Лабораторна робота №16

Розгортання та базове налаштування служби сертифікації у доменному середовищі

Мета: вивчити принципи функціонування інфраструктури відкритих ключів (PKI) та набути практичних навичок встановлення і базового налаштування служби сертифікації Active Directory Certificate Services у середовищі Windows Server 2022 для видачі та використання цифрових сертифікатів у доменній мережі.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-15.

Теоретичні відомості.

У сучасних комп'ютерних мережах важливим завданням є забезпечення конфіденційності, цілісності та автентичності інформації, що передається між користувачами та серверами. Для вирішення цих завдань широко застосовується інфраструктура відкритих ключів (PKI – Public Key Infrastructure), яка забезпечує використання цифрових сертифікатів для криптографічного захисту даних.

Цифровий сертифікат — це електронний документ, який містить інформацію про власника сертифіката, його відкритий криптографічний ключ та цифровий підпис центру сертифікації. Сертифікати використовуються для підтвердження автентичності серверів і користувачів, шифрування переданих даних та створення електронного підпису.

У середовищі операційних систем Windows служба центру сертифікації реалізована за допомогою ролі Active Directory Certificate Services, яка входить до складу серверної операційної системи Windows Server 2022. Дана служба дозволяє розгортати власний центр сертифікації (Certificate Authority, CA), видавати, відкликати та керувати цифровими сертифікатами в межах організації.

Центр сертифікації може використовуватися для видачі сертифікатів веб-серверам, службам віддаленого доступу, мережевим пристроям, користувачам та іншим інформаційним ресурсам. Це забезпечує захищений обмін даними за допомогою протоколів шифрування, зокрема HTTPS, TLS та інших.

Використання власного центру сертифікації у корпоративній або навчальній мережі дозволяє централізовано керувати сертифікатами, підвищити рівень безпеки мережевих сервісів та автоматизувати процес їх видачі у доменному середовищі.

Встановлення ролі сервера сертифікації

На першому етапі необхідно встановити роль служби сертифікації у системі Windows Server 2022. Для цього використовується серверна роль Active Directory Certificate Services, яка дозволяє розгорнути центр сертифікації (Certificate Authority) у доменному середовищі.

У даній лабораторній роботі роль сервера сертифікації буде встановлена на контролер домену DC1, який є єдиним сервером у лабораторному стенді.

Входимо до сервера DC1 під обліковим записом адміністратора домену, відкриваємо Server Manager, обираємо пункт Manage – Add Roles and Features.

У майстрі встановлення ролей виконуємо наступні дії:

- обираємо тип встановлення Role-based or feature-based installation;
- обираємо сервер Serv-22-40-1 (DC1) зі списку серверів;
- у списку ролей встановлюємо прапорець Active Directory Certificate Services;
- після вибору ролі погоджуємося з встановленням додаткових компонентів;
- на сторінці Select the role services for Active Directory Certificate Services обираємо наступні ролі:
  - ✓ Certification Authority — обов'язково. Це базовий компонент, який забезпечує основний функціонал сервера сертифікації: видачу та підпис сертифікатів.
  - ✓ Certificate Enrollment Web Service — рекомендовано для майбутніх сценаріїв. Дозволяє автоматично видавати сертифікати клієнтам і комп'ютерам через групові політики, що зручно для централізованого керування сертифікатами.

- ✓ Online Responder (OCSP) — рекомендовано за потреби для швидкої перевірки відкликаних сертифікатів у великих інфраструктурах.

Інші ролі залишаємо не відміченими, бо їх використання у цьому курсі не планується;

- ✓ Certification Authority Web Enrollment
- ✓ Certificate Enrollment Policy Web Service
- ✓ Network Device Enrollment Service (NDES)

- натискаємо Next, перевіряємо параметри встановлення та натискаємо Install.

Порядок виконання цього майстра інсталяції детально показаний на рис. 16.1.

Після завершення встановлення натиснути Configure Active Directory Certificate Services on the destination server для переходу до налаштування служби сертифікації.

