Лабораторна робота №15

Діагностика та усунення наслідків відмови контролера домену Active Directory

Мета: вивчити методи діагностики порушення реплікації Active Directory та набути практичних навичок усунення наслідків відмови контролера домену у середовищі Windows Server 2022.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №1-14.

Теоретичні відомості.

У доменній інфраструктурі на базі Active Directory ключову роль відіграють контролери домену. Контролер домену забезпечує автентифікацію користувачів і комп'ютерів, зберігає базу даних каталогу, обслуговує запити служб каталогу та бере участь у реплікації даних між іншими контролерами домену.

У домені зазвичай використовується кілька контролерів домену. Це дозволяє забезпечити відмовостійкість і безперервність роботи доменної інфраструктури. Усі контролери домену зберігають копію бази даних каталогу та синхронізують зміни між собою за допомогою механізму реплікації.

Під час експлуатації доменної інфраструктури можуть виникати різні типи відмов, які порушують роботу служби каталогів. До найбільш поширених належать:

- вихід з ладу або фізична втрата контролера домену;
- пошкодження або недоступність бази даних каталогу;
- порушення реплікації між контролерами домену;
- помилки у службі DNS, що унеможливлюють пошук контролерів домену;
- помилки конфігурації об'єктів у структурі Active Directory;
- некоректне завершення роботи віртуальних машин або відновлення з застарілих знімків.

Однією з найпоширеніших проблем є втрата або відмова контролера домену. Це може бути спричинено відмовою апаратного забезпечення, пошкодженням операційної системи, видаленням або пошкодженням віртуальної машини чи іншими технічними причинами.

У разі виходу з ладу контролера домену можуть виникати такі проблеми:

- порушення або припинення реплікації між контролерами домену;
- помилки під час автентифікації користувачів;
- неможливість застосування групових політик;
- помилки у службі DNS;
- накопичення помилок у журналах служби каталогів.

Якщо у домені працює лише один контролер домену, його відмова може призвести до повної недоступності доменної інфраструктури. Саме тому у практиці адміністрування систем на базі Windows Server рекомендується використовувати не менше двох контролерів домену, що забезпечує резервування служби каталогів і підвищує надійність системи.

У випадку остаточної втрати контролера домену адміністратор повинен виконати очищення доменної структури від залишкових об'єктів такого сервера. Це дозволяє усунути помилки реплікації, які виникають через спроби інших контролерів домену встановити зв'язок із недоступним сервером.

У цій лабораторній роботі буде змодельовано ситуацію відмови одного з контролерів домену. Для цього буде виконано вимкнення віртуальної машини другого контролера домену (DC2), що імітує його втрату або вихід з ладу. Після цього буде проведено діагностику стану доменної інфраструктури та виконано очищення каталогу від об'єктів недоступного сервера.

Після завершення лабораторної роботи віртуальна машина контролера домену DC2 може бути остаточно видалена із лабораторного середовища, а її місце у подальших роботах займе звичайний сервер, який буде використовуватися для виконання інших практичних завдань.

Перевірка працездатності домену

Перед початком виконання сценарію роботи необхідно переконатися, що домен працює нормально. Послідовно виконуємо команди для перевірки стану реплікації та роботи служб домену:

