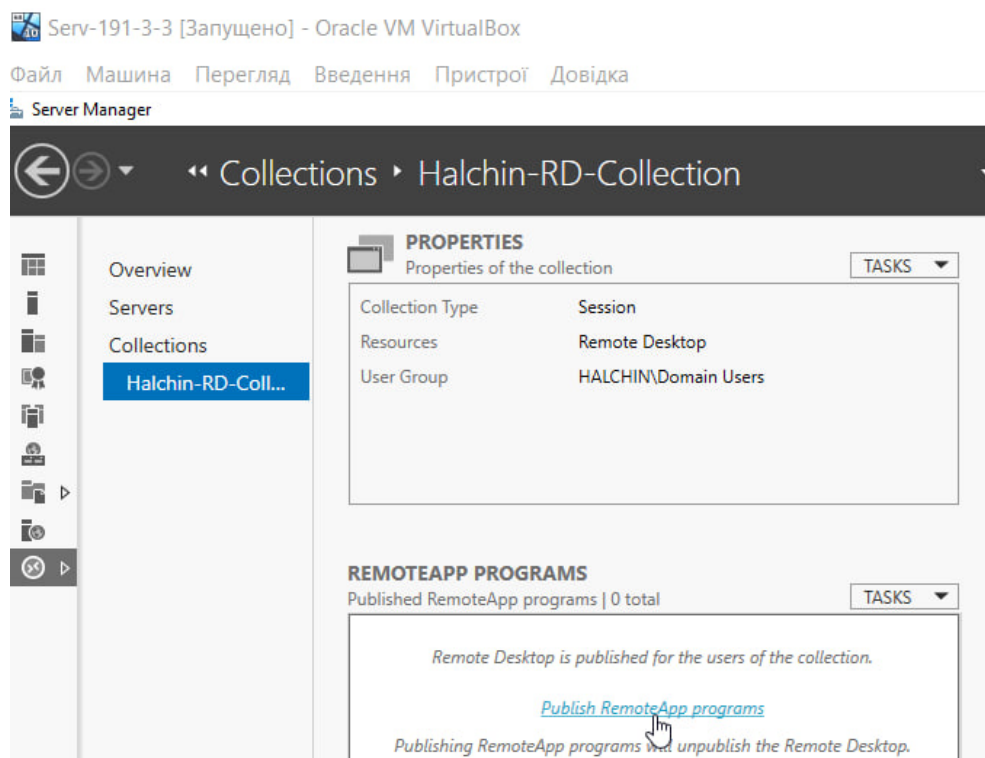


Рис. 2.41 Програми віддаленого доступу

Обираємо Active Directory Module for Windows Powershell, для змоги керування Active Directory за допомогою команд та натискаємо Publish (рис. 2.42).

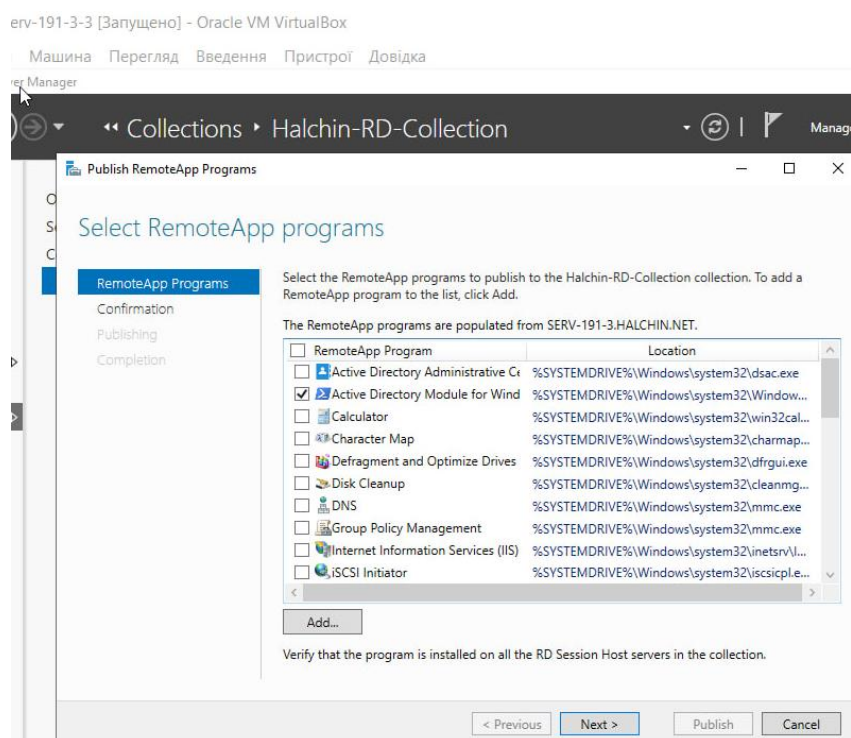


Рис. 2.42 Вибір програм

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

На рис. 2.43 показано вибрану програму, для завершення натисніть Publish.

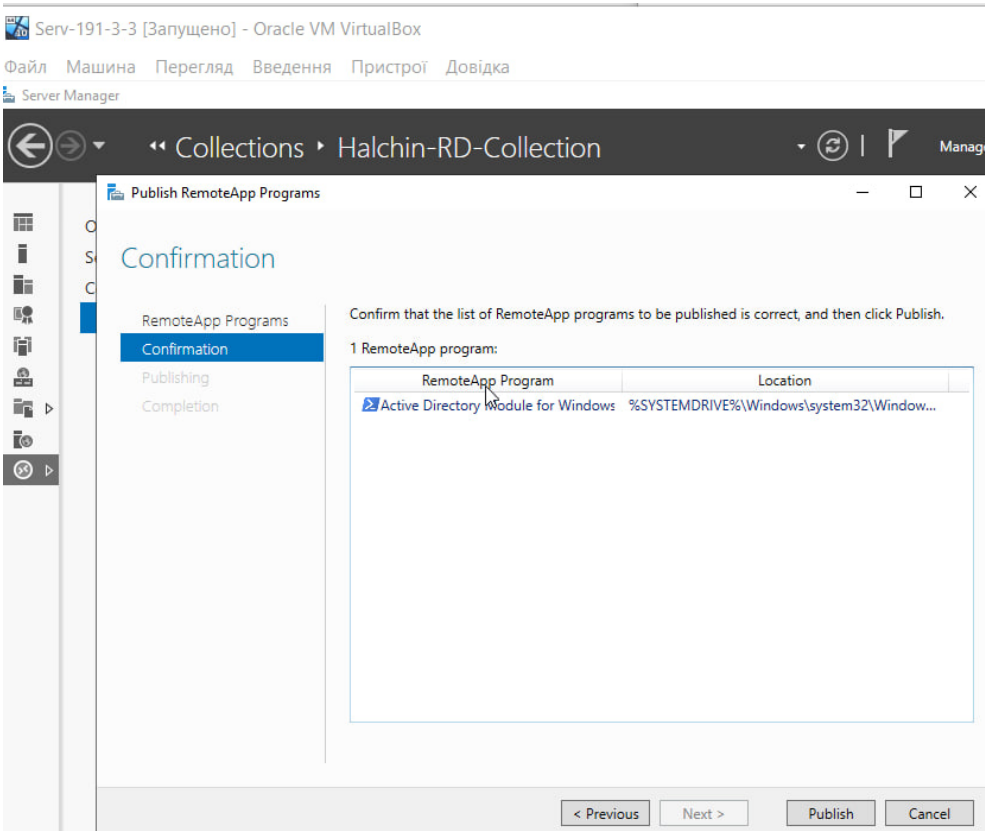


Рис. 2.43 Успішне додавання програм

Висновки до другого розділу

В даному розділі було покроково описано процес встановлення Windows Server, а також показано базові налаштування Active Directory. Зокрема Active Directory Domain Services, DNS Server, Remote Desktop Services.

РОЗДІЛ 3. СТВОРЕННЯ, НАЛАШТУВАННЯ ТА ПЕРЕВІРКА РОБОТИ СЕРВЕРА СЕРТИФІКАЦІЇ

3.1 Встановлення та налаштування сервера сертифікації

Для початку потрібно додати відповідну роль. У вікні Server Manager оберіть Manage → Add Roles and Features (рис. 3.1)^[8].

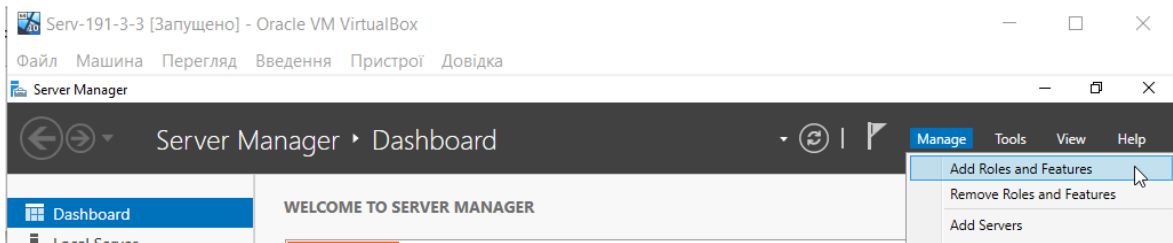


Рис. 3.1 Add Roles and Features

Встановлюємо прапорець навпроти ролі Active Directory Certificate Services (рис. 3.2).

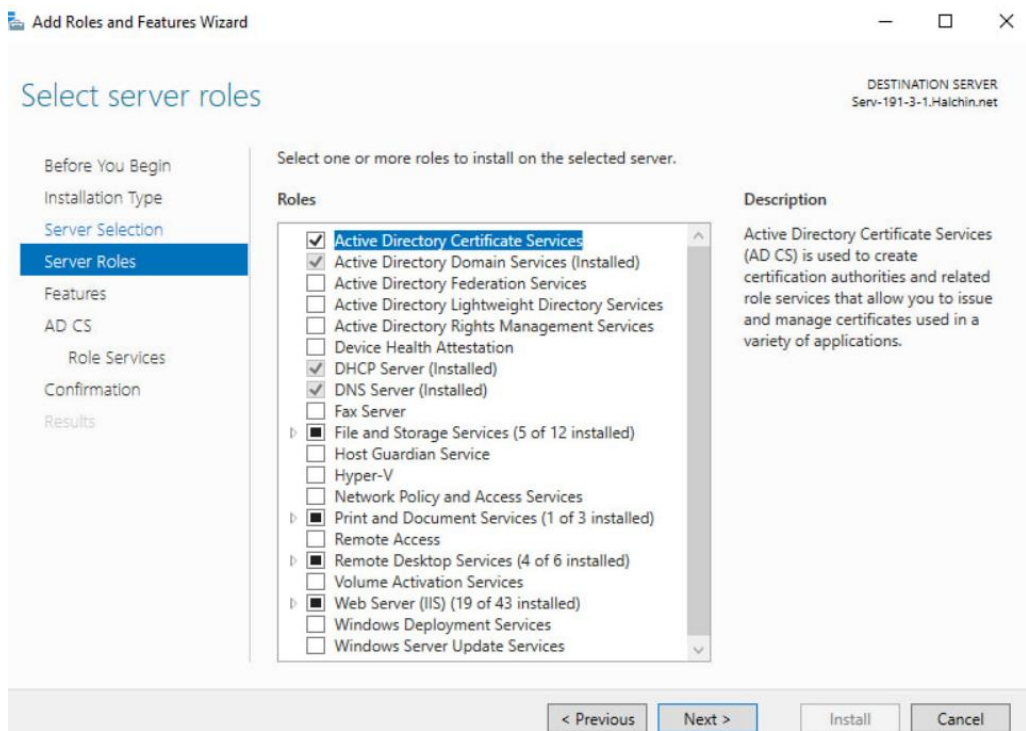


Рис. 3.2 Active Directory Certificate Services

Підтверджуємо зроблені налаштування (рис. 3.3).

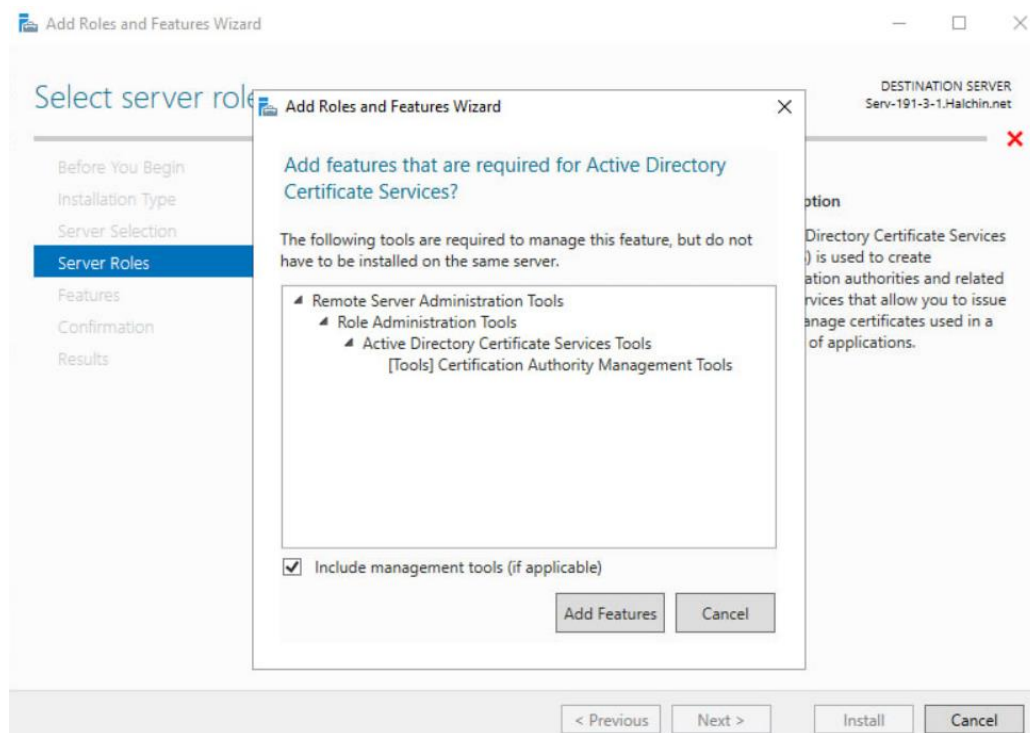


Рис. 3.3 Налаштування

Нових компонентів на даному етапі встановлювати не потрібно (рис. 3.4).