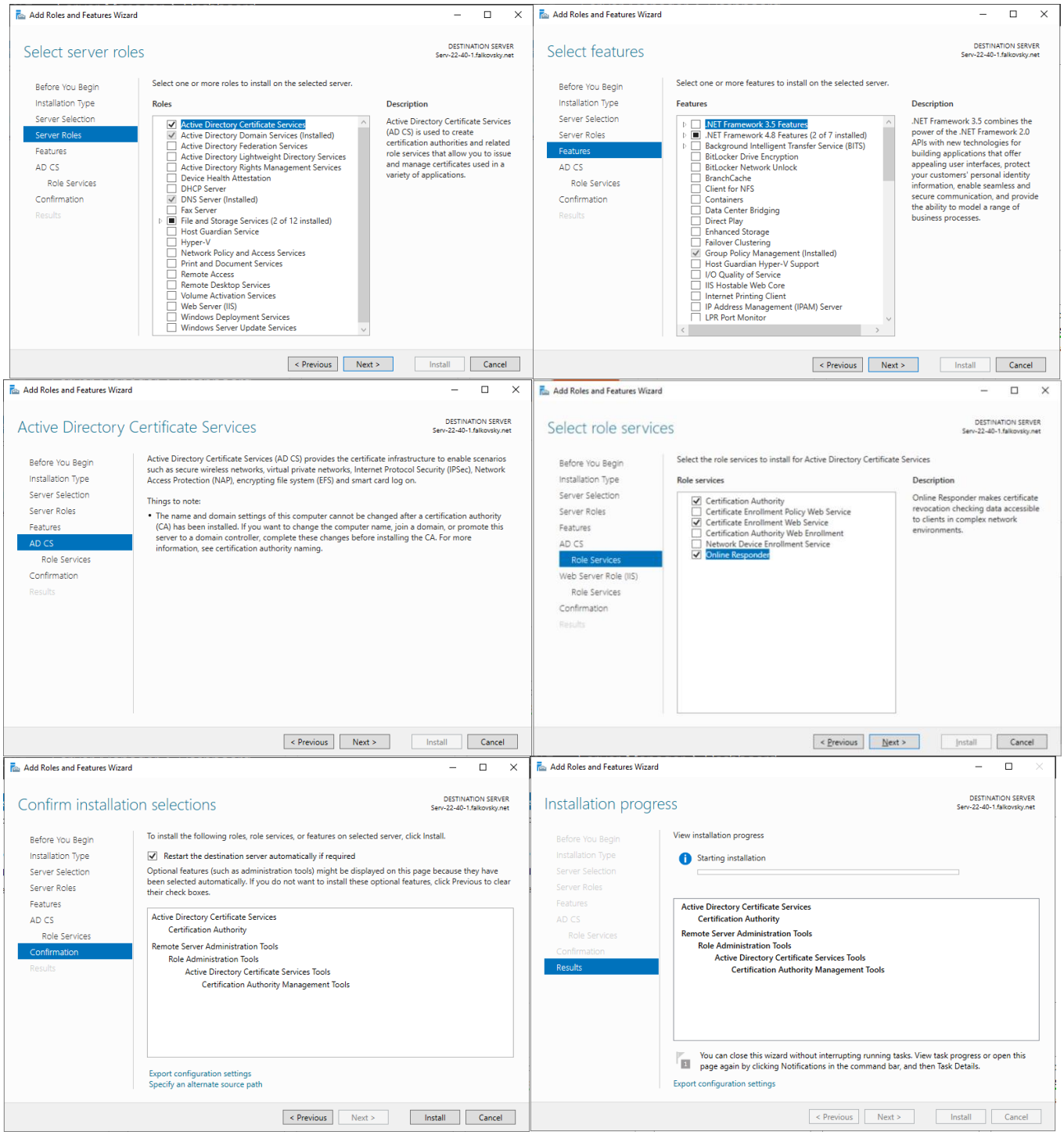


Рис.16.1. Додавання ролі Active Directory Certificate Services

Завдання №16.1.

1. Встановіть роль сервера сертифікації Active Directory Certificate Services на сервері Serv-G-N-1 (DC1) у середовищі Windows Server 2022 за допомогою майстра Add Roles and Features, обравши компонент Certification Authority.

Налаштування центру сертифікації

Після встановлення ролі необхідно виконати додаткову конфігурацію сервера сертифікації. Для цього у вікні Server Manager обираємо Post-deployment Configuration та запускаємо майстер налаштування. Всі кроки показано на рис.16.2, 16.3. У якості встановлюваних ролей обираємо Certification Authority та Online Responder (OCSP). Certification Authority — потребує обов'язкової конфігурації (створення CA, ключів і т.д.). Online Responder (OCSP) може також бути налаштований окремо через MMC (Online Responder snap-in) та потребує вже працюючого CA

На етапі вибору типу сервера сертифікації обираємо Enterprise CA, оскільки сервер працює у доменному середовищі Active Directory. Це забезпечує інтеграцію з доменом, використання шаблонів сертифікатів та можливість автоматичної їх видачі.