repadmin /replsummary
repadmin /showrepl
dcdiag
repadmin /syncall /AdeP

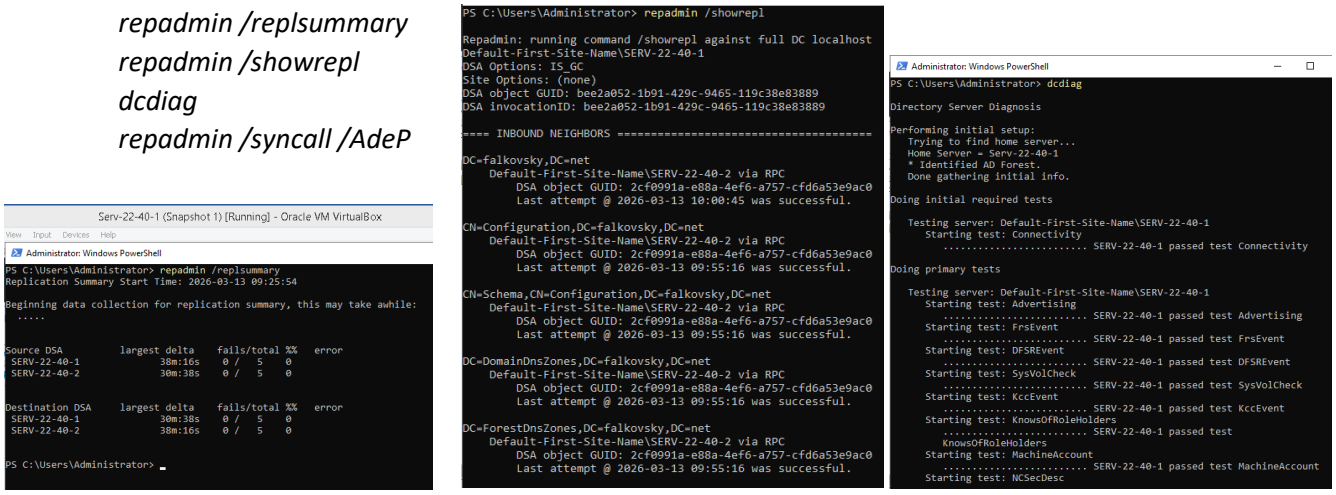


Рис.15.1. Перевірка стану реплікації та роботи служб домену на Serv-22-40-1

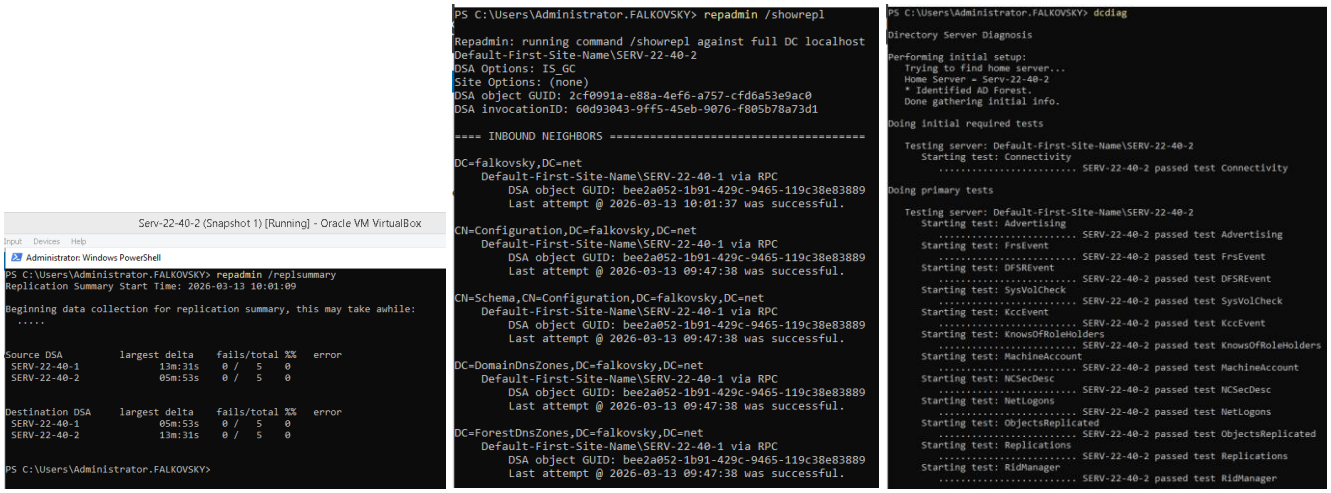


Рис.15.2. Перевірка стану реплікації та роботи служб домену на Serv-22-40-2

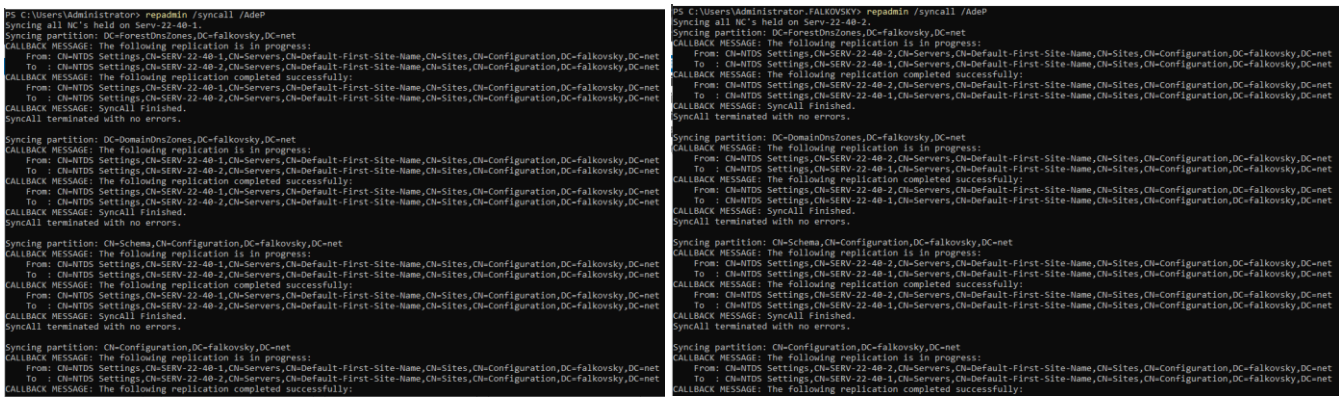


Рис.15.3. Перевірка repadmin /syncall /AdeP на контролерах

Завдання №15.1.

1. На обох контролерах домену увійдіть до системи під обліковим записом адміністратора домену. За допомогою інструментів командного рядка перевірте стан служби каталогів та реплікації між контролерами домену, використовуючи утиліти repadmin та dcdiag.
2. Проаналізуйте результати виконання команд та переконайтесь у відсутності помилок реплікації між контролерами домену.

Імітація аварійного виходу з ладу другого контролера домену.

Імітуємо аварійний вихід з ладу другого контролера домену. Для цього виконуємо примусове вимкнення віртуальної машини другого контролера домену (DC2) засобами гіпервізора. Після вимкнення другого контролера домену на першому контролері домену (DC1) виконуємо примусову перевірку стану реплікації служби каталогів за допомогою команди:

repadmin /syncall /AdeP

Використовуючи команди

repadmin /replsummary

repadmin /showrepl

перевіряємо стан реплікації та аналізуємо повідомлення про помилки, що виникли у зв'язку з відсутністю другого контролера домену.