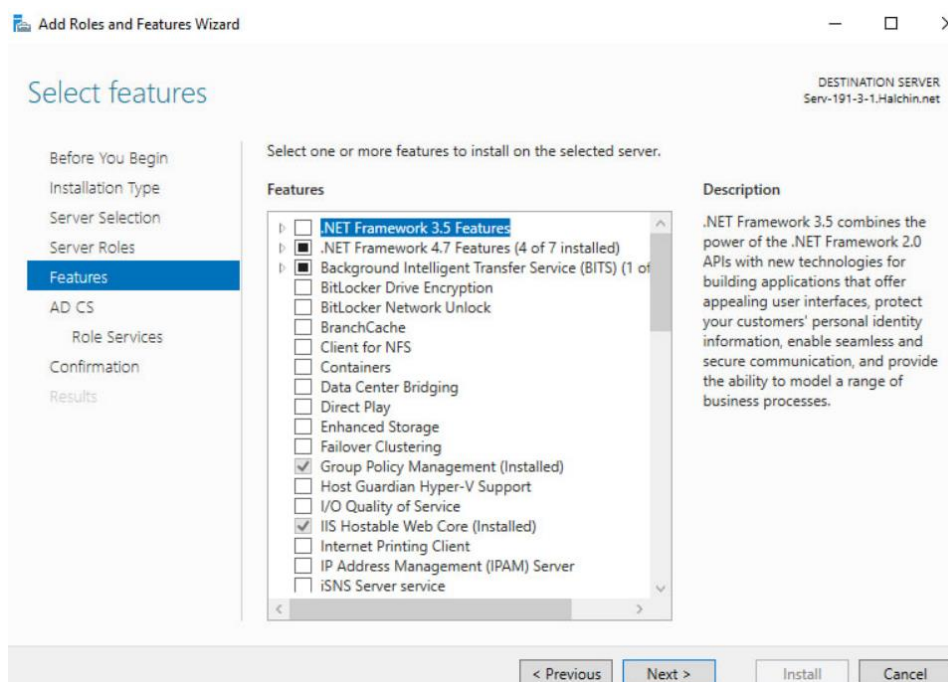


Рис. 3.4 Додаткові компоненти

Важливо врахувати, що після завантаження неможливо буде змінити ім'я домену. Тому якщо потрібно задати інше ім'я, необхідно зробити це до завантаження (рис. 3.5).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

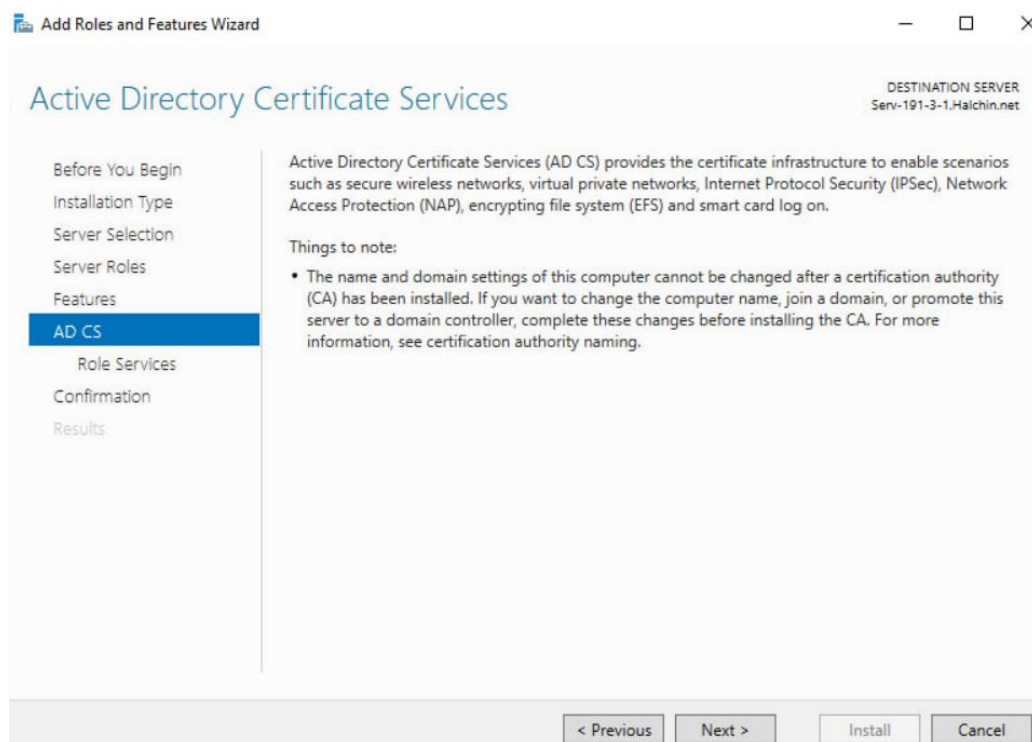


Рис. 3.5 Зміна доменного імені

Далі вибираємо ролі, як показано на рис. 3.6.

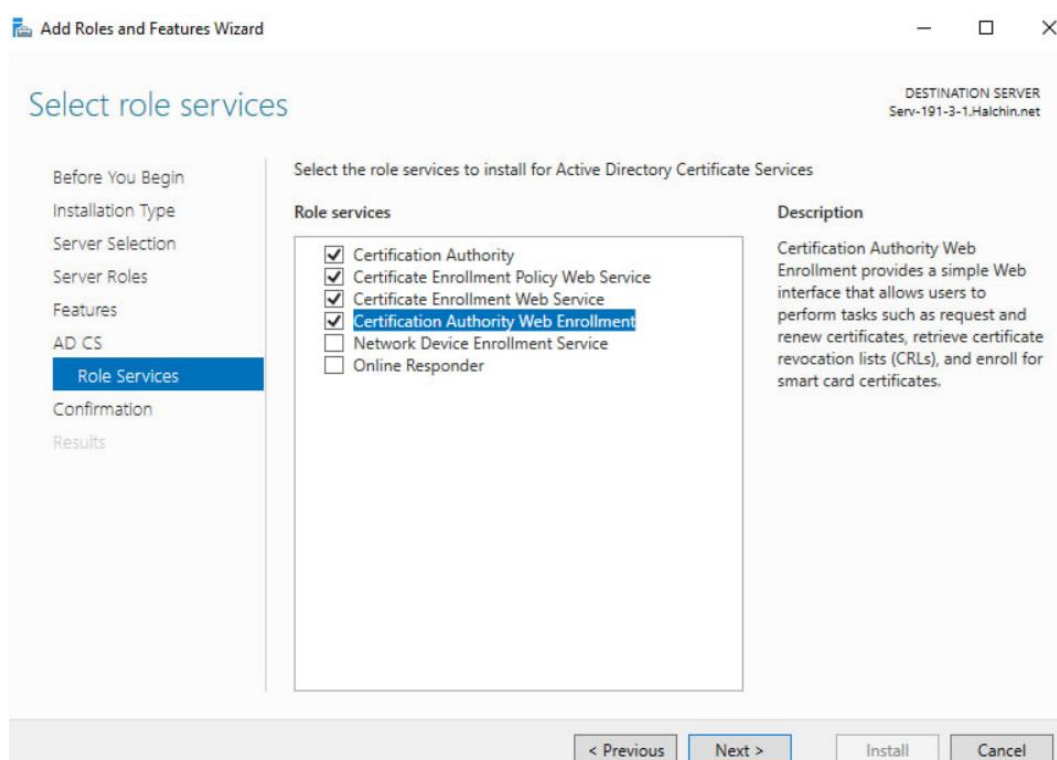


Рис. 3.6 Ролі сервера для встановлення

Перевіряємо вибрані налаштування та натискаємо Install (рис. 3.7).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

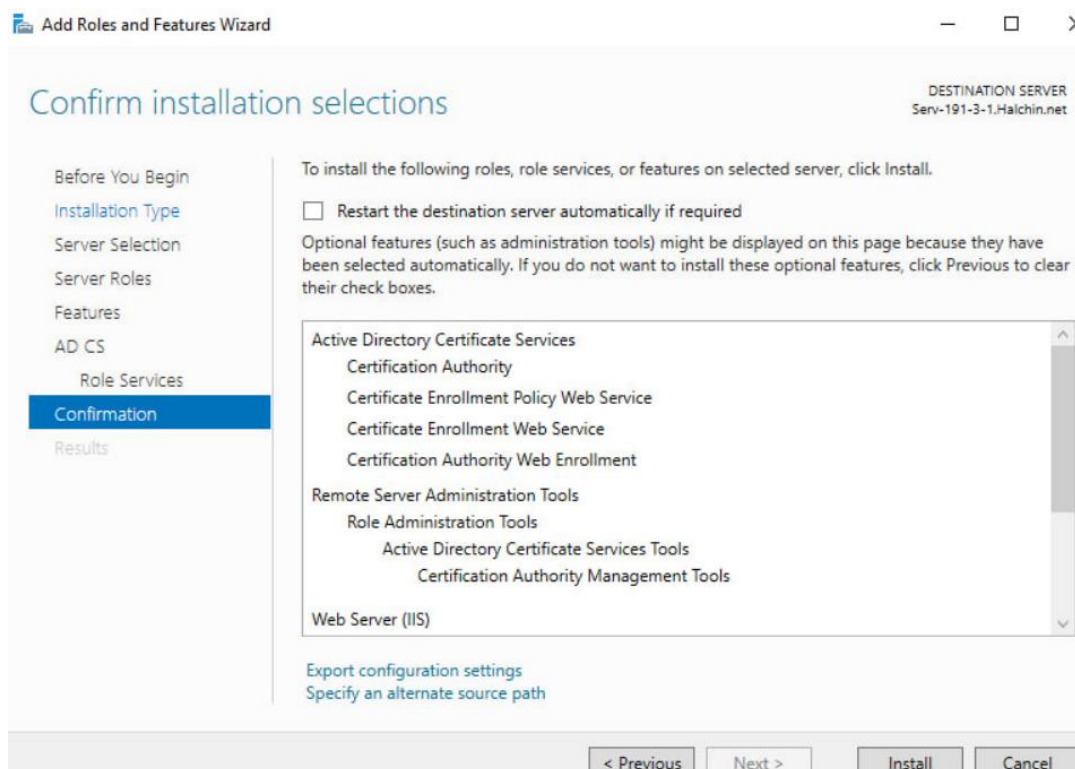


Рис. 3.7 Налаштування

Розпочинається встановлення Active Directory Certificate Services (рис. 3.8).

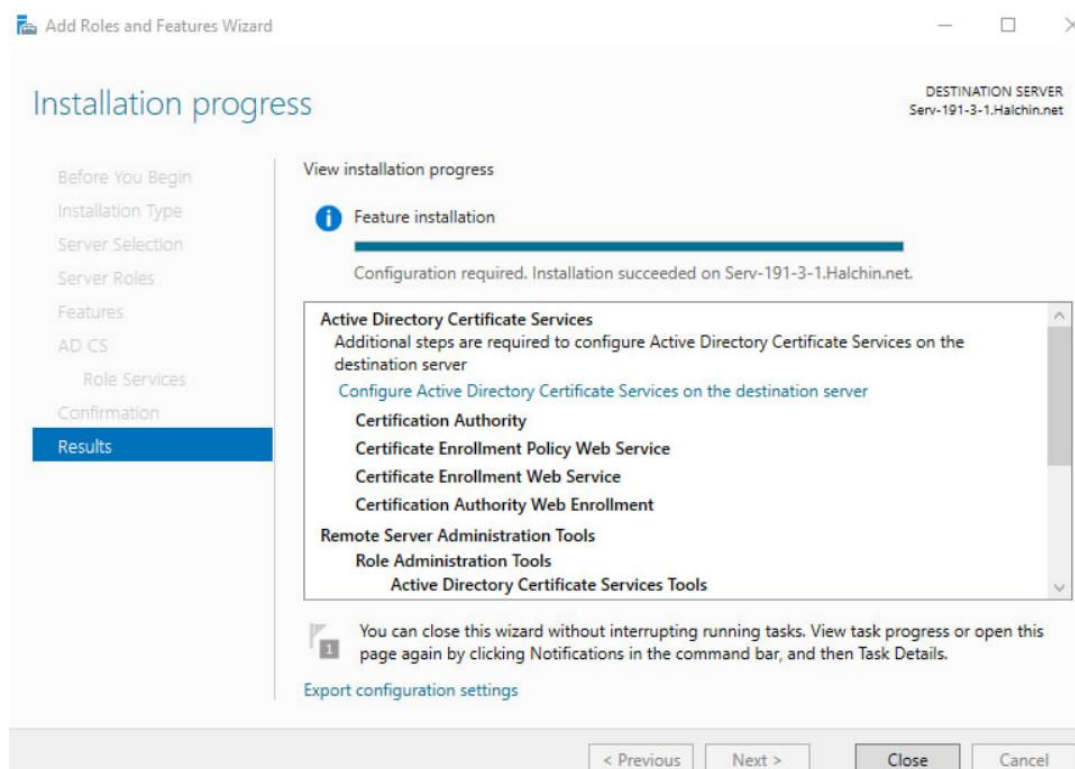


Рис. 3.8 Результат успішного встановлення

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Після встановлення ролі Active Directory Certificate Services у правій верхній частині вікна Server Manager, біля піктограми у вигляді прапорця, має з'явитися знак оклику (рис. 3.9). Щоб налаштувати щойно встановлений Active Directory Certificate Services обираємо опцію Configure Active Directory Certificate Services configuration.

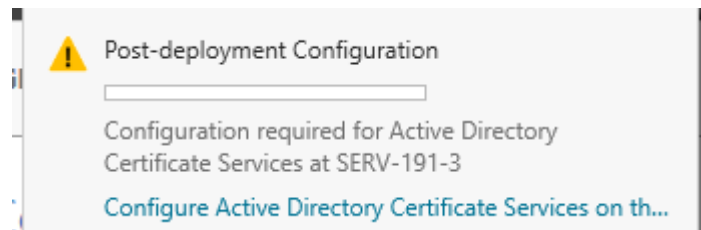


Рис. 3.9 Налаштування

На сторінці Credentials видно, що в полі Облікові дані відображається Адміністратор. Натискаємо кнопку Далі (рис. 3.10).

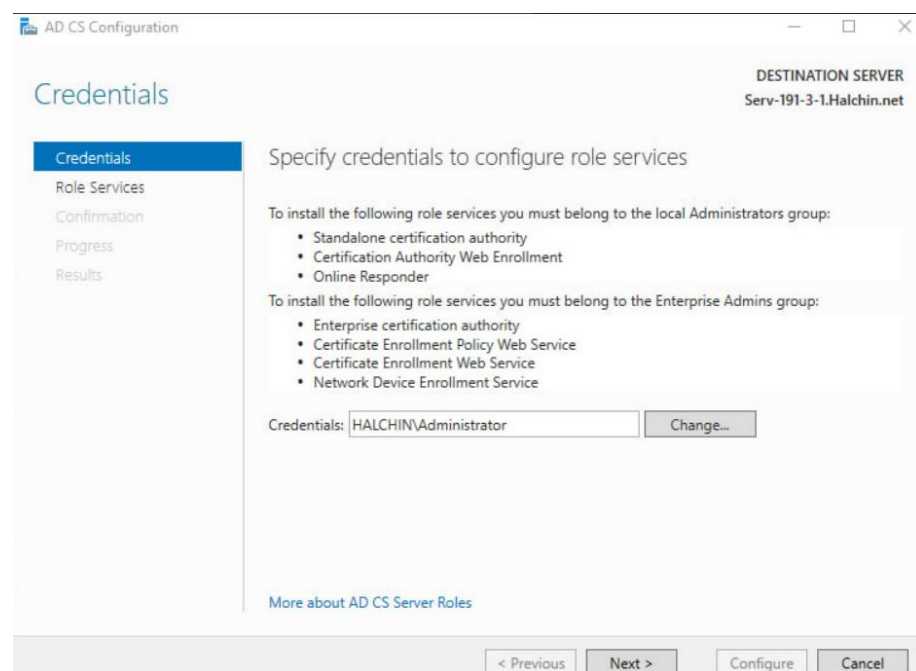


Рис. 3.10 Credentials

Для початку встановимо тільки Certification Authority, оскільки всі ролі неможливо встановити одночасно (рис. 3.11). Пізніше повернемося та встановимо інші ролі.