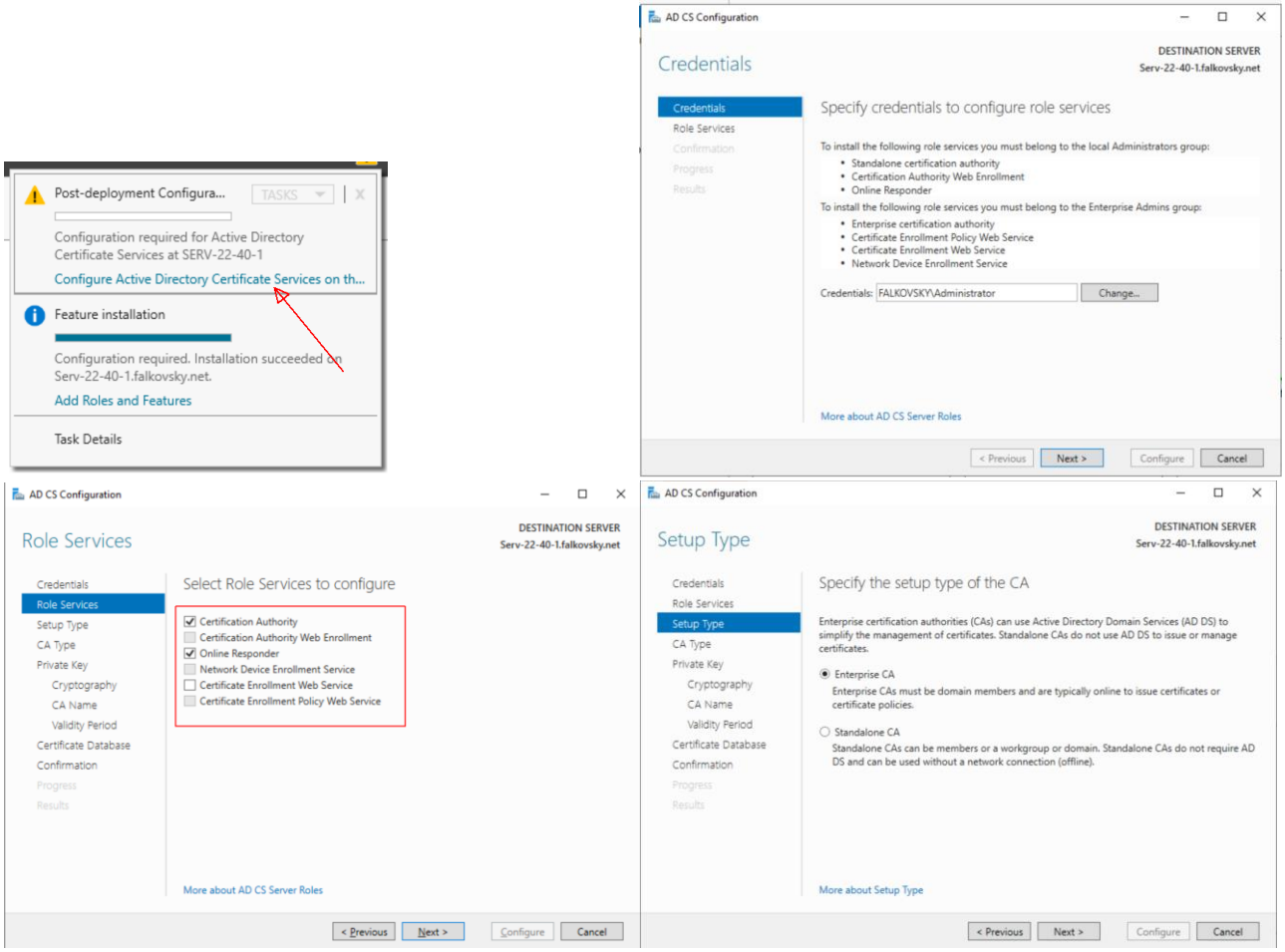


Рис.16.2. Додаткове конфігурування сервера сертифікації

У вікні CA Type обираємо Root CA. Оскільки у даній роботі розгортається перший і єдиний сервер сертифікації, він виконує роль кореневого центру сертифікації.

Коротко про налаштування приватного ключа.

У вікні Private Key обираємо Create a new private key. У вікні Cryptography for CA встановлюємо наступні параметри:

- ✓ Cryptographic provider: RSA#Microsoft Software Key Storage Provider
- ✓ Key length: 2048 (або 4096 для підвищеної безпеки)
- ✓ Hash algorithm: SHA256

Ці параметри забезпечують достатній рівень безпеки для лабораторного середовища та відповідають сучасним вимогам.

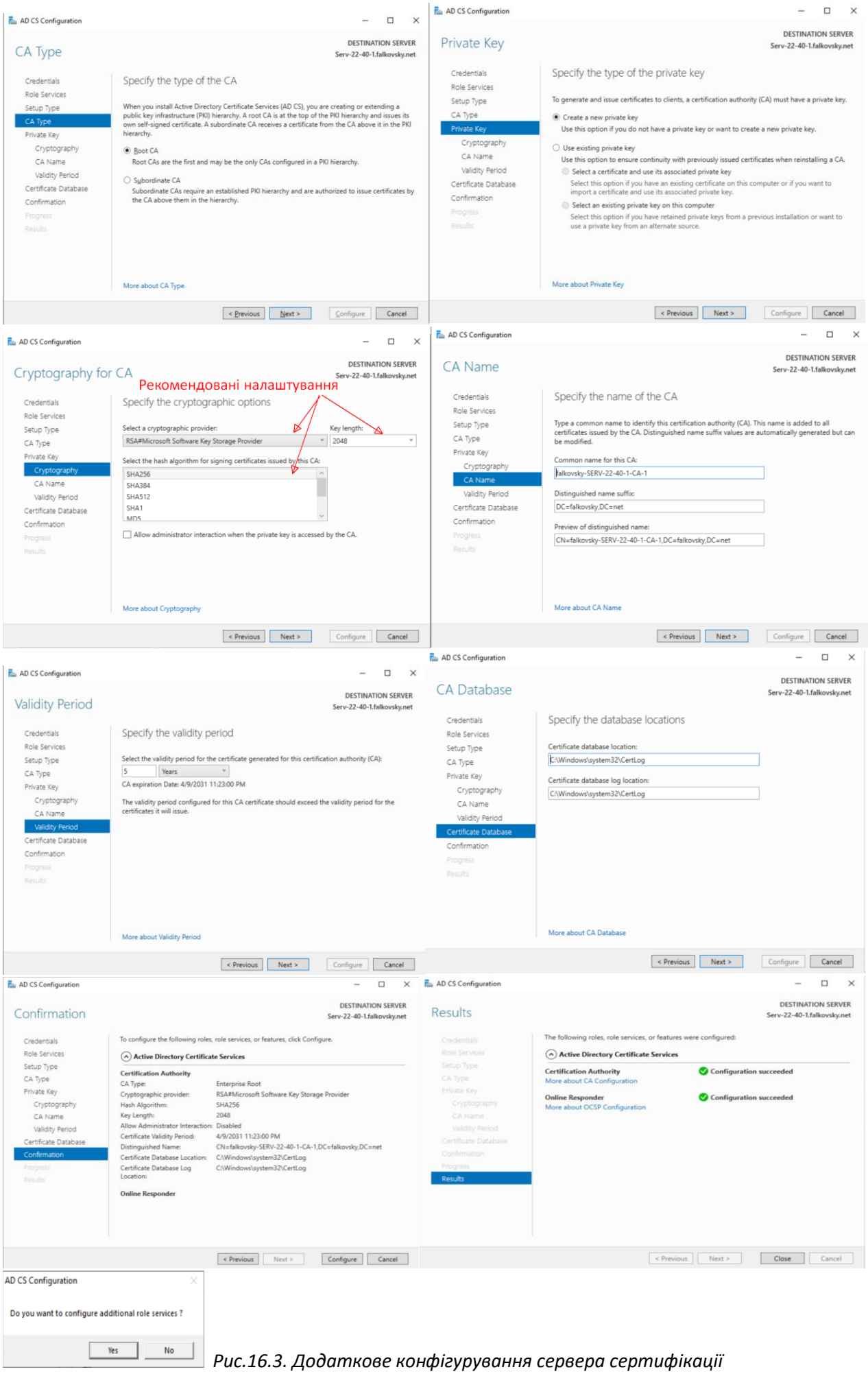


Рис.16.3. Додаткове конфігурування сервера сертифікації

У вікні CA Name залишаємо запропоноване значення або задаємо власне ім’я. Рекомендовано використовувати зрозумілу структуру імені (surname-CA або DC-1-CA). Це ім’я буде використовуватись у всіх виданих сертифікатах як видавець (Issuer), тому має бути однозначним та інформативним.