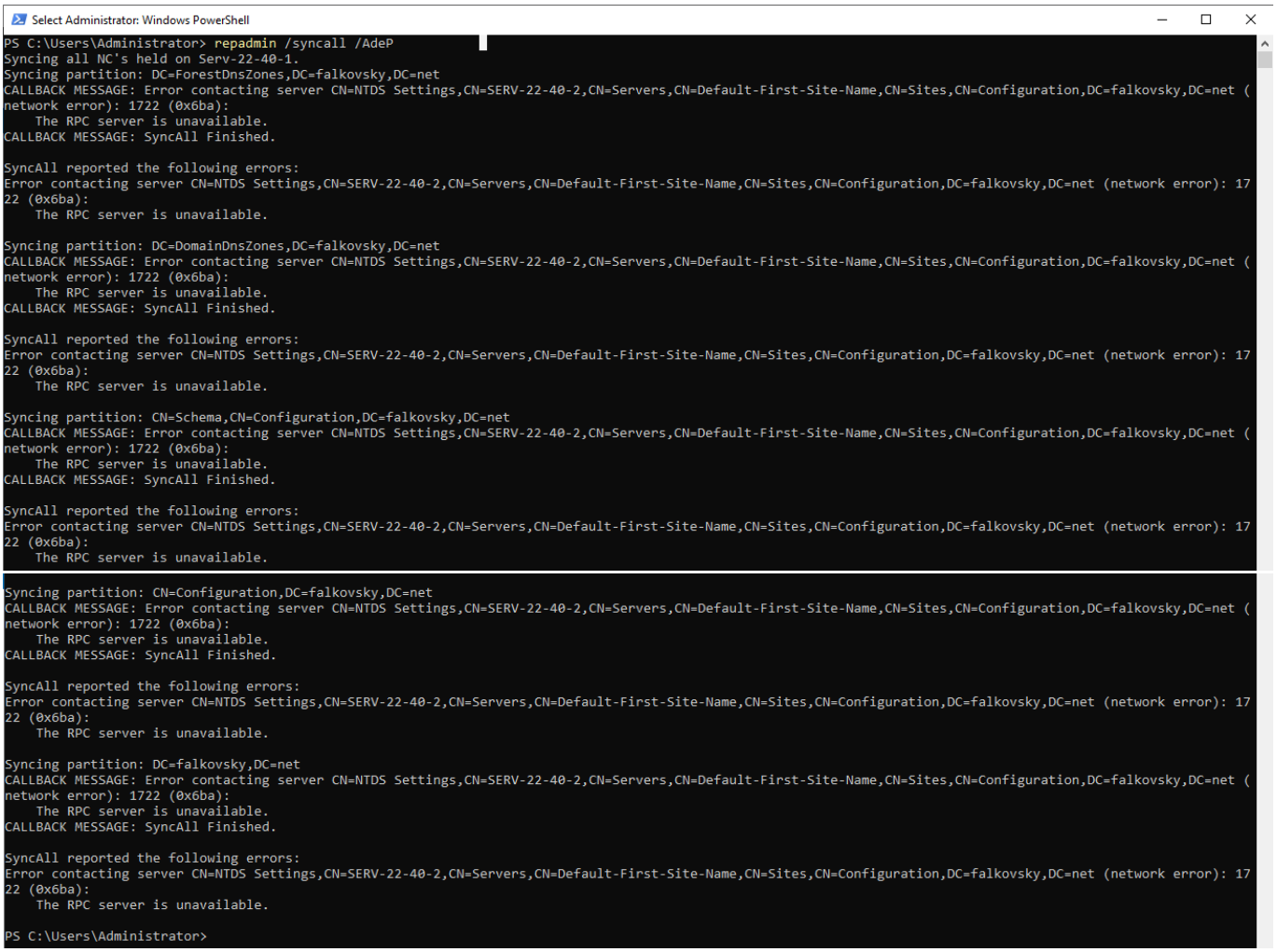


Рис.15.4. Перевірка repadmin /syncall /AdeP на DC1 після вимкнення DC2

Завдання №15.2.

1. Імітуйте аварійний вихід з ладу другого контролера домену. Для цього виконайте примусове вимкнення віртуальної машини другого контролера домену (DC2) засобами гіпервізора.
2. На першому контролері домену (DC1) за допомогою інструментів командного рядка виконайте примусову перевірку стану реплікації служби каталогів, використовуючи утиліту repadmin.
3. Проаналізуйте результати виконання команд та переконайтесь у виникненні помилок реплікації, пов'язаних із недоступністю другого контролера домену.
4. Зафіксуйте отримані результати та зробіть висновок щодо впливу аварійного вимкнення одного з контролерів домену на роботу служби каталогів.

Приведення структури домену у коректний стан. Видалення об'єктів зниклого контролера.

Після аварійної втрати контролера домену його об'єкти залишаються у службі каталогів Active Directory. Для відновлення коректної роботи служби реплікації необхідно виконати очищення метаданих контролера домену.

На першому контролері домену (DC1) відкриваємо оснастку Active Directory Sites and Services та переходимо до структури сайту, у якому розміщені контролери домену. У гілці Servers знаходимо серверний об’єкт, що відповідає другому контролеру домену (DC2). Видаляємо об’єкт NTDS Settings, що відповідає другому контролеру домену. Після цього видаляємо серверний об’єкт DC2 зі структури сайту.

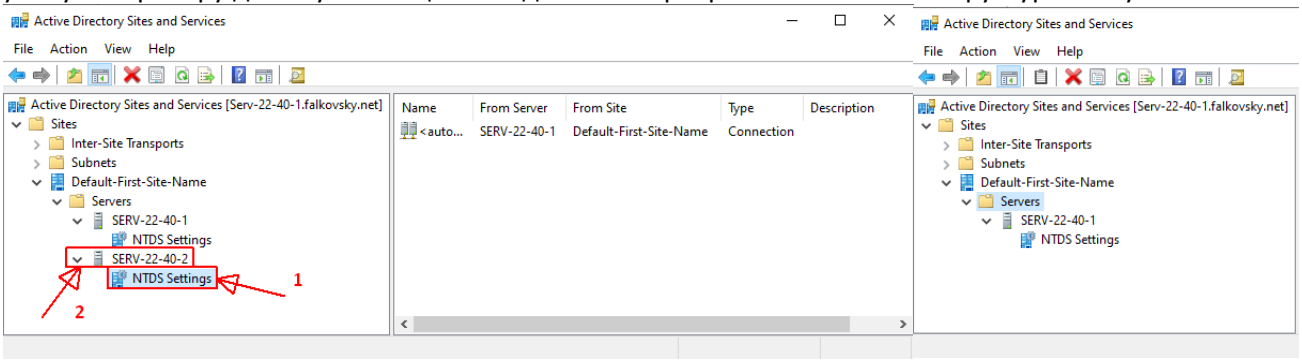


Рис.15.5. Видалення записів DC2 у оснастці Active Directory Sites and Services

Перевіряємо стан служби каталогів за допомогою утиліти repadmin та переконуємось у відсутності спроб реплікації з видаленим контролером домену. Примусова перевірка стану реплікації служби каталогів:

