Лабораторна робота №8

Налаштування реплікації між двома контролерами домену Active Directory

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

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №3-7.

Теоретичні відомості та завдання до лабораторної роботи

Реплікація в Active Directory

Внутрішньосайтова реплікація (intrasite replication)

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

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

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

Для передавання даних внутрішньосайтова реплікація використовує протокол IP.

Міжсайтова реплікація (intersite replication)

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

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

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

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

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

Робота з оснащенням Active Directory Sites and Services

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

Для запуску оснащення Active Directory Sites and Services у вікні Sever Manager оберіть Tools -> Active Directory Sites and Services (рис. 8.1).

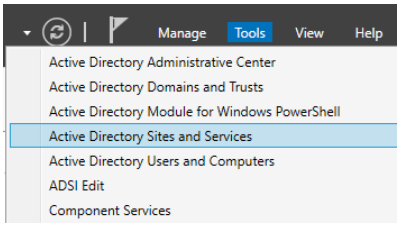


Рис. 8.1

Щоб переглянути з’єднання для конкретного сервера, виберіть *Sites* -> *ім’я сайту* -> *Servers* -> *ім’я сервера* -> *NTDS Settings* (рис. 8.2).

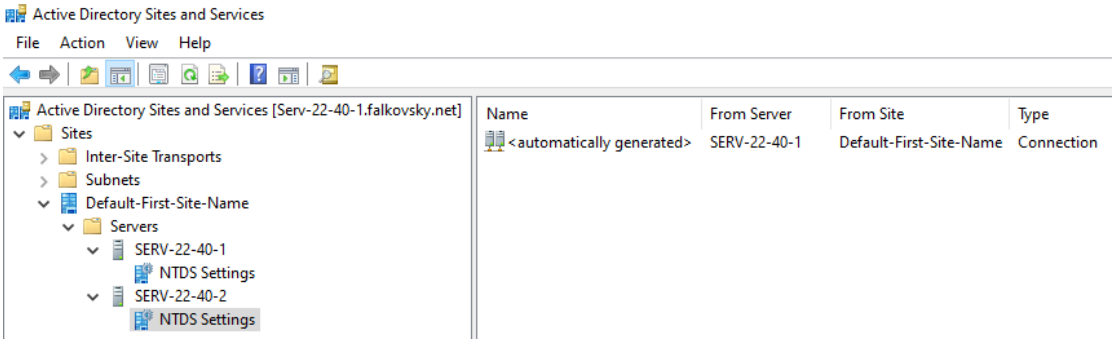


Рис. 8.2

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

Для того, щоб змусити KCC перегенерувати топологію реплікації, оберіть *Sites* -> *ім’я сайту* -> *Servers* -> *ім’я сервера* -> *NTDS Settings* -> *All tasks* -> *Check Replication Topology* (рис. 8.3). Щоб побачити результати, **оновіть** вміст вікна *Active Directory Sites and Servers*.