У вікні Validity Period обираємо термін дії сертифіката CA – 5 років (або інше значення відповідно до вимог). Для лабораторної роботи доцільно встановити стандартний або збільшений термін дії, щоб уникнути необхідності перевипуску ☺

У вікні Certificate Database залишаємо значення шляхів зберігання за замовчуванням. Після перевірки параметрів натискаємо Configure та очікуємо завершення налаштування сервера сертифікації.

Після завершення роботи майстра у системі буде створено та активовано центр сертифікації, який дозволяє видавати цифрові сертифікати для серверів, користувачів та служб доменної мережі.

Завершивши post deploy, відмовляємось від конфігурування додаткових ролей сервісів.

Також відмовляємось (поки що) від виконання другого етапу Post-deployment Configuration. Він призначений для налаштування служби Certificate Enrollment Web Service. Дана служба працює на базі веб-сервера та потребує розгортання і налаштування веб-стеку (IIS), а також додаткової конфігурації SSL.

У межах цієї роботи розгортання веб-інфраструктури не передбачається, тому налаштування цієї служби буде виконано в наступних роботах.

На даному етапі переходимо до генерації сертифіката сервера та перевірки його використання.

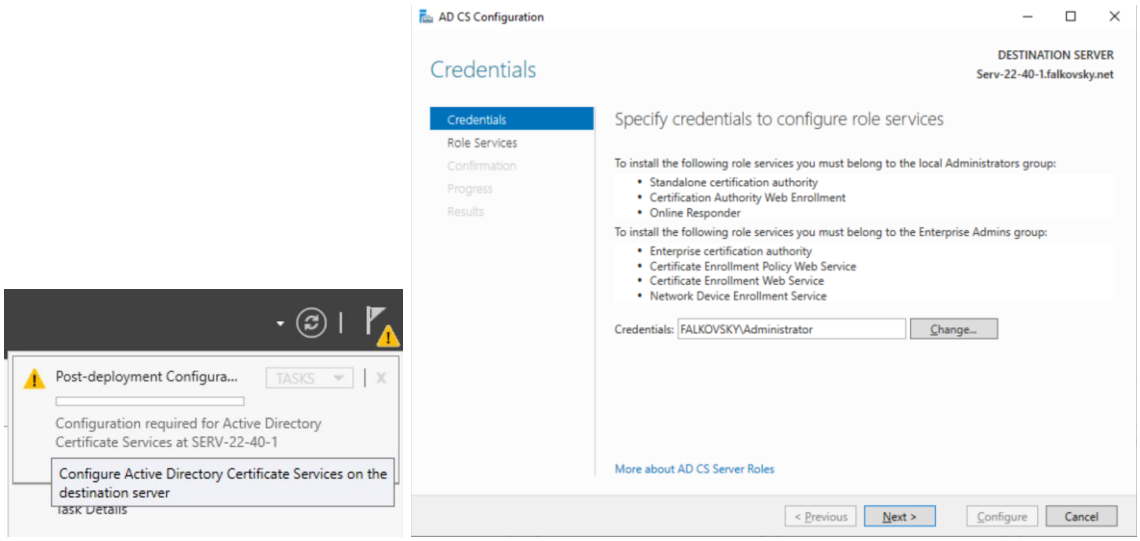


Рис.16.4. Post-deployment Configuration налаштування служби Certificate Enrollment Web Service. (НЕ ВИКОНУЄТЬСЯ У ЦІЙ РОБОТІ)

Завдання №16.2.

1. Виконайте первинне налаштування центру сертифікації після встановлення ролі Active Directory Certificate Services у середовищі Windows Server 2022 за допомогою майстра Post-Deployment Configuration. Під час налаштування створіть центр сертифікації типу Enterprise Root CA.
2. Оберіть створення нового приватного ключа (Create a new private key) та встановіть параметри криптографічного захисту: алгоритм RSA з довжиною ключа 2048 біт і алгоритм хешування SHA256.
3. Вкажіть ім’я центру сертифікації, встановіть термін дії кореневого сертифіката та залиште стандартні параметри зберігання бази даних сертифікатів і журналу сертифікаційних подій.
4. Завершіть роботу майстра конфігурації та переконайтеся, що центр сертифікації успішно створено та готовий до видачі цифрових сертифікатів у доменному середовищі.

Перегляд сертифіката

Після налаштування центру сертифікації необхідно перевірити його роботу шляхом отримання цифрового сертифіката від створеного центру сертифікації. Для цього використовується консоль керування сертифікатами операційної системи Windows Server 2022.

Отриманий сертифікат дозволяє переконатися у працездатності розгорнутого центру сертифікації Active Directory Certificate Services та ознайомитися з процесом видачі сертифікатів у доменному середовищі.

Відкриваємо Server Manager. У правому верхньому кутку обираємо меню Tools де використовується Certification Authority — для перегляду роботи центру сертифікації (рис. 16.5).