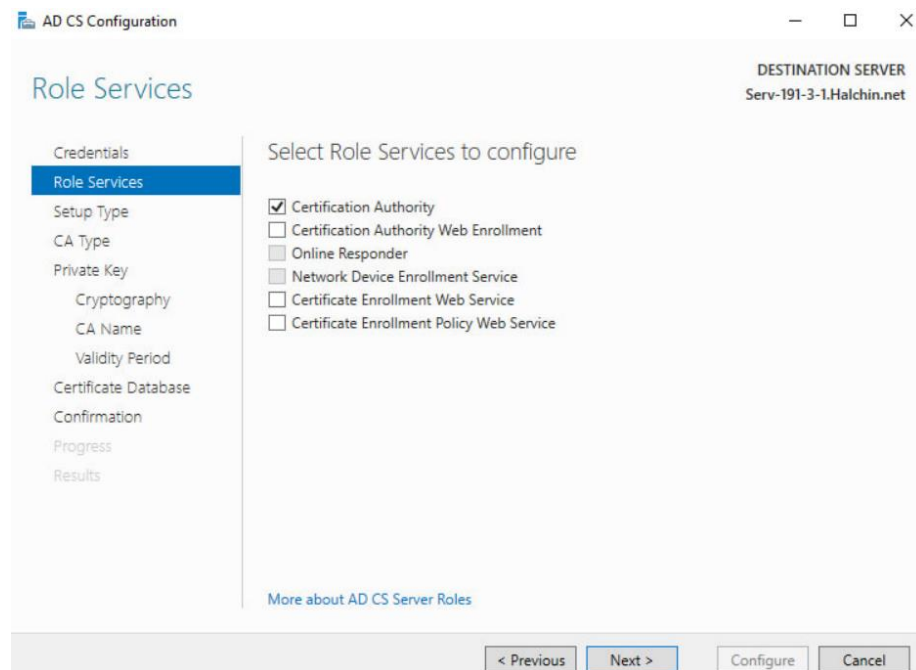


Рис. 3.11 Certification Authority

На сторінці Тип налаштування виберемо Enterprise CA як тип СА, щоб дозволити інтеграцію з наявним AD (рис. 3.12).

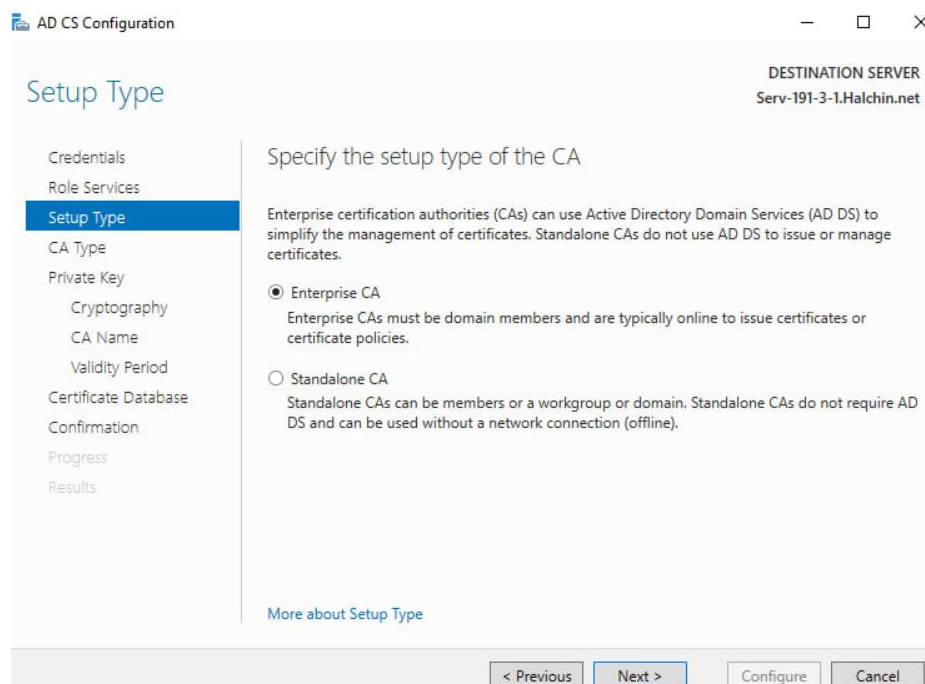


Рис. 3.12 Тип налаштування

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

На сторінці CA Type виберемо Root CA, оскільки це перший CA у даному середовищі і натискаємо Далі (рис. 3.13).

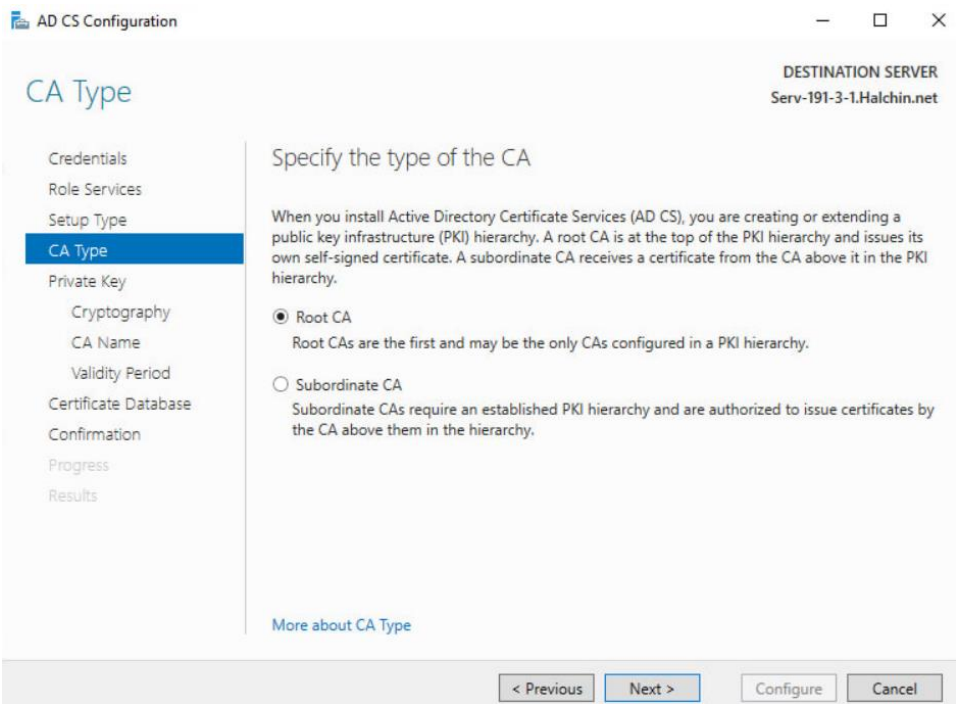


Рис. 3.13 Root CA

На сторінці Private Key вибираємо Create a new private key, оскільки ключ ще не було створено. Натискаємо кнопку Далі (рис. 3.14).

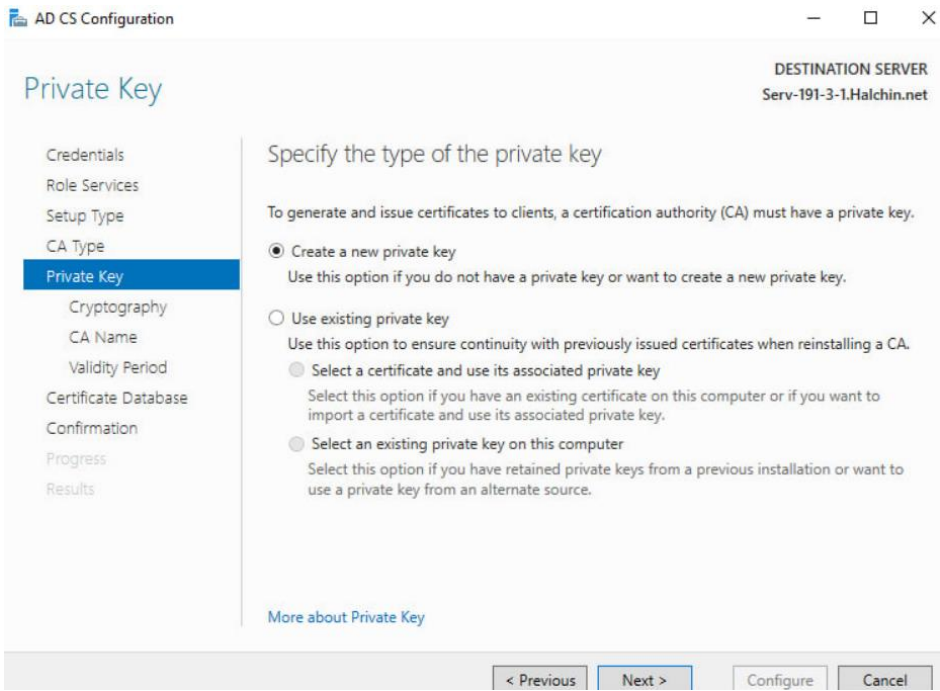


Рис. 3.14 Private Key

На сторінці Криптографія для ЦСК виконуємо наступні дії:

- Виберемо постачальника криптографічних послуг за замовчуванням як RSA#Microsoft Software Key Storage Provider. Він є вбудованим у Windows і має глибоку інтеграцію з операційною системою. Це дозволяє зручно та ефективно використовувати його для зберігання та управління криптографічними ключами в середовищі Windows.
- Обираємо Key length як 2048. Такий ключ потребує менше місця для зберігання та менше навантажуватиме процесор у ході використання.
- Вибираємо SHA256 як алгоритм хешування. Перевагами такого алгоритму є висока швидкість шифрування і практично неможливість розшифрування без ключів, а також мінімальний ризик появи колізій (однакових образів). Потім натискаємо Далі (рис. 3.15).

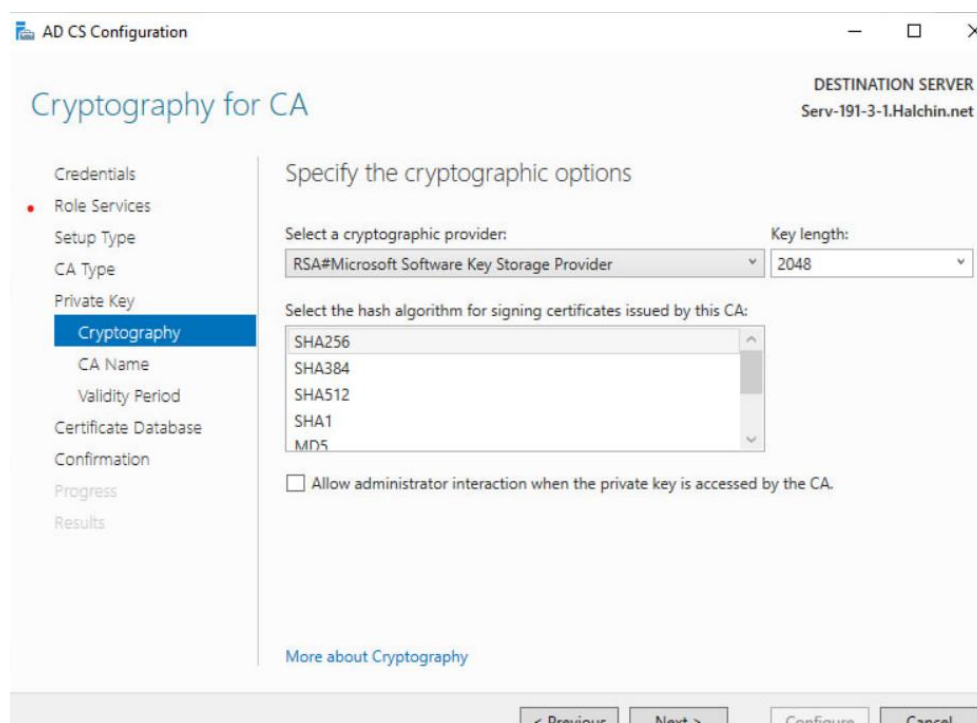


Рис. 3.15 Криптографія

На сторінці CA Name можемо вказати ім'я ЦС у текстовому полі. Загальну назву для цього ЦС, в нашому випадку залишимо за замовчуванням (рис. 3.16).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Рис. 3.16 CA Name

На сторінці **Validity Period** виберемо кількість років, протягом яких буде діяти сертифікат. Обираємо 5 років, оскільки, довші терміни дії забезпечують більш безперебійну роботу користувачів, оскільки їм не потрібно часто поновлювати або перевидавати сертифікати (рис. 3.17).

Рис. 3.17 Validity Period

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

На сторінці CA Database вибираємо розташування бази даних і файлів журналів бази даних (рис. 3.18).

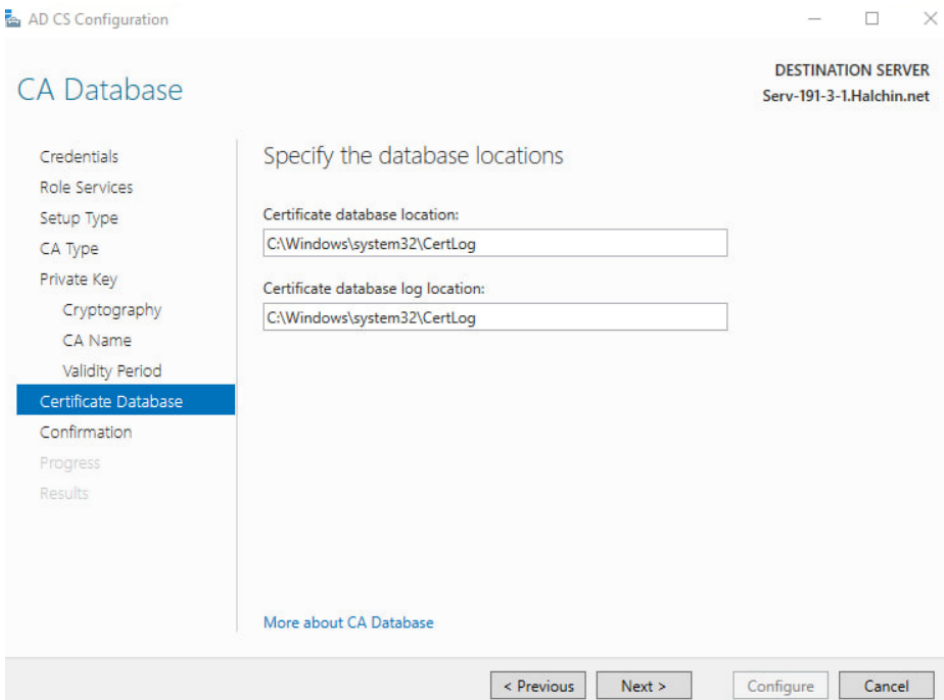


Рис. 3.18 Розташування бази даних

На сторінці підтвердження перевіряємо обрані налаштування та натискаємо Configure. Після завершення налаштування з'являється вікно результатів (рис. 3.19).

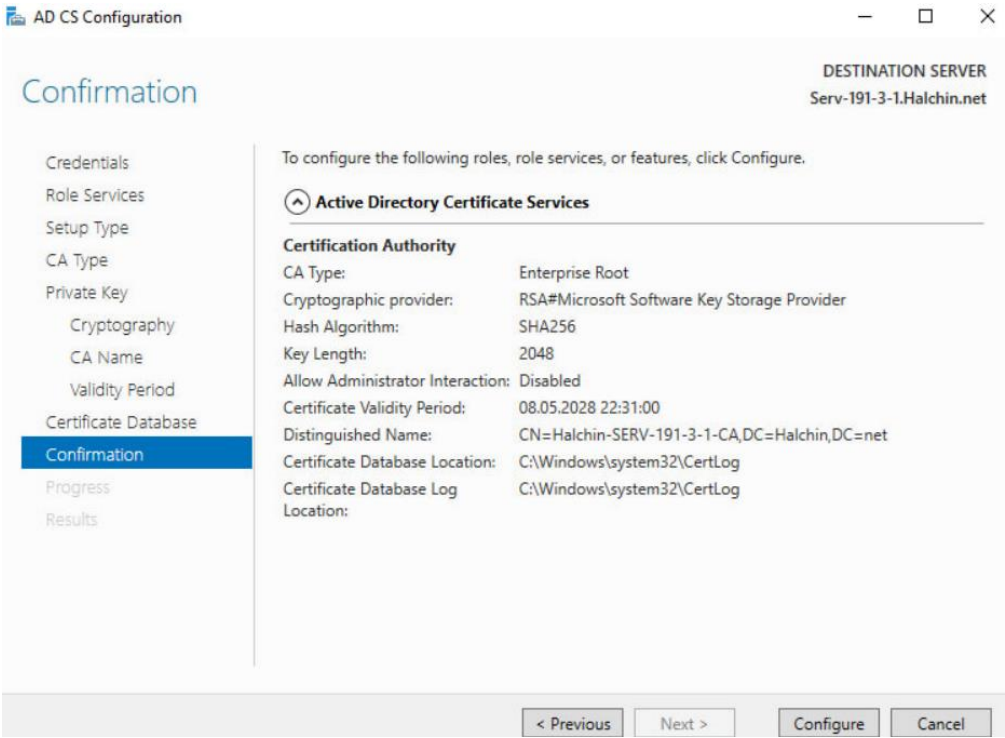


Рис. 3.19 Configure

На рис. 3.20 показано успішне завершення налаштування.