repadmin /syncall /AdeP

Стан реплікації:

repadmin /replsummary

repadmin /showrepl

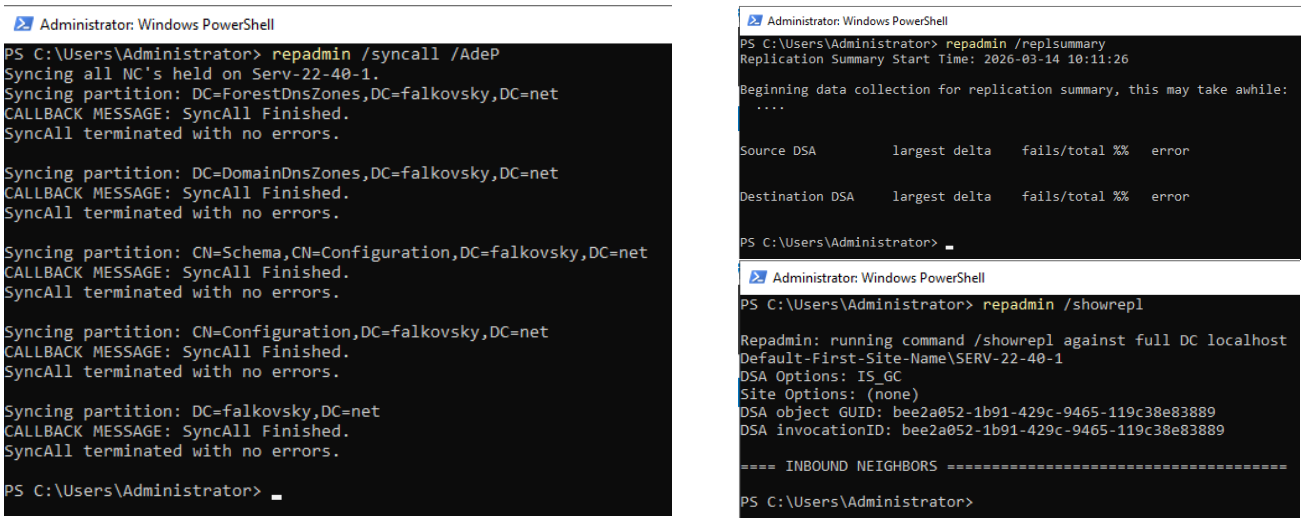


Рис.15.6. Перевірка стану служби каталогів за допомогою утиліти repadmin

Завдання №15.3.

1. На першому контролері домену (DC1) відкрийте оснастку Active Directory Sites and Services та перейдіть до структури сайту, у якому розміщені контролери домену.
2. У гілці Servers знайдіть серверний об’єкт, що відповідає другому контролеру домену (DC2), та відкрийте його структуру. Видаліть об’єкт NTDS Settings, що відповідає другому контролеру домену. Після видалення об’єкта NTDS Settings видаліть серверний об’єкт DC2 зі структури сайту.
3. За допомогою утиліти repadmin перевірте стан реплікації служби каталогів та переконайтесь у відсутності спроб реплікації з видаленим контролером домену.
4. Зафіксуйте отримані результати та зробіть висновок щодо впливу видалення об’єктів недоступного контролера домену на структуру служби каталогів.

Примітка

У реальних корпоративних мережах рекомендується використовувати щонайменше два контролери домену для забезпечення відмовостійкості служби каталогів. У межах даної лабораторної роботи, з метою спрощення подальших експериментів із серверною інфраструктурою, домен тимчасово функціонуватиме лише з одним контролером домену.

У реальній інфраструктурі зазвичай виконують повний metadata cleanup через ntdsutil. Але для навчального стенду видалення через GUI + очищення DNS часто достатньо.

Після успішного виконання завдань цієї лабораторної роботи видаліть, не вмикаючи, віртуальну машину «збійного» контролера домену.

Критично важливо для збереження цілісності доменної структури не вмикати віртуальну машину Serv-G-N-2 (DC2) та повністю видалити її з усіма файлами.

Корисні посилання

Видалення збійного контролера домену з Active Directory
https://surl.li/hexivv

Контролер домену Windows і керування Active Directory
https://surl.li/yjjfeh