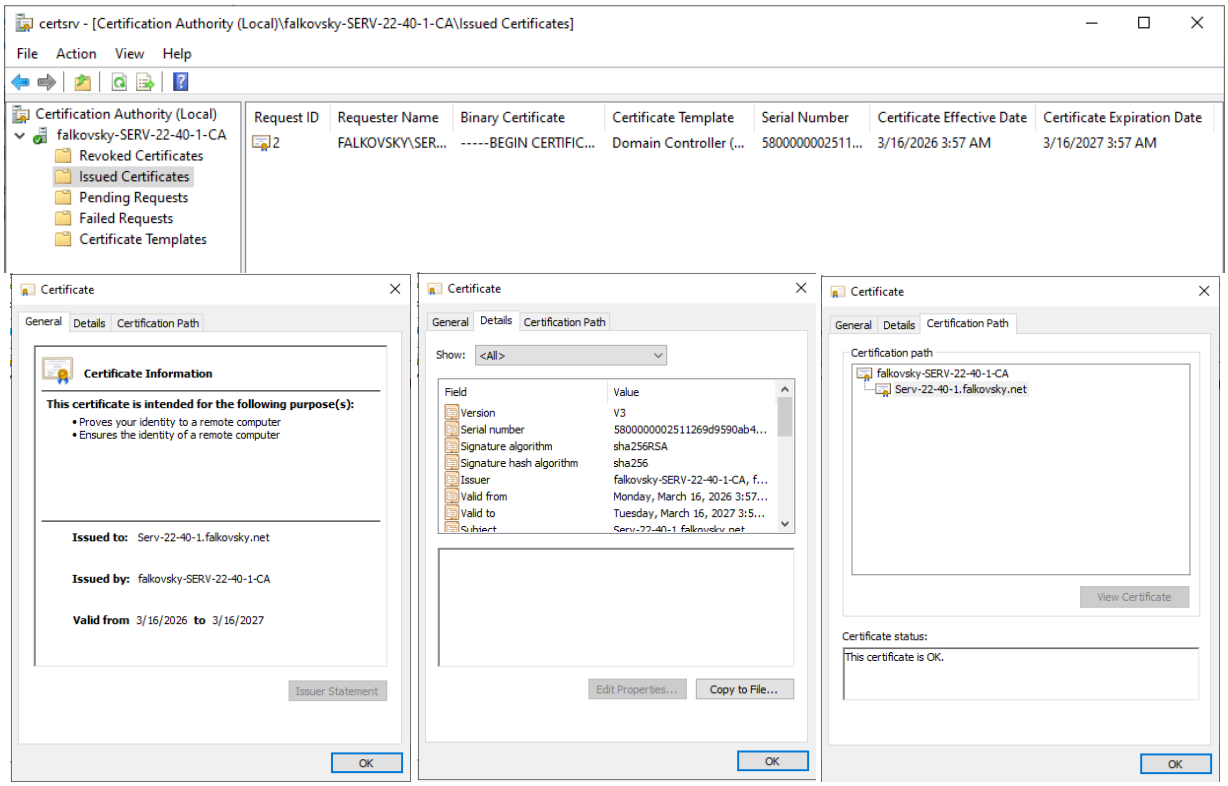


Рис.16.5. Перегляд отриманого сертифіката у Certification Authority Tools

Також можна скористатись універсальною консоллю керування MMC (Microsoft Management Console), яку можна запустити через комбінацію клавіш Win + R та команду mmc. Після запуску необхідно додати оснастку Certificates (File → Add/Remove Snap-in → Certificates → Computer account → Local Computer), що дозволяє переглядати сертифікати локального комп'ютера та перевірити наявність отриманого сертифіката.

У консолі MMC основні сертифікати переглядаються у відповідних сховищах. Сертифікати, видані даному серверу, знаходяться у розділі Personal → Certificates, тоді як кореневі сертифікати центру сертифікації — у Trusted Root Certification Authorities → Certificates.

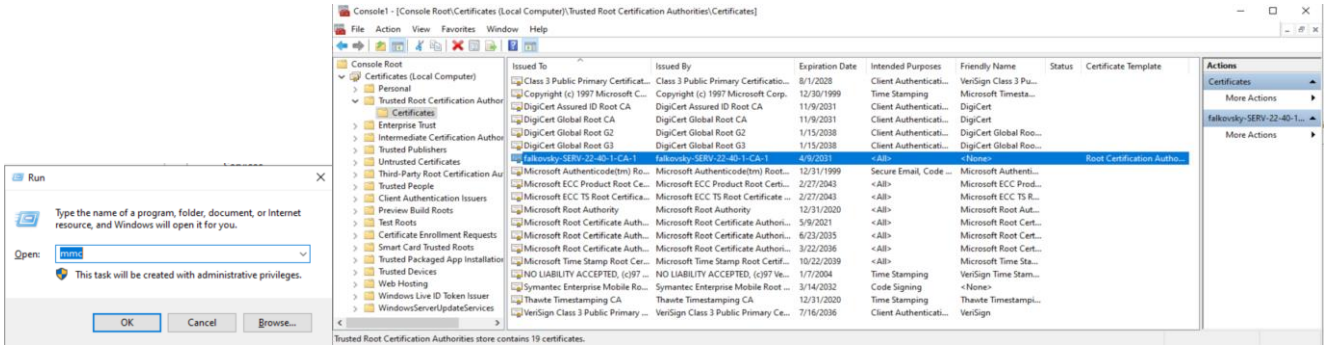


Рис.16.6. Перегляд отриманого сертифіката у Trusted Root Certification Authorities (Certificates)

Завдання №16.3.

1. Перегляньте атрибути створеного сертифікату. Чи є невідповідності та помилки.
2. Під яким іменем записаний згенерований сертифікат у центрі сертифікації Active Directory Certificate Services та у Trusted Root Certification Authorities (Certificates)

Додавання ВМ сервера у лабораторний стенд

У попередній лабораторній роботі було виведено з експлуатації контролер домену **Serv-G-N-2 (DC2)**. Для виконання наступних завдань до лабораторного стенду необхідно додати новий сервер у домені з аналогічним ім'ям, такою ж адресою, але без встановлених серверних ролей. Для цього рекомендується використати універсальний шаблон віртуальної машини на базі Windows Server 2022, створений у лабораторній роботі №2. При відсутності (втраті) шаблону, проінсталюйте ще один сервер.