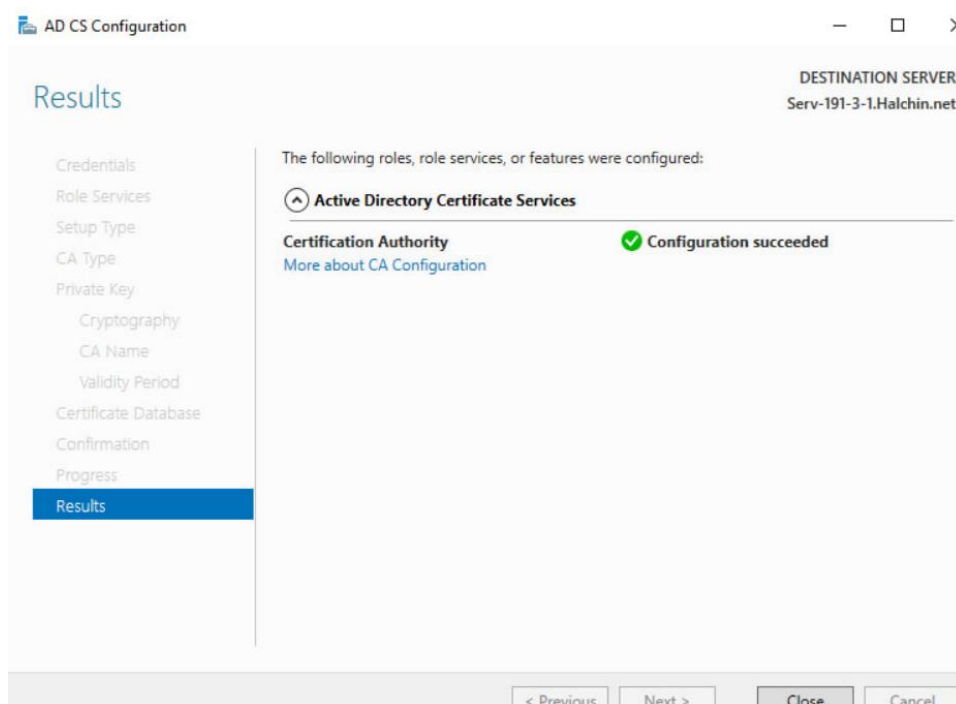


Рис. 3.20 Успішне налаштування

Далі з'являється повідомлення із пропозицією повернутися та встановити інші ролі. У разі згоди, перед нами відкривається вікно, де вибираємо інші три ролі, які маємо потребу довстановити (рис. 3.21). Ці ролі знадобляться для наступної роботи серверу сертифікації.

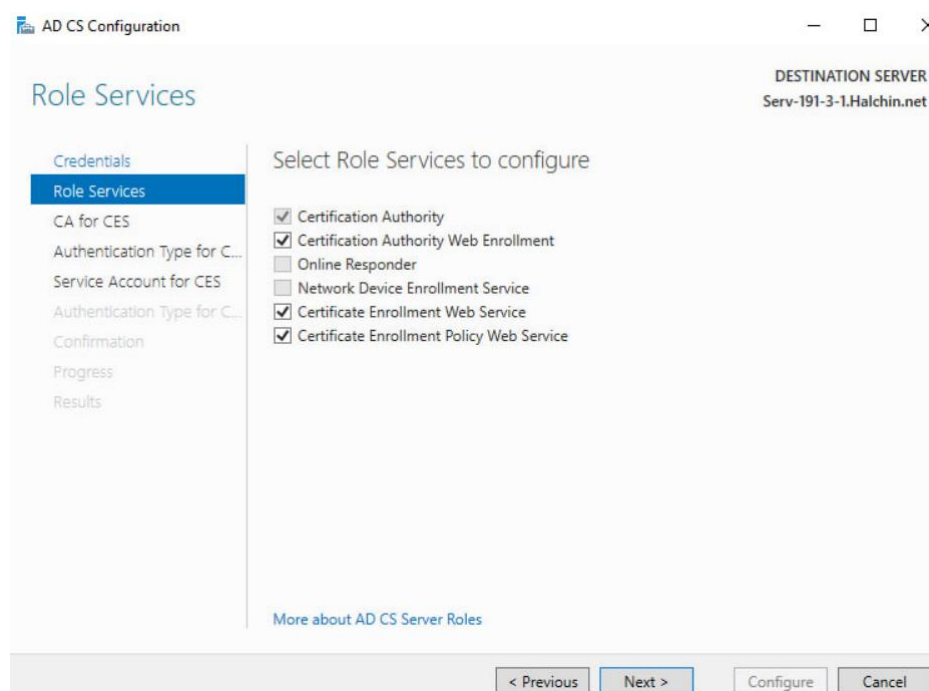


Рис. 3.21 Встановлення ролей

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

Далі виберемо сервер СА, на якому буде розміщено роль CES (рис. 3.22).

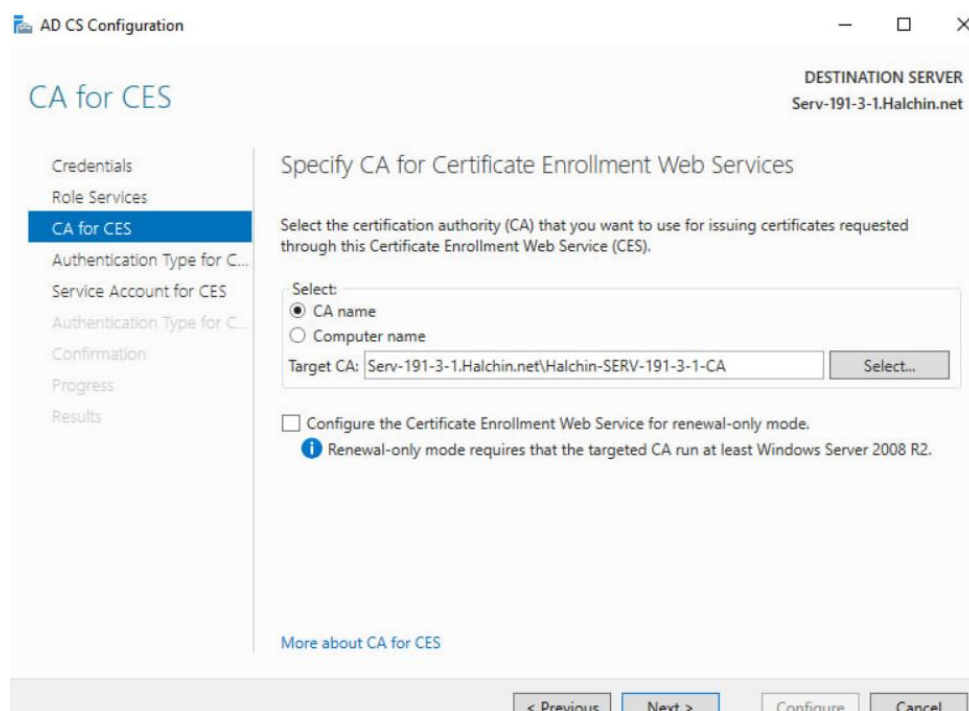


Рис. 3.22 CES

Далі потрібно вибрати, як саме буде виконано автентифікацію. Виберемо автентифікацію Windows. У разі якщо розгортання сертифікатів буде відбуватися демілітаризованій зоні, тоді, краще використовувати ім'я користувача/пароль (рис. 3.23).

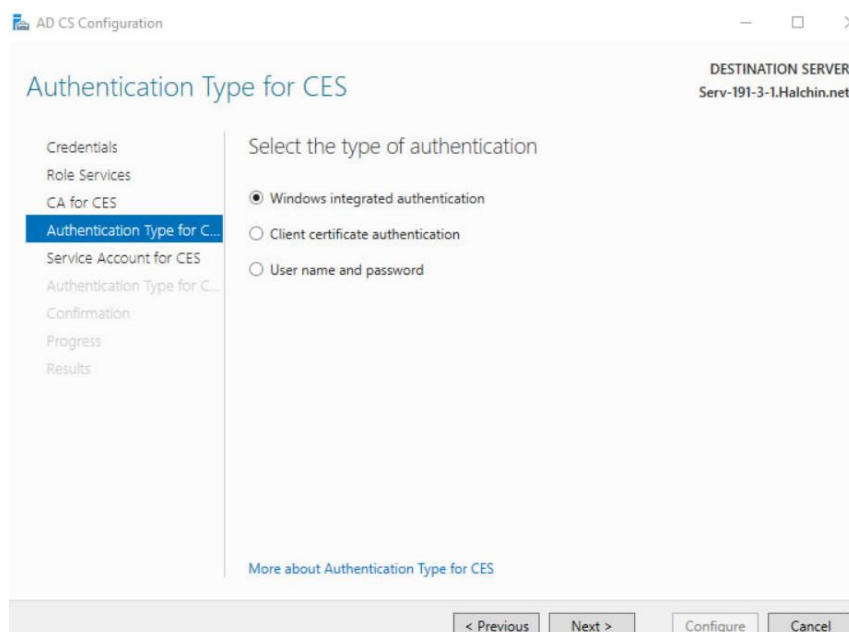


Рис. 3.23 Автентифікація

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Далі потрібно вказати свій обліковий запис, так як в нас його поки немає то використаємо вбудований (рис. 3.24).

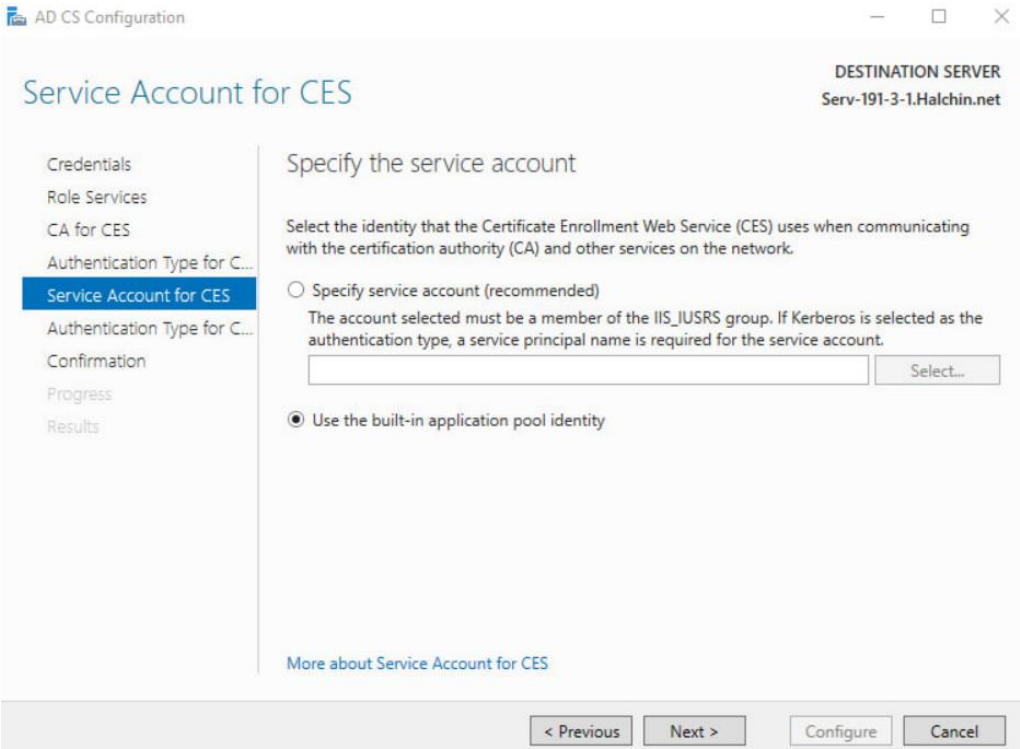


Рис. 3.24 Обліковий запис

На сторінці підтвердження натискаємо Configure. Після завершення налаштування з'являється вікно результатів (рис. 3.25).

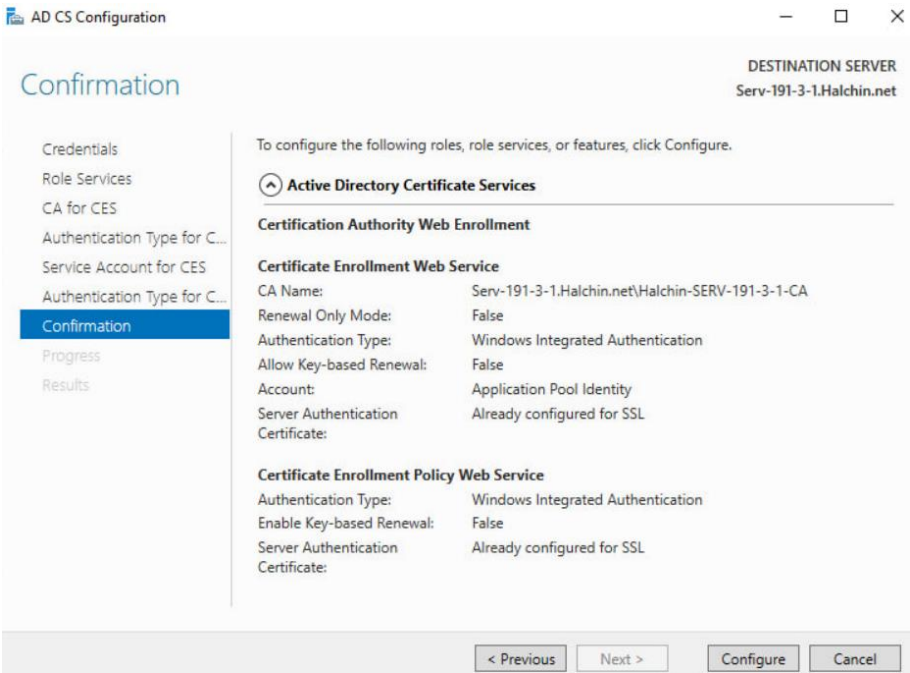


Рис. 3.25 Configure

На рис. 3.26 показано успішне налаштування.