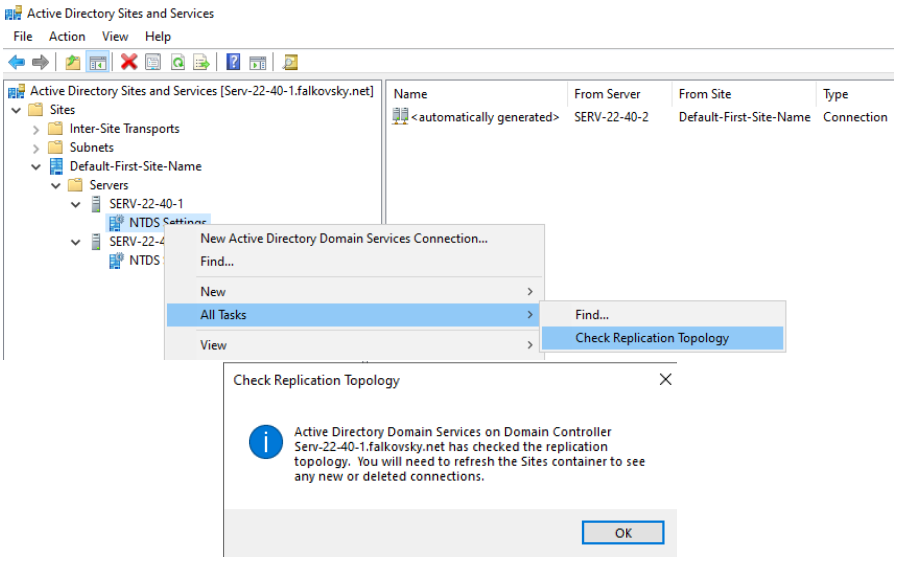


Рис. 8.3

Щоб розпочати примусову реплікацію, зробіть активним вузол *NTDS Settings* відповідного сервера, знайдіть з’єднання, через яке має відбутися реплікація і у контекстному меню цього з’єднання оберіть *Replicate Now* (рис. 8.4). У вашому випадку серверів два, і таку операцію треба повторити на обох.

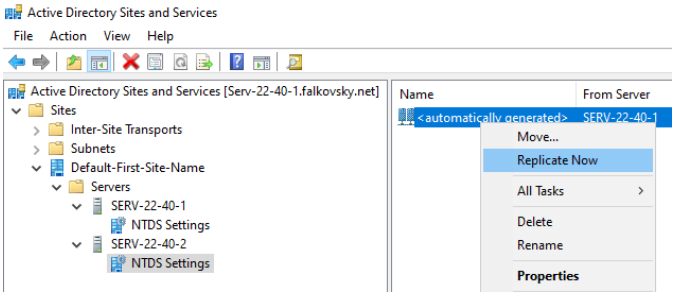


Рис. 8.4

Якщо реплікація успішна, відобразиться повідомлення, подібне до зображеного на рис. 8.5. **Ви маєте одержати таке повідомлення для кожного сервера (у вас їх два).**

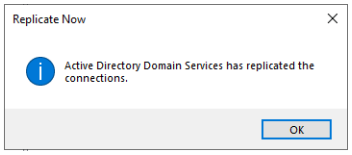


Рис. 8.5

Також примусову реплікацію можна запустити з командного рядка:

repadmin /SyncAll

Наочно побачити, чи успішна реплікація, можна, наприклад, переглянувши структуру домену в оснащенні *Active Directory Users and Computers* (рис. 8.6). Зокрема, якщо ви внесете зміни на першому контролері, то після успішної реплікації структура має співпадати на обох контролерах (рис. 8.6).

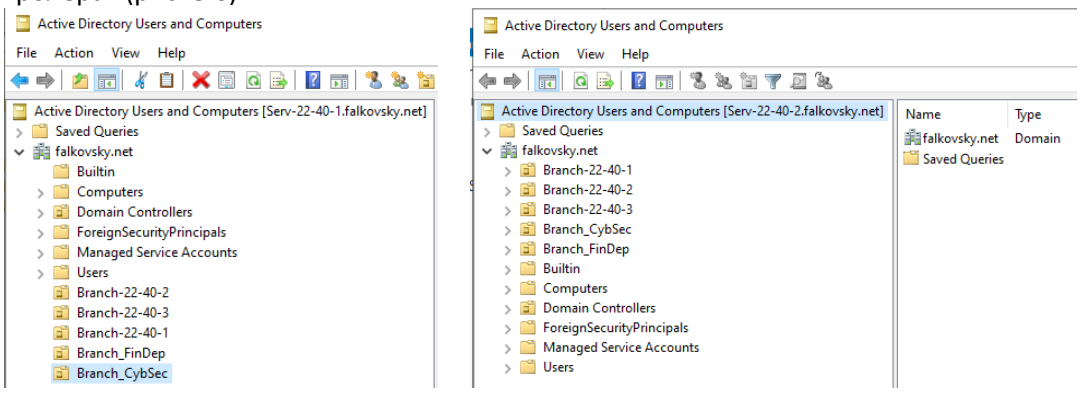


Рис. 8.6

<u>Завдання №8.1</u>. *Дослідження сайтів та наявної топології реплікації*

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

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

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

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

<u>Завдання №8.2</u>. *Дослідження роботи KCC*

1. Видаліть автоматично створені з'єднання для кожного з серверів.
2. Запустіть примусову перевірку топології реплікації.
3. Оновіть вміст вікна *Active Directory Sites and Servers*. Які з'єднання згенерував *KCC*? Чи відрізняються вони від тих, які ви досліджували у **завданні №8.1**.