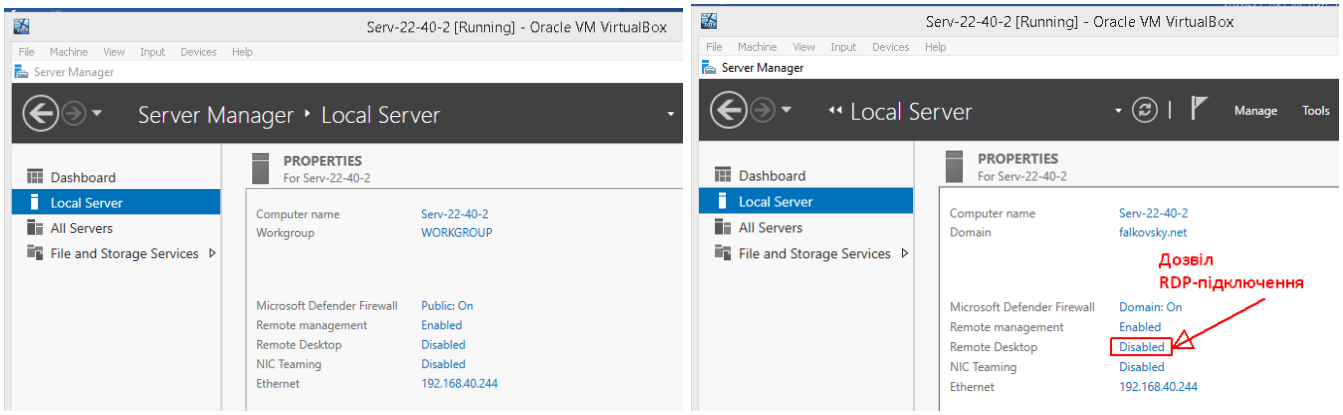


Рис.16.6. Local Server Properties for Serv-22-40-2 до та після включення до домену.

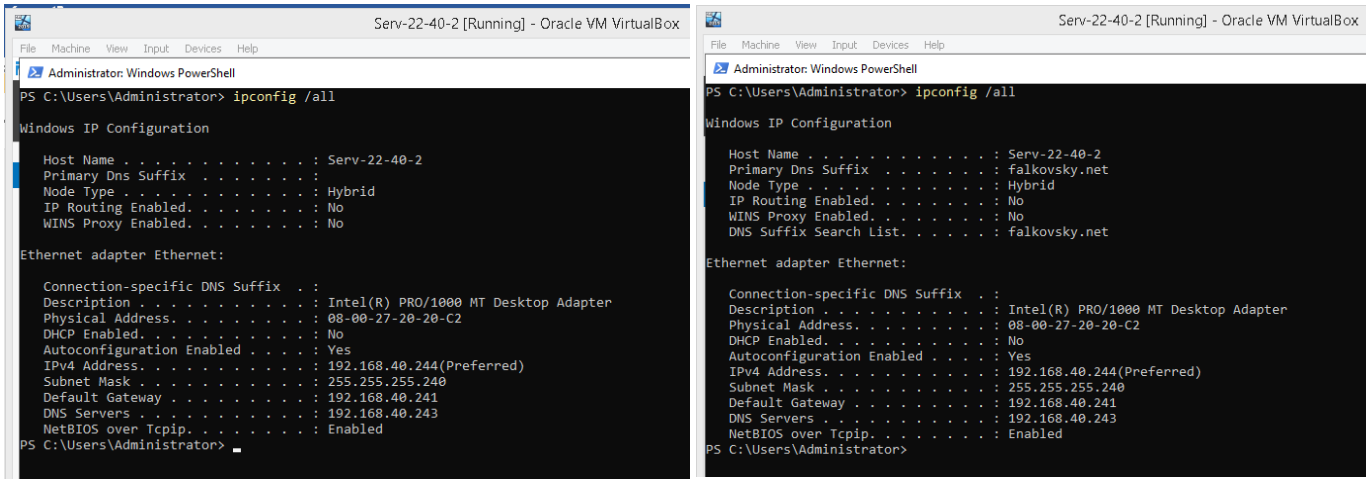


Рис.16.7. ipconfig /all у консолі Serv-22-40-2 до та після включення до домену.

Отримання сертифікату сервера.

Для налаштування захищеного зв'язку на сервері виконаємо запит сертифікату безпосередньо на комп'ютері, для якого він призначений. Це дозволяє забезпечити унікальність та безпеку приватного ключа.

Запит сертифіката виконується під доменним обліковим записом на цільовому сервері, що гарантує коректну прив'язку сертифіката до комп'ютера та захищене зберігання приватного ключа.

Таким чином розподіл ролей наступний:

Клієнт (у даному випадку Serv-22-40-2) — запитує сертифікат, встановлює та використовує його, а CA (сервер сертифікації) (Serv-22-40-1, DC-1) — видає сертифікати, підписує їх та зберігає базу сертифікатів.

На сервері Serv-22-40-2 відкриваємо меню Start і у полі пошуку вводимо mmc, або через комбінацію клавіш Win + R та команду mmc. Відкриваємо Microsoft Management Console.

У меню обираємо File → Add/Remove Snap-in та обираємо у списку Certificates і натискаємо Add → Computer account → Next → Finish → OK