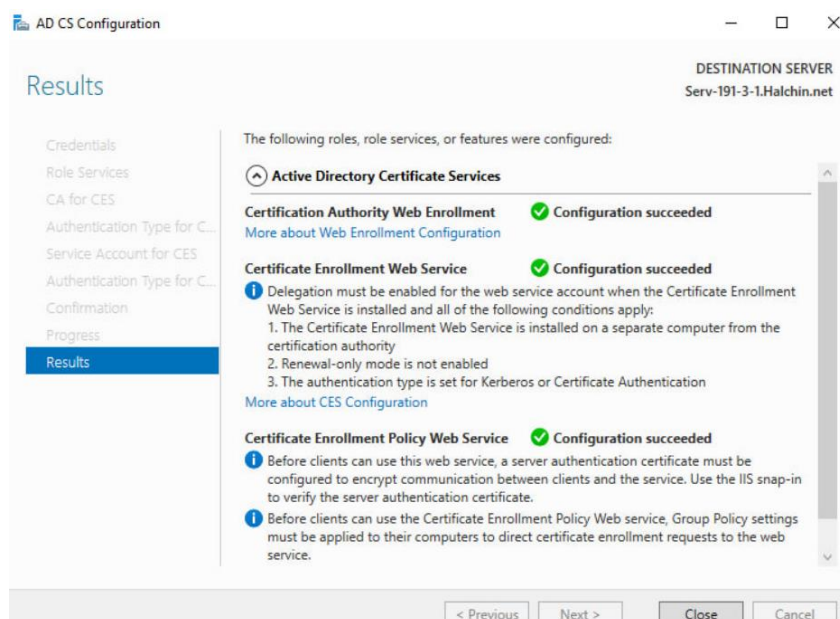


Рис. 3.26 Успішне налаштування

3.2 Створення запиту на сертифікат

У меню "Пуск" Windows обираємо Диспетчер інформаційних служб Інтернету (IIS). У диспетчері Internet Information Services (IIS) у дереві меню "Підключення" (ліва панель) вибираємо потрібне ім'я сервера. На домашній сторінці з назвою сервера (центральна панель) у розділі IIS двічі клацаємо по Server Certificates (рис .3.27)^[9].

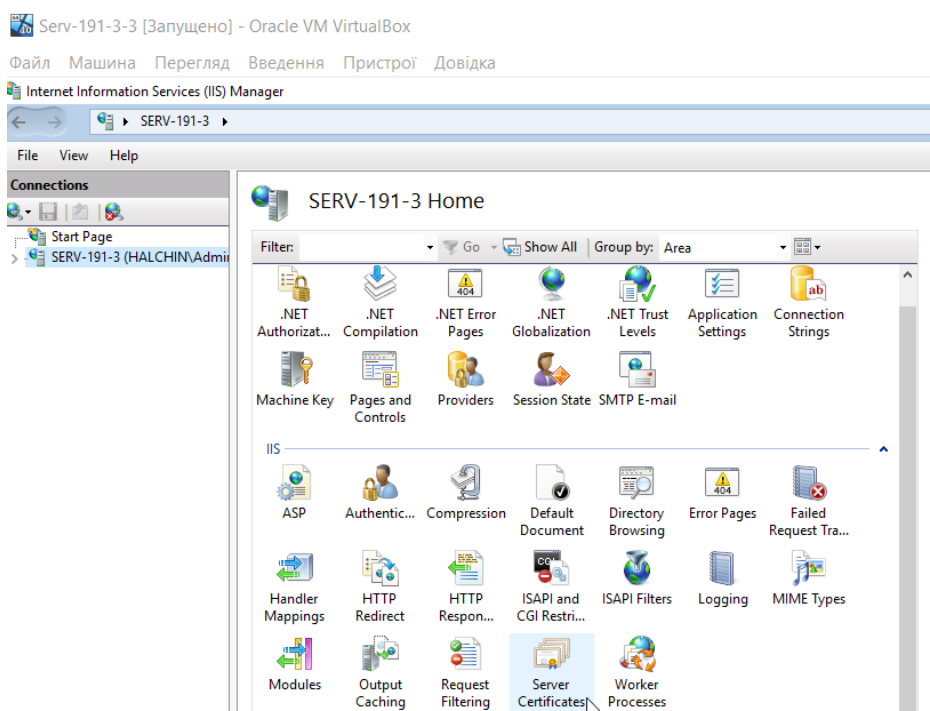


Рис. 3.27 Server Certificates

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

На сторінці Сертифікати сервера (центральна панель) в меню Дії (права панель) натискаємо посилання Create Certificate Request... (рис. 3.28).

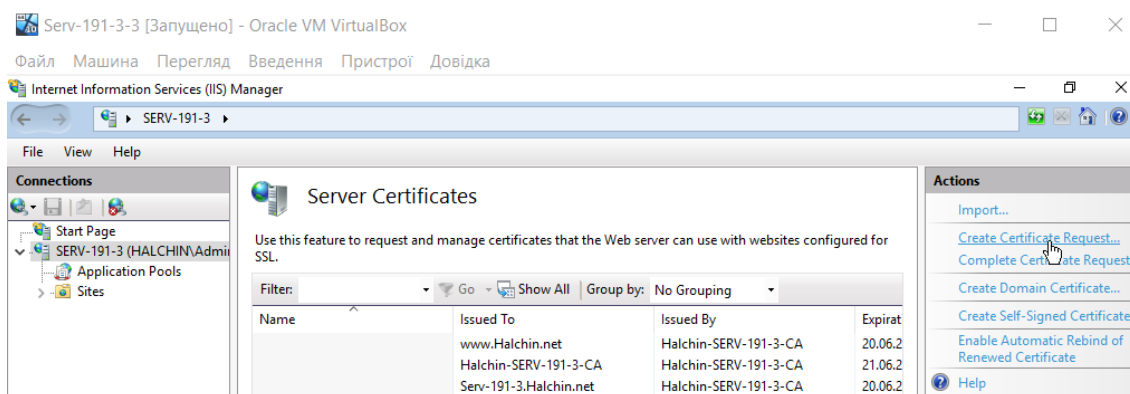


Рис. 3.28 Create Certificate Request

У майстрі запиту сертифіката на сторінці "Властивості доменного імені" вводимо наведену нижче інформацію, а потім натискаємо кнопку "Далі" (рис. 3.29).

Відомості для заповнення полів на сторінці "Властивості доменного імені" є наступними.

- Загальне ім'я. Повне доменне ім'я (FQDN) (www.Halchin.net).
- Організація. Вводимо юридично зареєстровану назву компанії (Company).
- Організаційний підрозділ. Назва підрозділу в організації. Часто в цьому полі вказується "ІТ", "Веб-безпека" або просто залишається порожнім.
- Місто/місцевість. Місто, в якому юридично розташована компанія.
- Штат/провінція. Вводимо штат/провінцію, де юридично розташована компанія.
- Країна. У випадяючому списку обираємо країну, де компанія має юридичну адресу.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

Рис. 3.29 Властивості доменного імені

На сторінці Властивості постачальника криптографічних послуг вводимо наведену нижче інформацію, а потім натискаємо Далі (рис. 3.30).

Cryptographic. У випадяючому списку обираємо Microsoft RSA SChannel Cryptographic Provider, постачальник послуг (оскільки в цій роботі не використовується інший постачальник криптографічних послуг).

Довжина біта. У випадяючому списку обираємо 1024. Можна обрати більший розмір ключа, але тільки якщо це необхідно, оскільки більша довжина ключа збільшує затримку і може погіршити сумісність.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

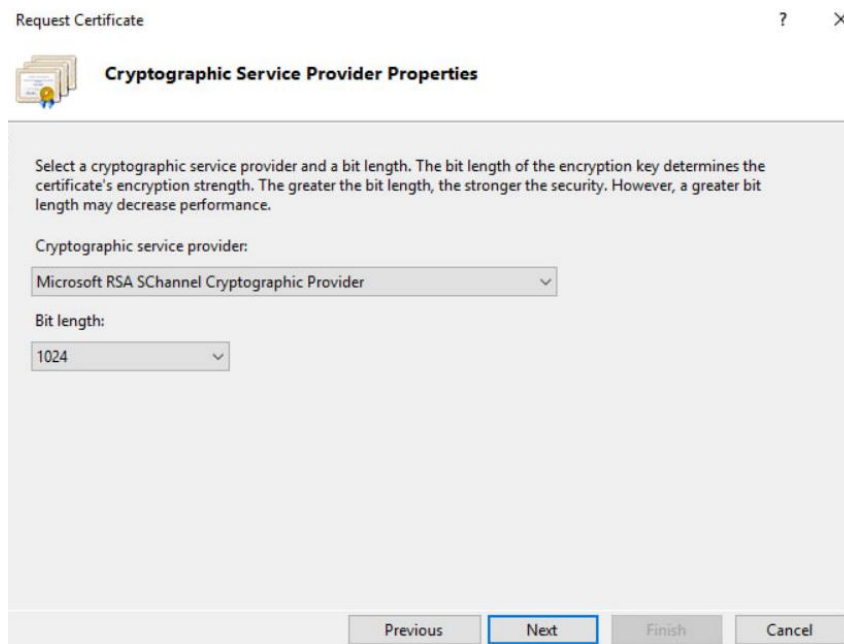


Рис. 3.30 Властивості постачальника криптографічних послуг

На сторінці Ім'я файлу в розділі Вкажіть ім'я файлу для запиту на сертифікат натискаємо поле ..., щоб перейти до місця, де потрібно зберегти свій CSR. Завершивши, натискаємо Готово (рис. 3.31).

Важливо запам'ятати обране ім'я та розташування файлу. За замовчуванням, CSR буде збережено у C:\Windows\System32.

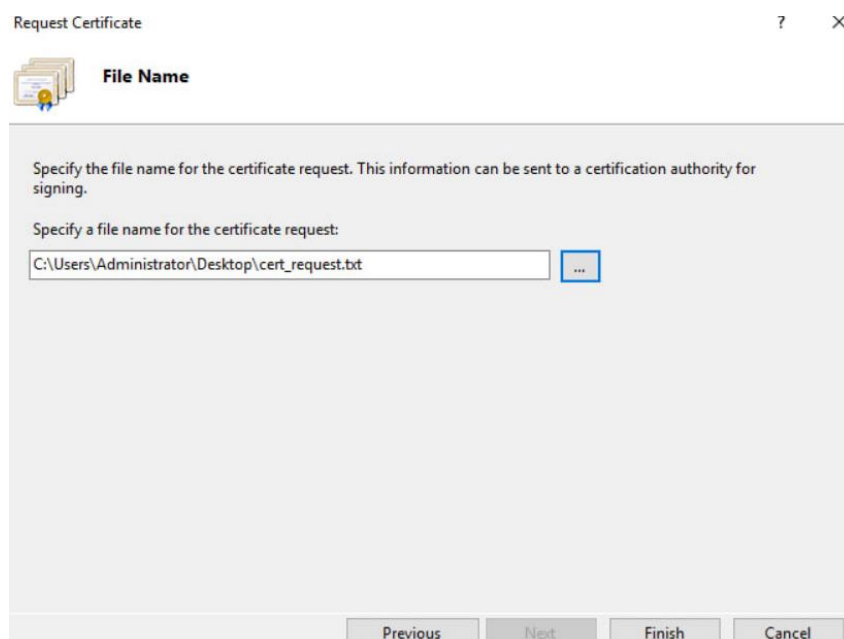


Рис. 3.31 Збереження файлу

На рис. 3.32 показано успішний результат створення та збереження файлу.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

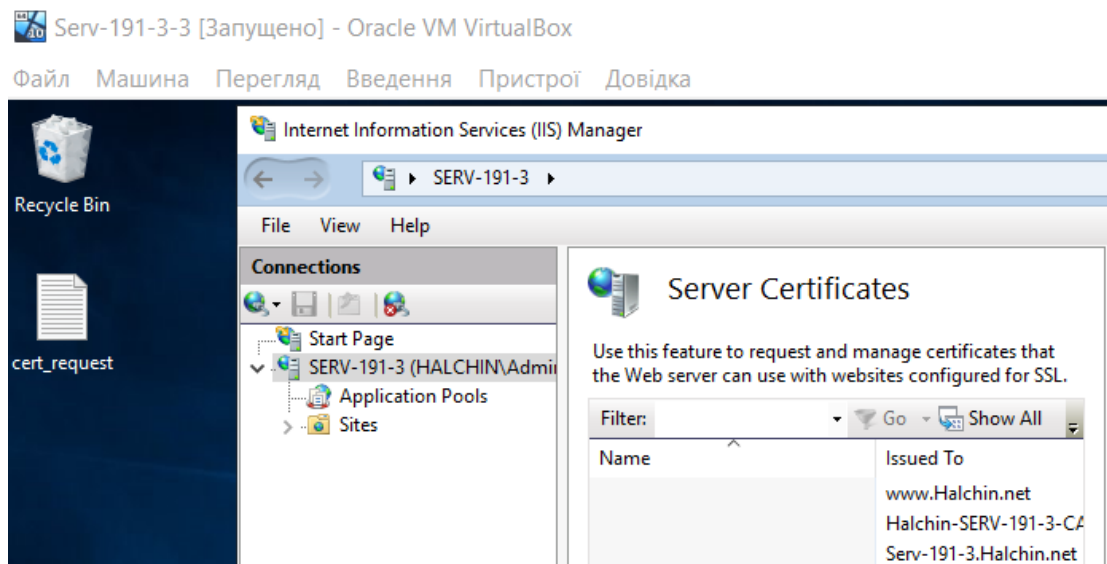


Рис. 3.32 Збереження файлу

Відкриваємо файл за допомогою текстового редактора (наприклад, Блокнот). Можна побачити успішне створення запита на сертифікат (рис. 3.33).

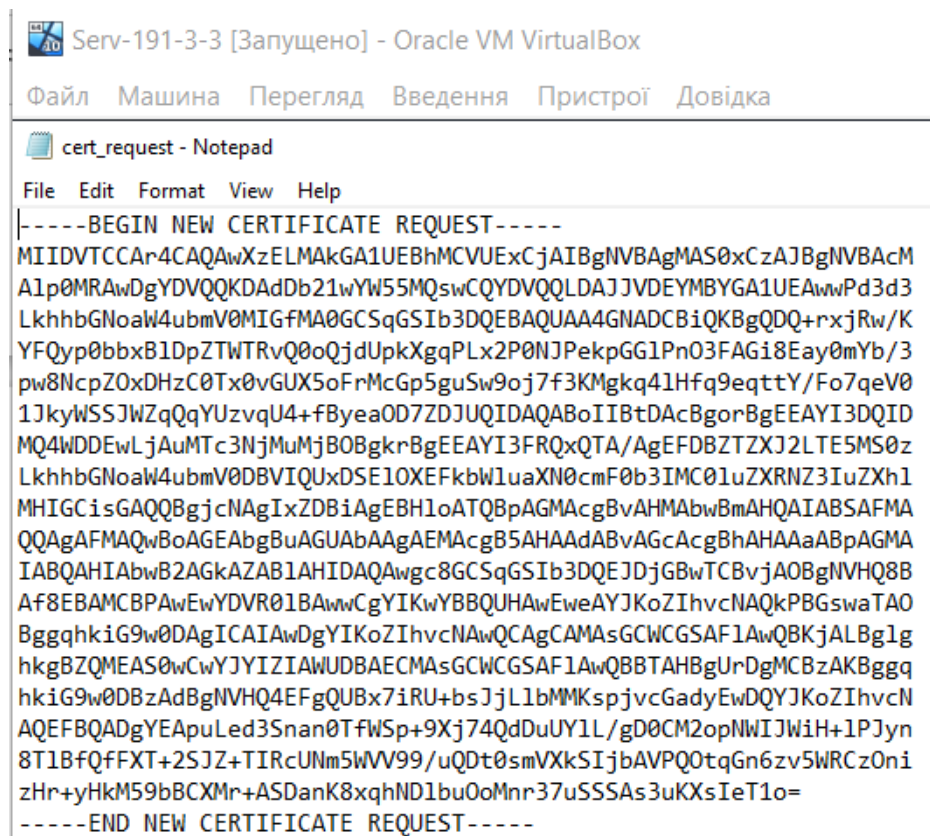


Рис. 3.33 Запит на сертифікат

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

3.3 Створення сертифікату

Після отримання запиту на сертифікат перейдемо до самого сертифікату. Для початку в веб-браузері потрібно підключитися до `https://<ім'я сервера>/certsrv`, де `<ім'я сервера>` - це ір-адреса або ім'я комп'ютера, на якому запущено службу ролей веб-реєстрації СА. При спробі підключення з'являється запит на вхід. На рис. 3.34 показано вхід через користувача Administrator, оскільки, він має найбільші права.