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

Завдання №8.3. ***Дослідження та налаштування реплікації AD***

1. Запустіть другий контролер домену (перший лишіть ввімкненим також).

2. На другому контролері домену відкрийте оснащення *Active Directory Users and Groups*. Чи відповідає структура домену, що відображається у цьому оснащенні, від тієї, яку ви створювали на першому контролері домену у межах *лабораторних робіт №4* і *№6*? Зробіть висновки про те, чи коректно функціонує реплікація.

3. З першого контролера домену ініціюйте примусову реплікацію на обох серверах. Після одержання двох повідомлень про успішну реплікацію повторіть п. 2.

4. Якщо реплікація не працює так, як очікувалося, з'ясуйте та усуньте причини. Якщо усе гаразд, пропустіть цей пункт.

5. На першому контролері домену додайте до однієї з організаційних одиниць нового користувача.

6. Переконайтеся, що реплікація виконалася успішно і цього разу: цей користувач має відображатися і на другому контролері домену коли перший контролер домену недоступний (відповідна віртуальна машина неактивна), то вхід від імені новоствореного користувача з однієї з робочих станцій домену все одно має вдаватися.

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

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

1) Порушено мережне з'єднання між контролерами домену (перевірте шляхом пінгування, виправте мережні налаштування – у ролі DNS-сервера вкажіть адресу першого контролера домену, інші адреси DNS-серверів приберіть).
2) Проблеми з синхронізацією часу на контролерах домену.

Навіть якщо візуально здається, що годинники на вузлах домену йдуть однаково, для реплікації навіть невелика розсинхронізація може виявитися суттєвою.

Налаштовуємо синхронізацію часу із зовнішнім сервером на **першому контролері домену**:

w32tm /config /manualpeerlist:"pool.ntp.org" /reliable:YES /update

net stop w32time

net start w32time

На **другому контролері домену** налаштовуємо синхронізацію часу з першим контролером:

w32tm /config /syncfromflags:domhier /reliable:YES /update

net stop w32time

net start w32time

Варто повторити дії, які ви робили на другому контролері домену, і на робочій станції.

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

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

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

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

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

Завдання 8.4. Дослідження міжсайтової реплікації

1) В оснащеннні Active Directory Sites and Services оберіть вузол Inter-Site Transports (рис.8.7.)

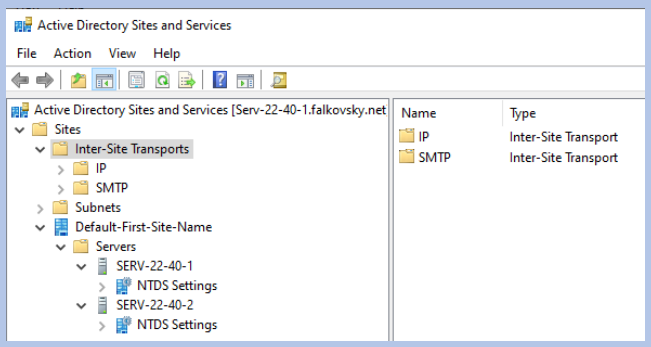


Рис. 8.7.

2) З'ясуйте, який протокол має використовуватися для міжсайтової реплікації. Обґрунтуйте, чому налаштування за замовчуванням зроблено саме таким чином (див. теоретичні відомості).
3) Чи відбувається міжсайтова реплікація зараз? Чому?

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

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 8.1-8.4.