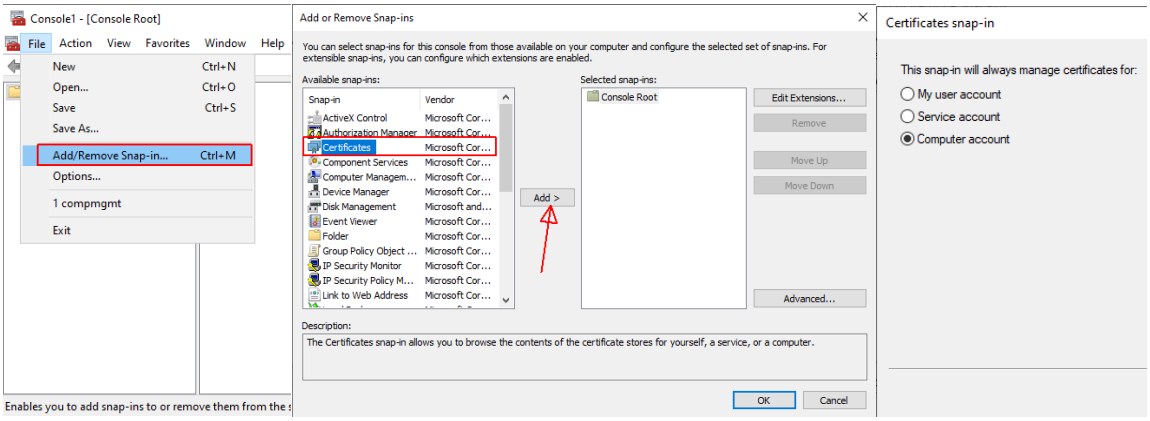


Рис.16.8. Додавання Snap-in сертифікату ПК на Serv-22-40-2.

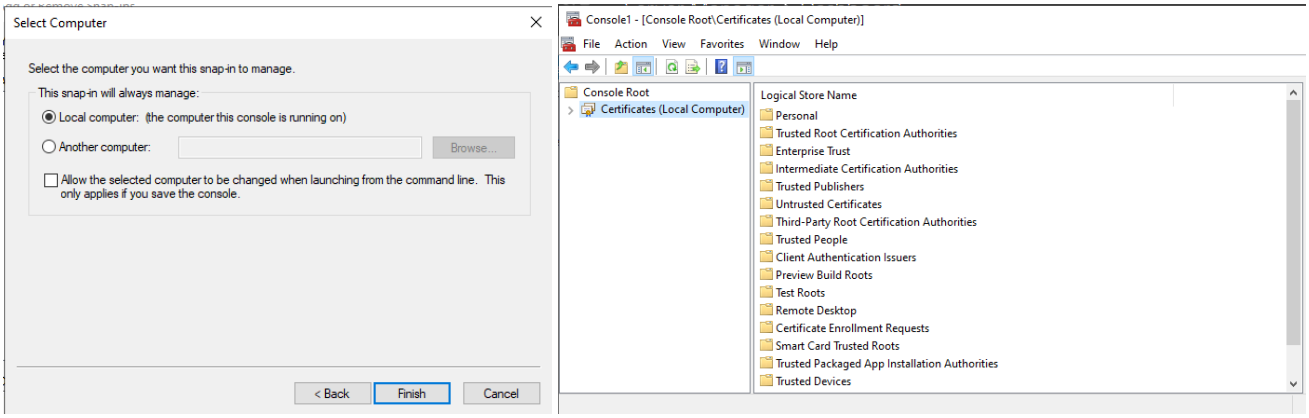


Рис.16.9.Додавання Snap-in сертифікату ПК на Serv-22-40-2.

Примусово оновлюємо політики сертифікатів на Serv-22-40-2 у командному рядку під адміністратором домену:

gpupdate /force

certutil -pulse

Після додавання оснастки Certificates у консолі MMC переходимо до виконання запиту сертифіката.

У лівій частині вікна відкриваємо Certificates (Local Computer) → Personal. Натискаємо правою кнопкою миші на розділі Certificates та обираємо All Tasks → Request New Certificate

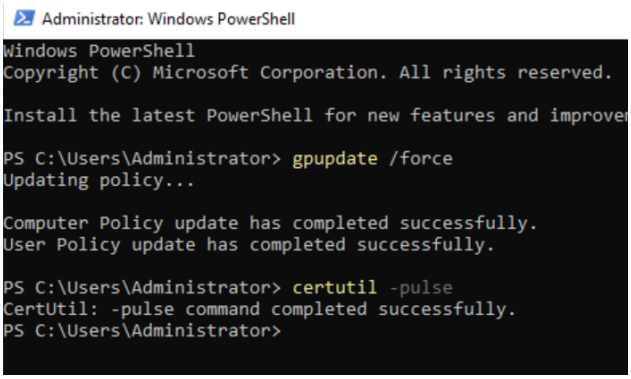


Рис.16.10.Оновлення політик

У вікні Select Certificate Enrollment Policy залишаємо значення за замовчуванням (Active Directory Enrollment Policy) та натискаємо Next та обираємо шаблон сертифіката Computer. Після вибору шаблону натискаємо Enroll. Після успішного виконання з'явиться повідомлення про те, що сертифікат встановлено. Натискаємо Finish.