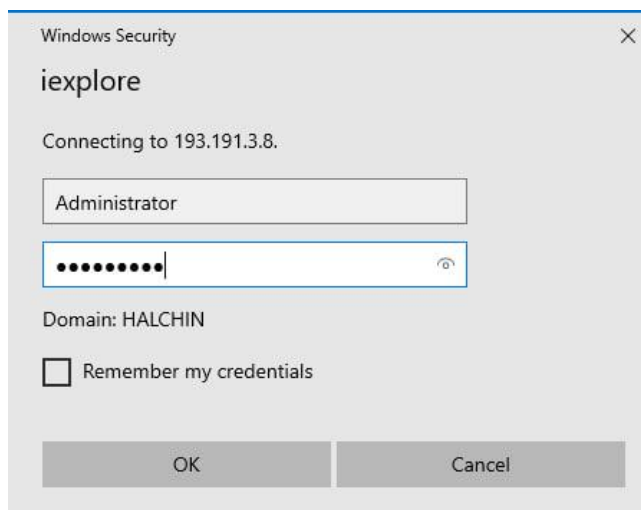


Рис. 3.34 Підключення до сервера

Наразі з'єднання з сайтом не є захищеним, тому під час переходу буде виведення застереження. Для того аби продовжити далі роботу потрібно додати сайт до списку довірених сайтів. Для цього натискаємо Add (рис. 3.35).

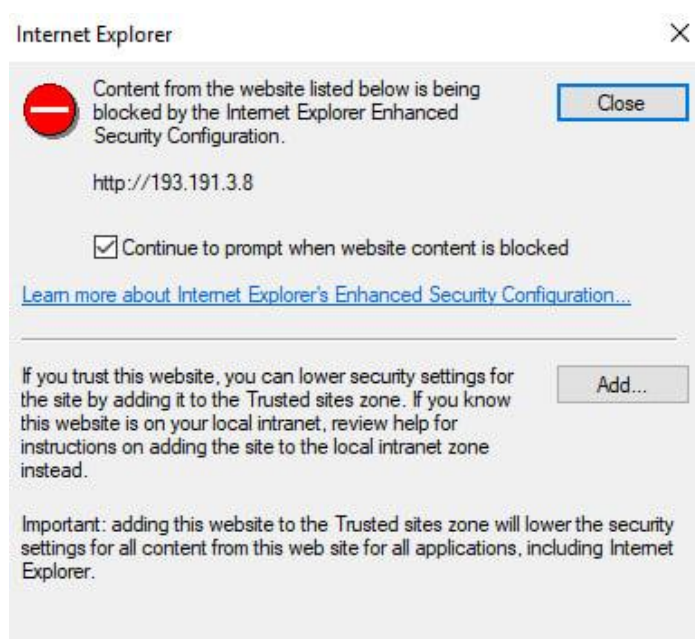


Рис. 3.35 Застереження

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Далі відкриється вікно з списком довірених сайтів. Додаємо до цього списку сайт, натискаючи Add (рис. 3.36).

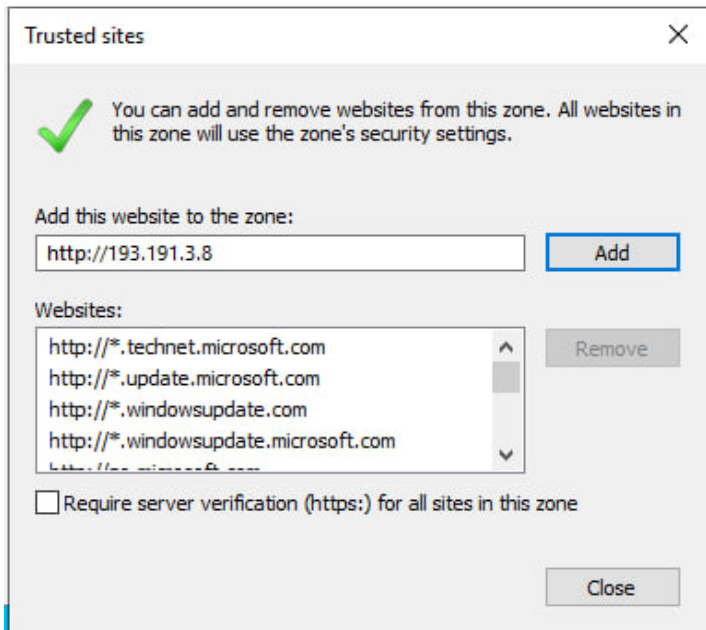


Рис. 3.36 Довірений сайт

При успішному вході буде показано початкову сторінку Служби сертифікації Microsoft Active Directory (рис. 3.37). Натискаємо Request a certificate ^[10].

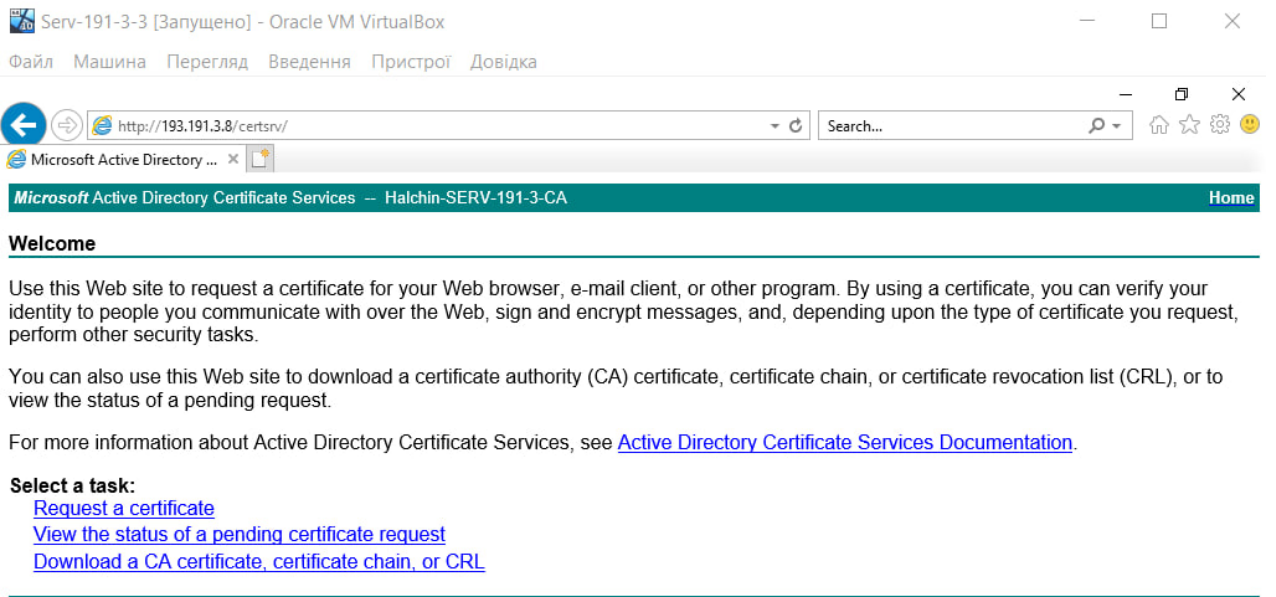


Рис. 3.37 Початкова сторінка

Далі потрібно натиснути advanced certificate request (рис. 3.38).

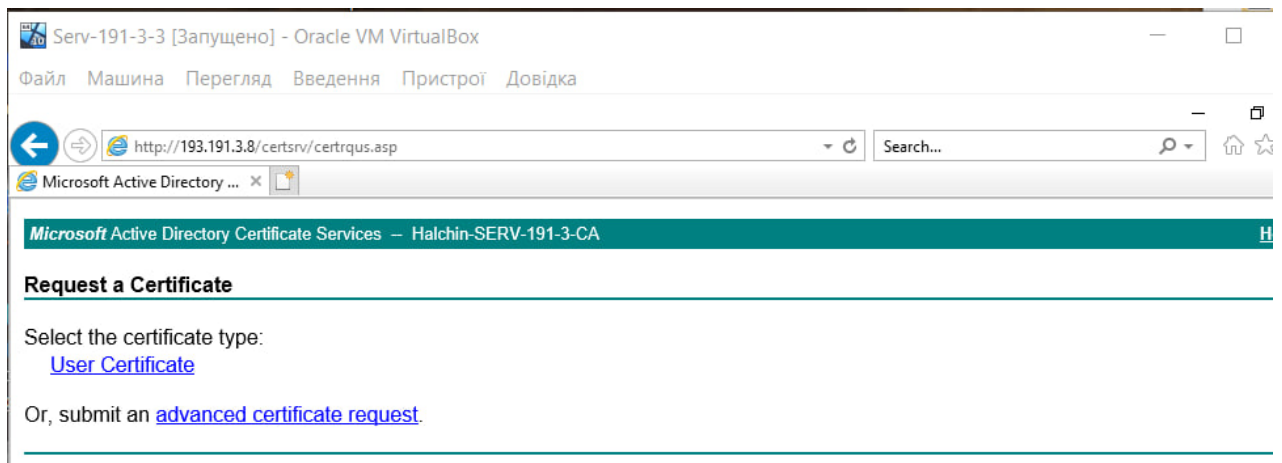


Рис. 3.38 Advanced certificate request

Далі обираємо Submit a renewal request by using a base-64-encoded PKCS #7 file. Цей варіант рекомендовано для більш розширеного і точного запиту на сертифікат з усіма деталями, що належать програмі або системі. Потрібно згенерувати запит на сертифікат з додатку або системи з необхідними деталями та надіслати дані в кодуванні base-64, використовуючи цю опцію (рис. 3.39).

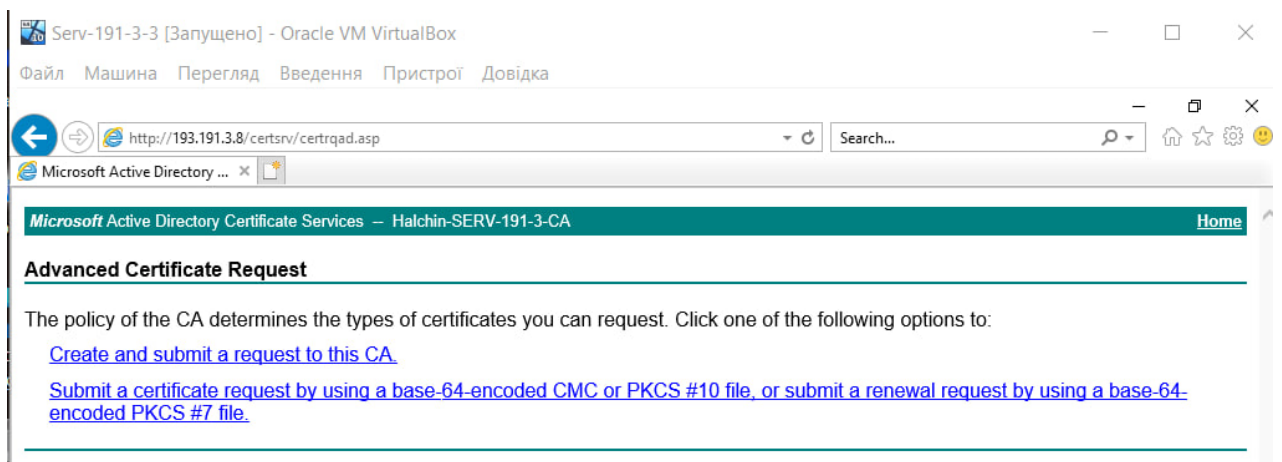


Рис. 3.39 Запит на сертифікат

Вставляємо запит на сертифікат у кодуванні base-64 (CSR) у відведене місце. Обираємо 'Web server'. Залишаємо поле "Атрибут" порожнім. Натискаємо на кнопку "Submit" (рис. 3.40).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

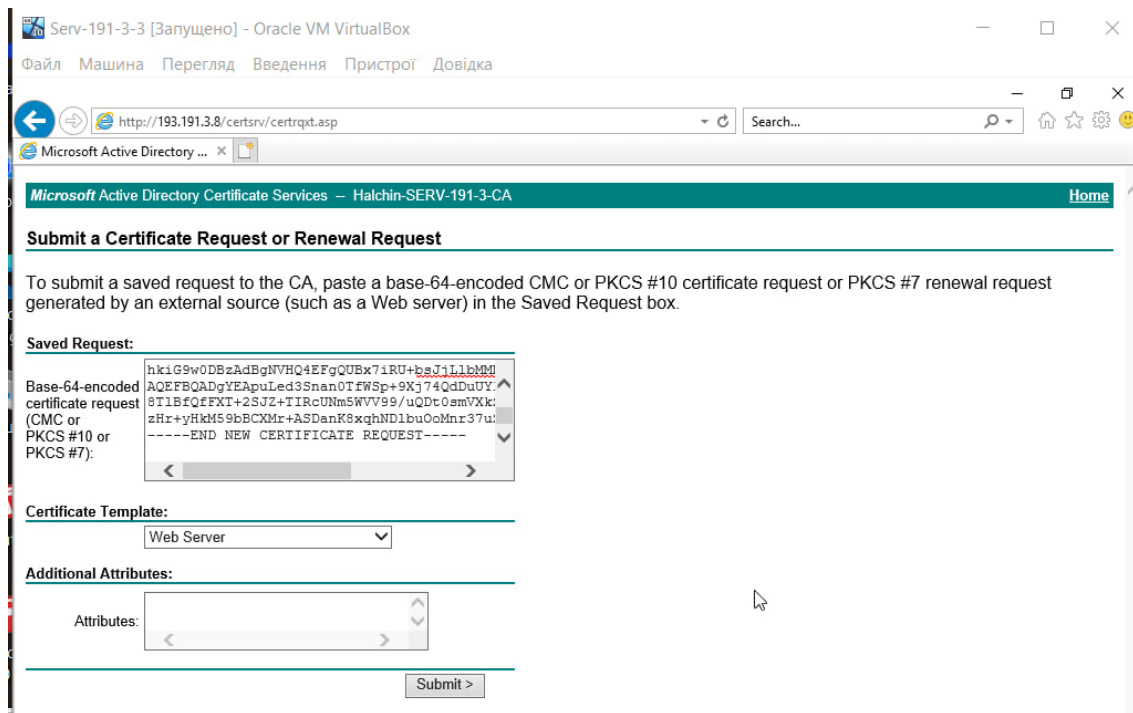


Рис. 3.40 Створення сертифікату

Далі постає вибір між типом кодування DER encoded та Base64 encoded. Перший варіант експортує сертифікат, закодований у форматі Distinguished Encoding Rules, який є двійковим форматом. Другий варіант експортує сертифікат у кодуванні Base64 - методі кодування, який перетворює двійкові дані на звичайний текст ASCII. Використаємо DER encoded, оскільки, він забезпечує строгу структуру даних, що найкраще підходить для сертифікату. Після вибору кодування натискаємо Download certificate. Внизу сторінки можна побачити повідомлення, вибираємо Save (рис. 3.41).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