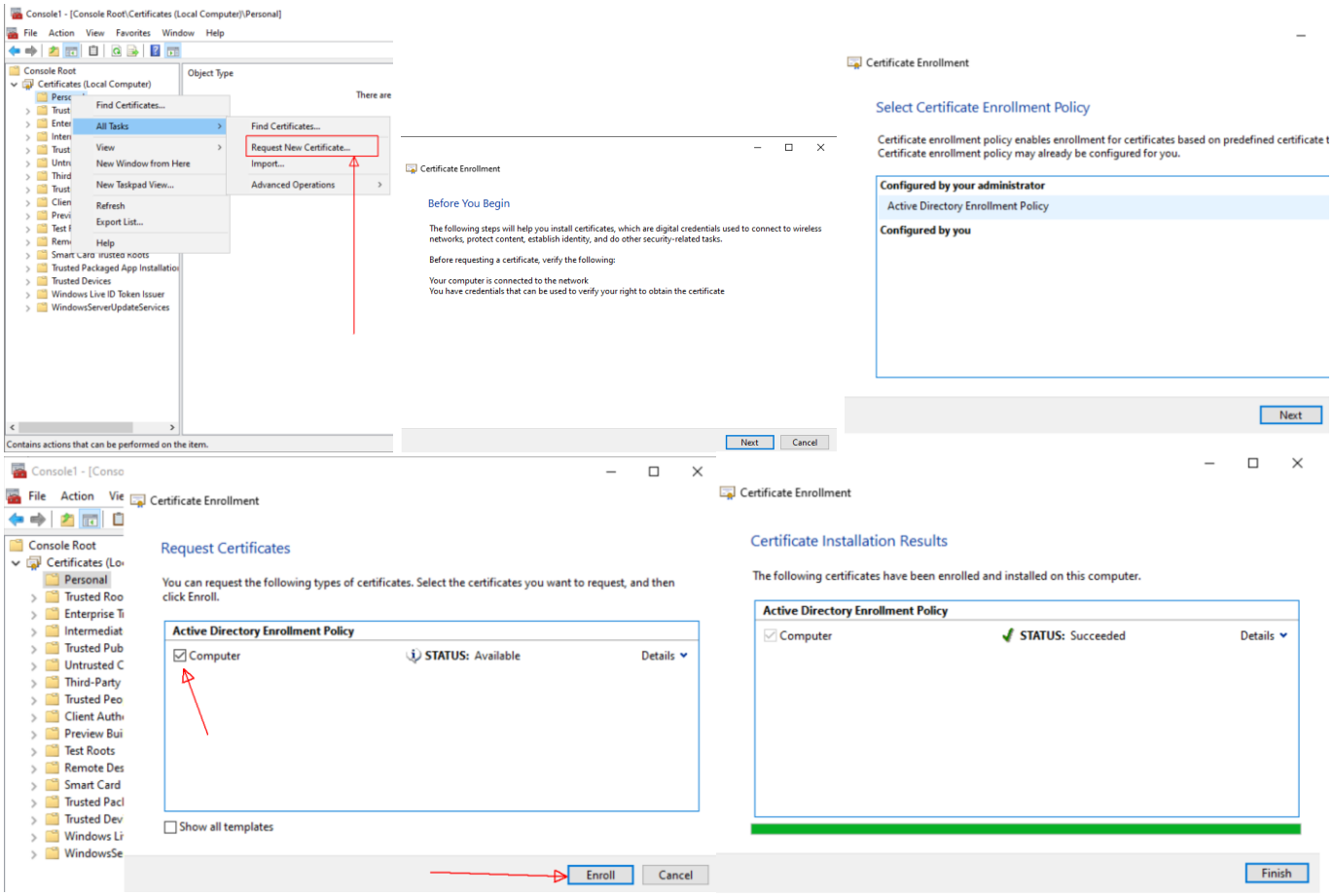


Рис.16.11.Запит та отримання Computer Sertificate для Serv-22-40-2.

У папці Certificates знаходимо отриманий сертифікат, відкриваємо його та перевіряємо:

- ✓ Issued to: Serv-22-40-2
- ✓ Issued by: центр сертифікації
- ✓ Enhanced Key Usage:
- ✓ Server Authentication

Перевірка у центрі сертифікації

Для підтвердження видачі сертифіката перевіримо його на сервері сертифікації.

На сервері Serv-22-40-1 (DC-1) відкриваємо Server Manager → Tools → Certification Authority. У консолі переходимо до <Ім'я CA> → Issued Certificates.

У списку виданих сертифікатів знаходимо сертифікат, виданий для сервера Serv-22-40-2, та перевіряємо:

- ✓ поле Issued To — ім'я сервера
- ✓ поле Certificate Template — Computer
- ✓ поле Issued By — ім'я центру сертифікації

Наявність сертифіката у списку підтверджує успішну роботу центру сертифікації та коректне виконання запиту сертифіката клієнтом.

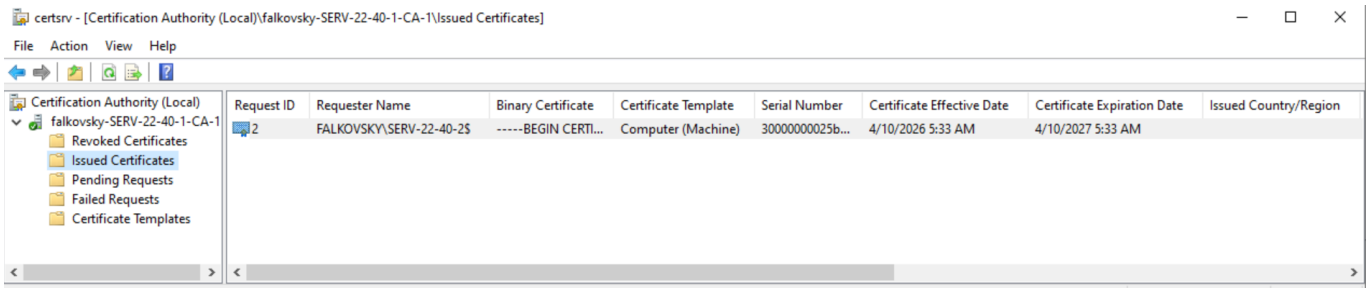


Рис.16.12.Перегляд сертифікату Serv-22-40-2 у Certification Authority DC

Таким чином, було виконано розгортання центру сертифікації, налаштування його основних параметрів та отримання серверного сертифіката у доменному середовищі.

Завдання №16.4.

1. Додайте у домен Serv-G-N-2 серверний хост без встановлених ролей.
2. Отримайте сертифікат комп'ютера для сервера Serv-G-N-2 за допомогою центру сертифікації Active Directory Certificate Services.
3. Після отримання сертифіката перевірте його наявність та основні атрибути:

✓ на сервері Serv-22-40-2 — у консолі MMC (Certificates → Personal → Certificates)

✓ на сервері сертифікації Serv-22-40-1 (DC-1) — у консолі Certification Authority → Issued Certificates)

Зверніть увагу на відповідність полів Issued To, Issued By та шаблону сертифіката.

Корисні посилання

Microsoft ca
https://fact.huastlor.cx.ua/articles/microsoft-ca.html