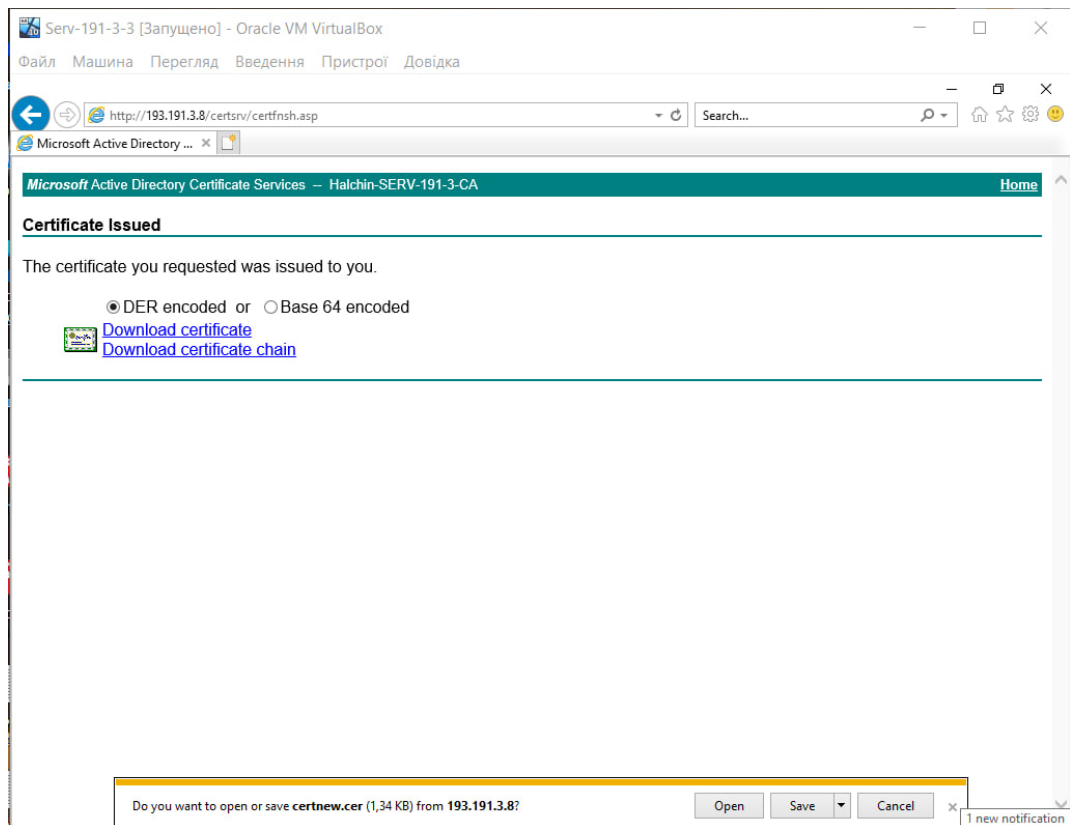


Рис. 3.41 Завантаження сертифікату

На рис. 3.42 показано успішно завантажений сертифікат.

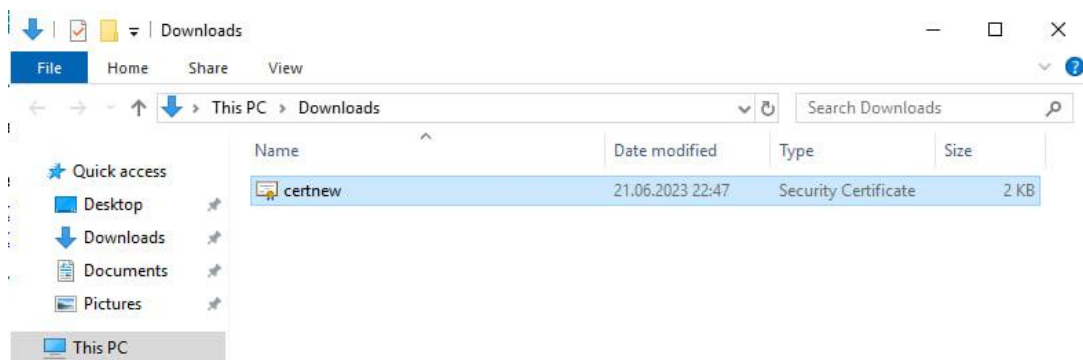


Рис. 3.42 Сертифікат

Далі відкриваємо IIS. Натискаємо Server Certificates. Праворуч на панелі вибираємо Complete Certificate Request (рис 3.43).

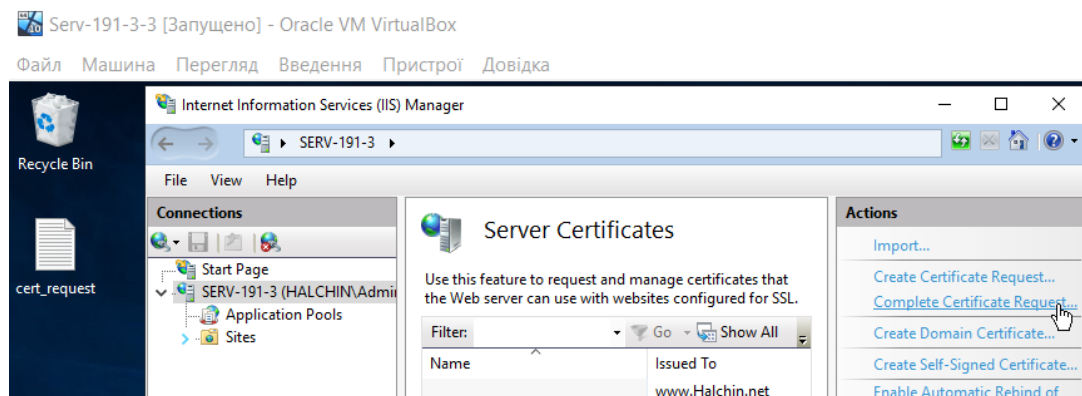


Рис. 3.43 Complete Certificate Request

Далі відкривається діалогове вікно. Переходимо в папку, де раніше було збережено файл сертифікату та вибираємо його. Далі в Friendly Name записуємо назву для ідентифікації сертифікату в IIS Manager. При виборі сховища для сертифікату постає дві позиції Personal та WebHosting. Web Hosting призначений для масштабування на більшу кількість сертифікатів, тому виберемо його. Натисніть ОК, щоб завершити роботу майстра імпорту сертифікатів (рис. 3.44).

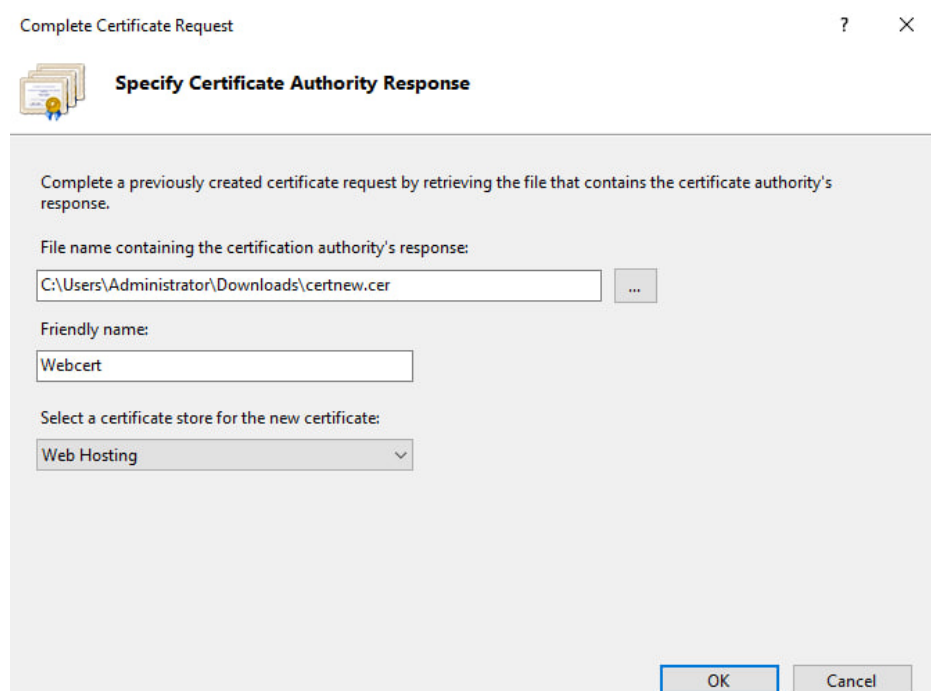


Рис. 3.44 Імпортування сертифіката

На рис. 3.45 видно успішно встановлений сертифікат у сховищі сертифікатів IIS.

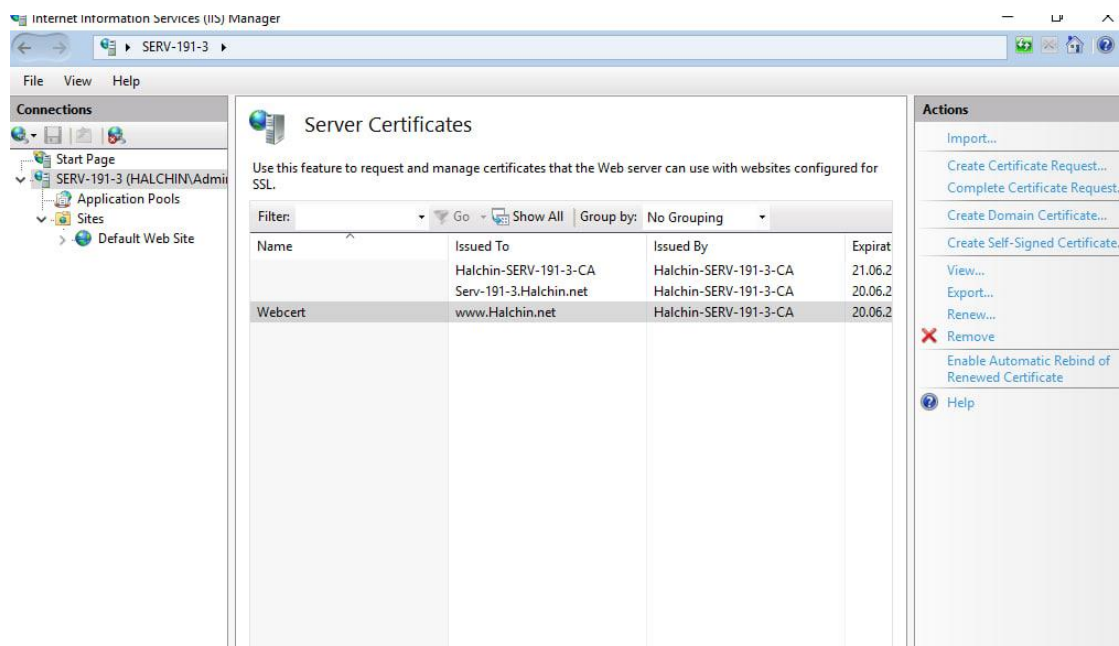


Рис. 3.45 Сертифікат

3.4 Перевірка працездатності

Для того, щоб перевірити працездатність сертифіката встановимо прив'язку сертифіката до сайту на сервері IIS. Для цього відкриємо Internet Information Services (IIS) Manager, виберемо Server Name → Sites де вкажемо вебсайт, до якого потрібно прив'язати сертифікат (Default Web Site). Далі натискаємо 'Bindings...' праворуч в колонці 'Edit Site' (рис. 3.46).

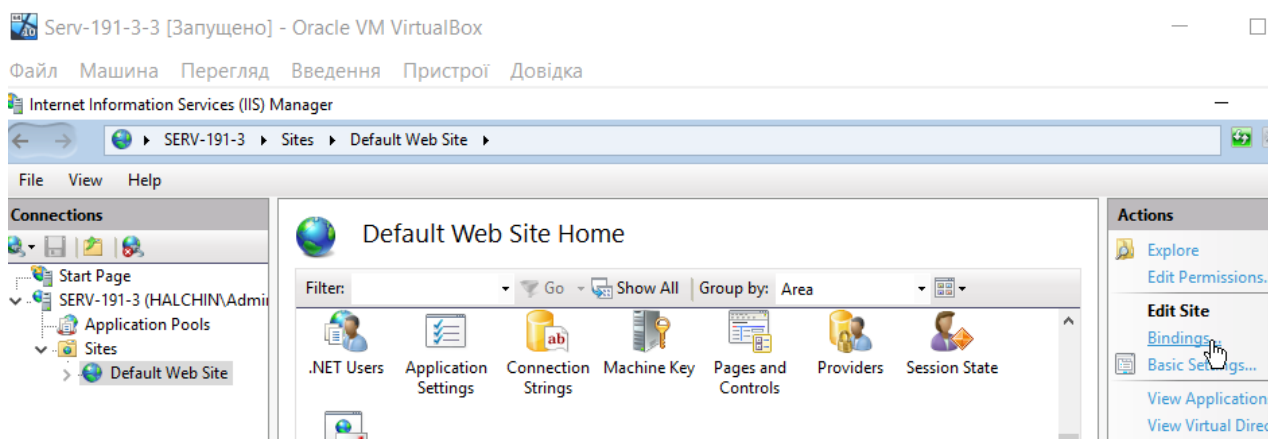


Рис. 3.46 Прив'язка сертифікату

Далі в Site Binding натискаємо Add (рис. 3.47).

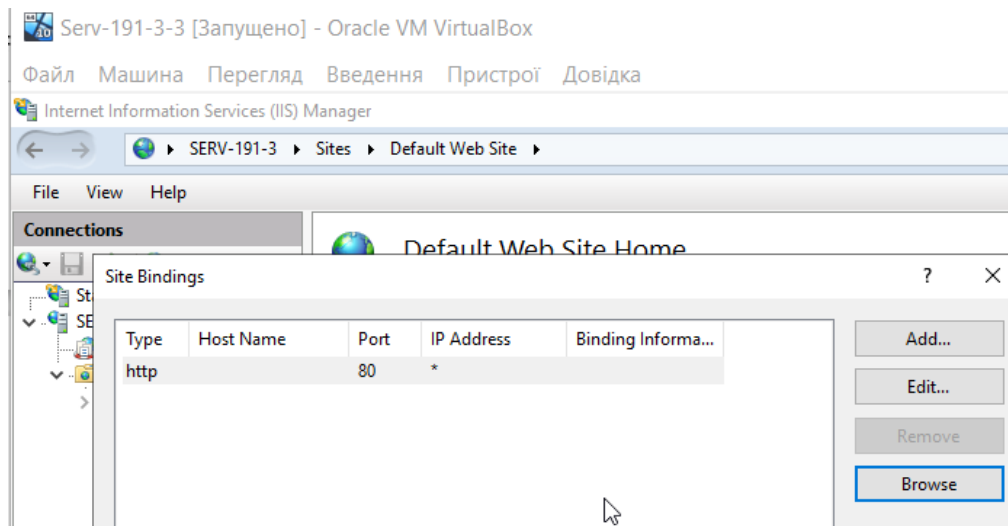


Рис. 3.47 Site Binding

Потім виконуємо наступні налаштування.

Type: https (захищений сайт)

Сертифікат SSL: Виберіть відповідний сертифікат зі спадного списку.

Список містить всі встановлені сертифікати в сховищі сертифікатів. (Webcert)

Натискаємо OK для завершення (рис. 3.48).

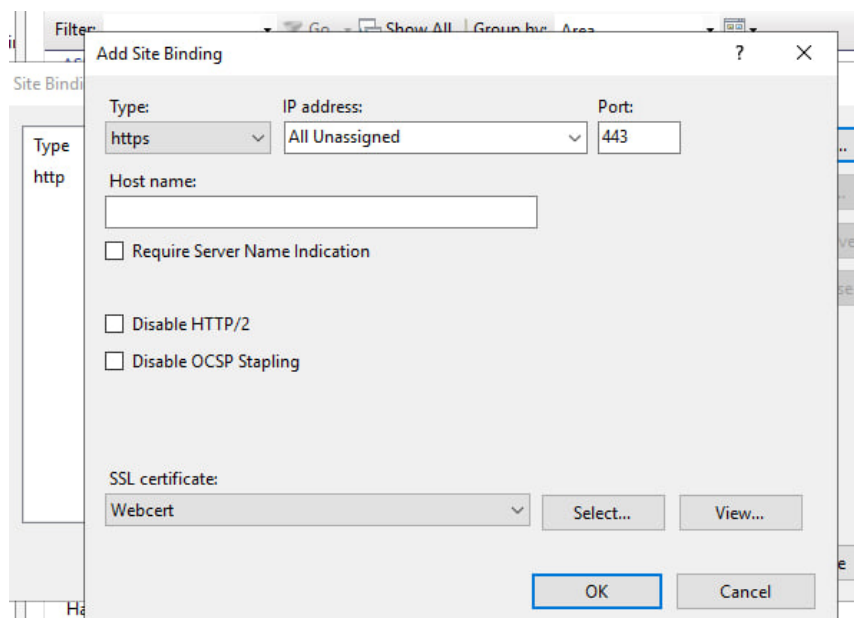


Рис. 3.48 Налаштування сайту для прив'язки

Далі для перевірки правильності налаштування сертифіката, потрібно виконати вхід на робочу станцію. Найкраще відкрити Internet Explorer, оскільки, він має вбудований список центрів сертифікації Windows. Далі переходимо в налаштування та вибираємо Властивості браузера (рис. 3.49).

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

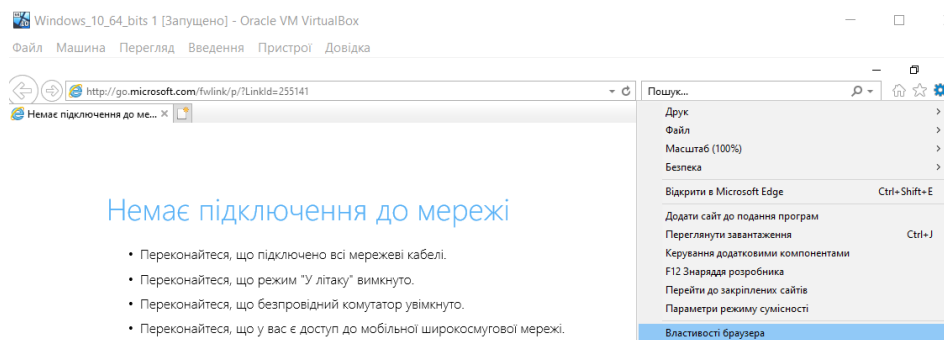


Рис. 3.49 Властивості браузера

Потім на вкладці Вміст вибираємо сертифікати та переходимо в вкладку довірені кореневі центри сертифікації. На рис. 3.50 показано створений сертифікат.

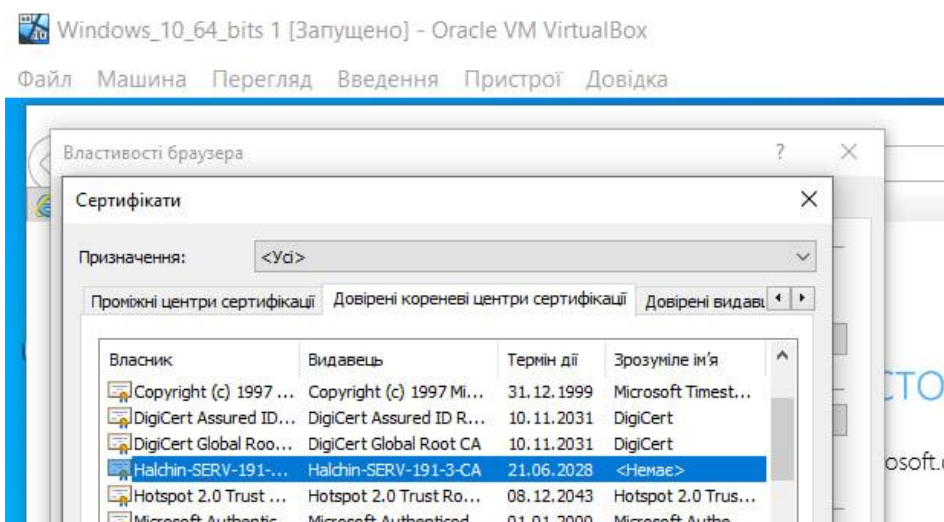


Рис. 3.50 Довірені кореневі центри сертифікації

Далі потрібно створити доменне ім'я. Для цього на DNS-сервері потрібно зробити відповідний запис. Запускаємо DNS Manager (Tools → DNS). У зоні прямого перегляду Haldin.net додаємо DNS-запис типу A з ім'ям www. Як IP-адресу задаємо адресу контролера домену (рис. 3.51).

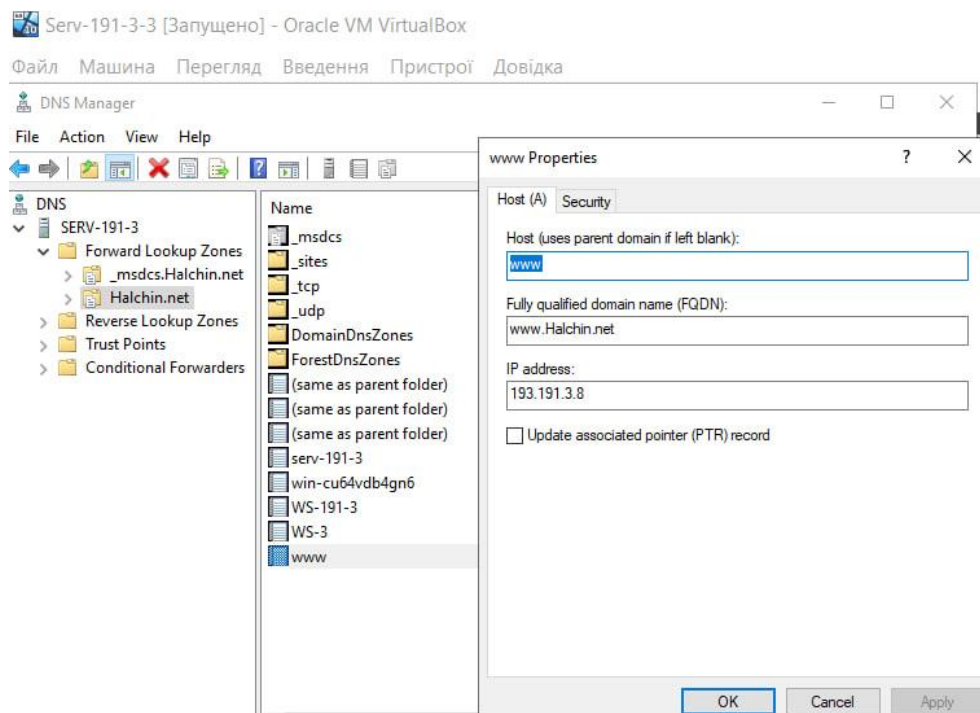


Рис. 3.51 Доменне ім'я

На робочій станції в адресному рядку веббраузера введемо адресу <https://halchin.net>. Буква s означає, що це захищений сайт. При натисненні на значок замка можна побачити додаткову інформацію про безпеку цього сайту (рис. 3.52).

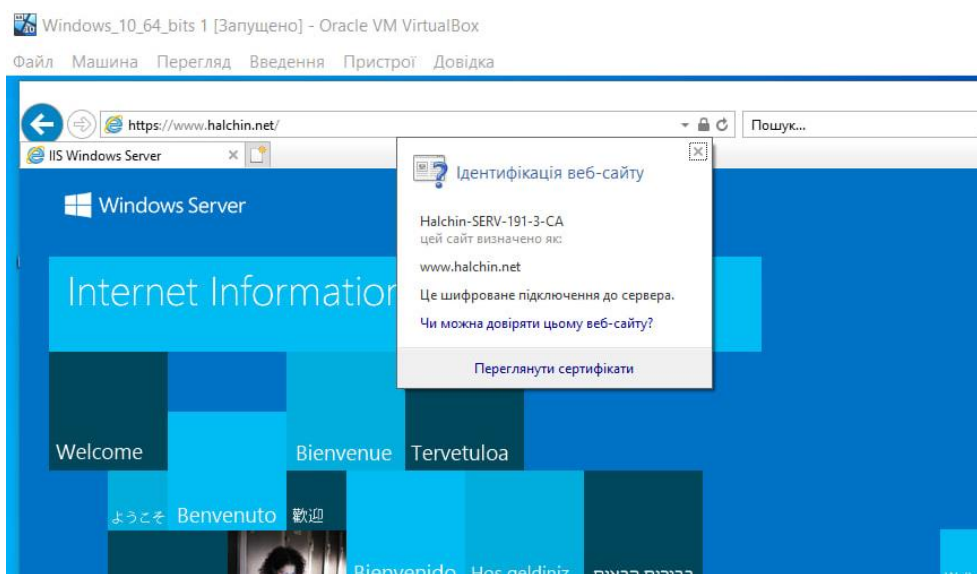


Рис. 3.52 Захищений сайт

Додаємо в пошуковому рядку /RDWeb/ та натискаємо Connect to a remote PC. Вводимо ім'я комп'ютера, до якого потрібно отримати доступ та натискаємо Connect (рис. 3.53)

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

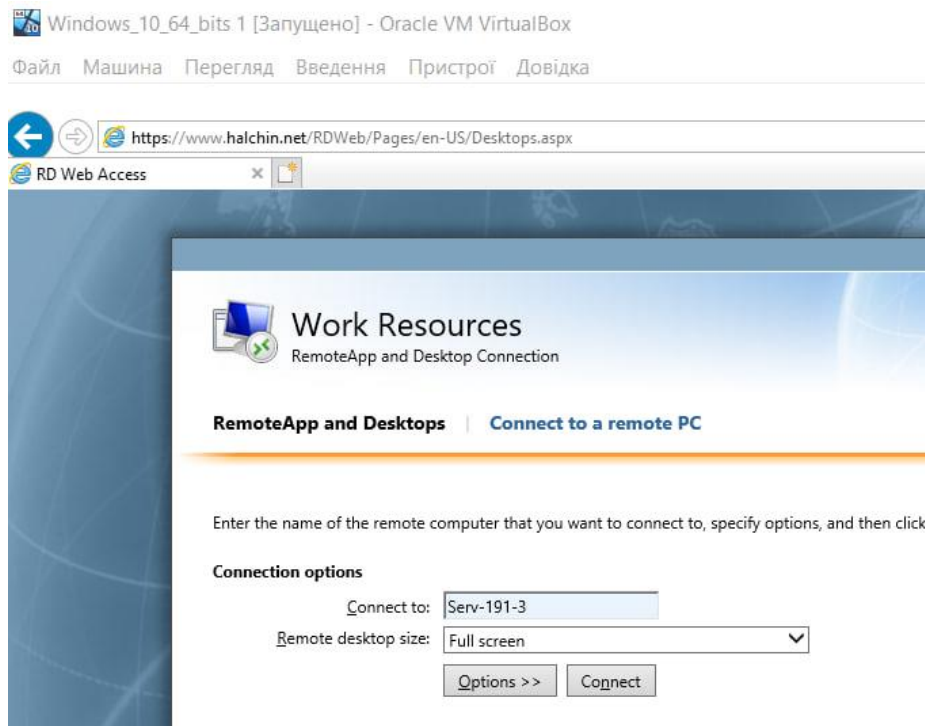


Рис.3.53 Віддалене підключення

На рис. 3.54 показано успішне підключення. Натискаємо на значок замка та отримуємо інформацію, що підключення захищене.

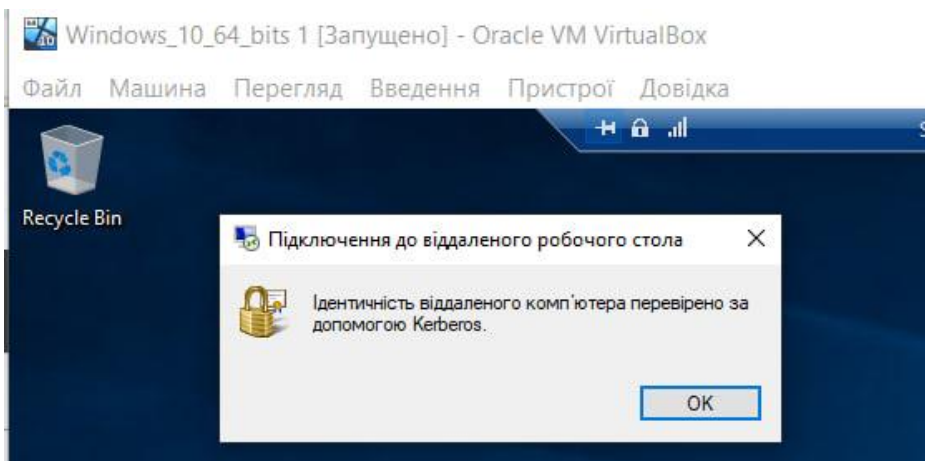


Рис.3.54 Безпечне з'єднання

Висновки до третього розділу

В даному розділі було покроково розписано процес встановлення Active Directory Certificate Services, створення сертифікату, а також перевірка сертифікату... .

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

ВИСНОВКИ

Під час виконання курсової роботи було виконано налаштування Active Directory на базі Windows Server.

В першому розділі було виконано опис теоретичних відомостей про центр сертифікації, переваги та недоліки створення центру сертифікації, розглянуто сертифікати SSL, а також виконано порівняння служб сертифікацій.

В другому розділі було наведено таблицю ір-адресації та вказано інструкції щодо встановлення Windows Server та проведено налаштування ролей Active Directory, таких як DNS, Domain Services та RDP.

В третьому розділі було покроково розписано процес встановлення Active Directory Certificate Services, створення запиту на сертифікат, а також показано створення сертифікату та виконано перевірку на його працездатність.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Server Certificate Deployment Overview [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment-overview>.
2. Створення власного сервера центру сертифікації [Електронний ресурс] – Режим доступу до ресурсу: https://ssl.org.ua/org_pki.html#gsc.tab=0.
3. Чим відрізняються SSL-сертифікати: самопідписані, Let's Encrypt, від центрів сертифікації [Електронний ресурс] – Режим доступу до ресурсу: <https://ssl.com.ua/blog/ukr/comparison-of-certificates/>.
4. Відкликання сертифікатів [Електронний ресурс] – Режим доступу до ресурсу: https://https.com.ua/check_url_crl_help.html.
5. SSL-сертифікат [Електронний ресурс] – Режим доступу до ресурсу: <https://horoshop.ua/ua/blog/ssl/#%D0%92%D0%B8%D0%B4%D0%B8-%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D1%96%D0%B2>.
6. Active Directory Certificate Services [Електронний ресурс] – Режим доступу до ресурсу: <https://www.encryptionconsulting.com/understanding-active-directory-certificate-services/>.
7. How to Create Certificates with XCA [Електронний ресурс] – Режим доступу до ресурсу: <https://campus.barracuda.com/product/campus/doc/28475773/how-to-create-certificates-with-xca/>.
8. Building a Microsoft Certificate Authority [Електронний ресурс] – Режим доступу до ресурсу: <https://virtuallythere.blog/2018/04/24/making-things-a-bit-more-secure-part-1/>.
9. Create CSR [Електронний ресурс] – Режим доступу до ресурсу: <https://www.digicert.com/kb/csr-creation-ssl-installation-iis-10.htm>.
10. Step-By-Step Procedure To Install An SSL Certificate On The IIS Server [Електронний ресурс] – Режим доступу до ресурсу:

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

<https://theseccmaster.com/step-by-step-procedure-to-install-an-ssl-certificate-on-the-iis-server/>.

		Гальчин А. В.,			ККІК.КР.Б – 123 – 3 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

