Лекція 5

Реплікація

План

1. Реплікація. Види реплікації
2. Гарні практики, пов’язані з реплікацією

1. Реплікація. Види реплікації

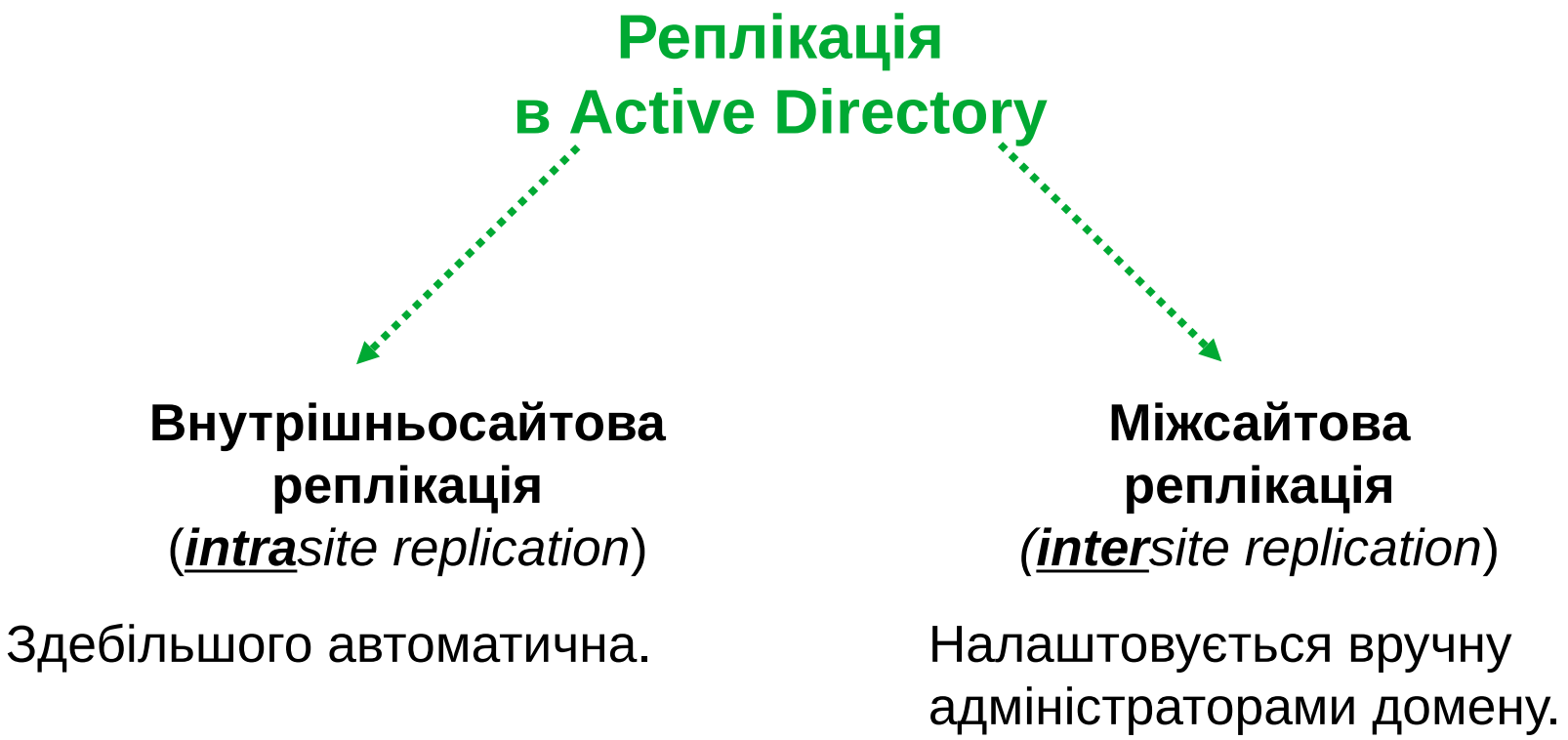
[З попередніх тем]

Реплікація *(replication)* - процес синхронізації всіх копій бази даних домену між контролерами цього домену.

Передається інформація про будь-які зміни.

Результат: всі контролери домену повинні містити точну копію інформації про всі каталоги домену.

1. Реплікація. Види реплікації



1. Реплікація. Види реплікації

Внутрішньосайтова реплікація (*intrasite replication*)

Є здебільшого **автоматичною**.

Внутрішньосайтова реплікація організована **надлишковим чином** (для надійності):

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:

під час реплікації між контролерами домену може бути **досить інтенсивний мережний трафік** — саме тому й існує рекомендація щодо максимально стабільного та швидкого з'єднання всередині сайту Active Directory.

Для передавання даних внутрішньосайтова реплікація використовує **протокол IP**.

1. Реплікація. Види реплікації

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***).

Нюанс: якщо на момент реплікації сервер-плацдарм, якому треба надавати перевагу (preffered bridgehead server) виявиться недоступний, то міжсайтова реплікація не відбудеться.

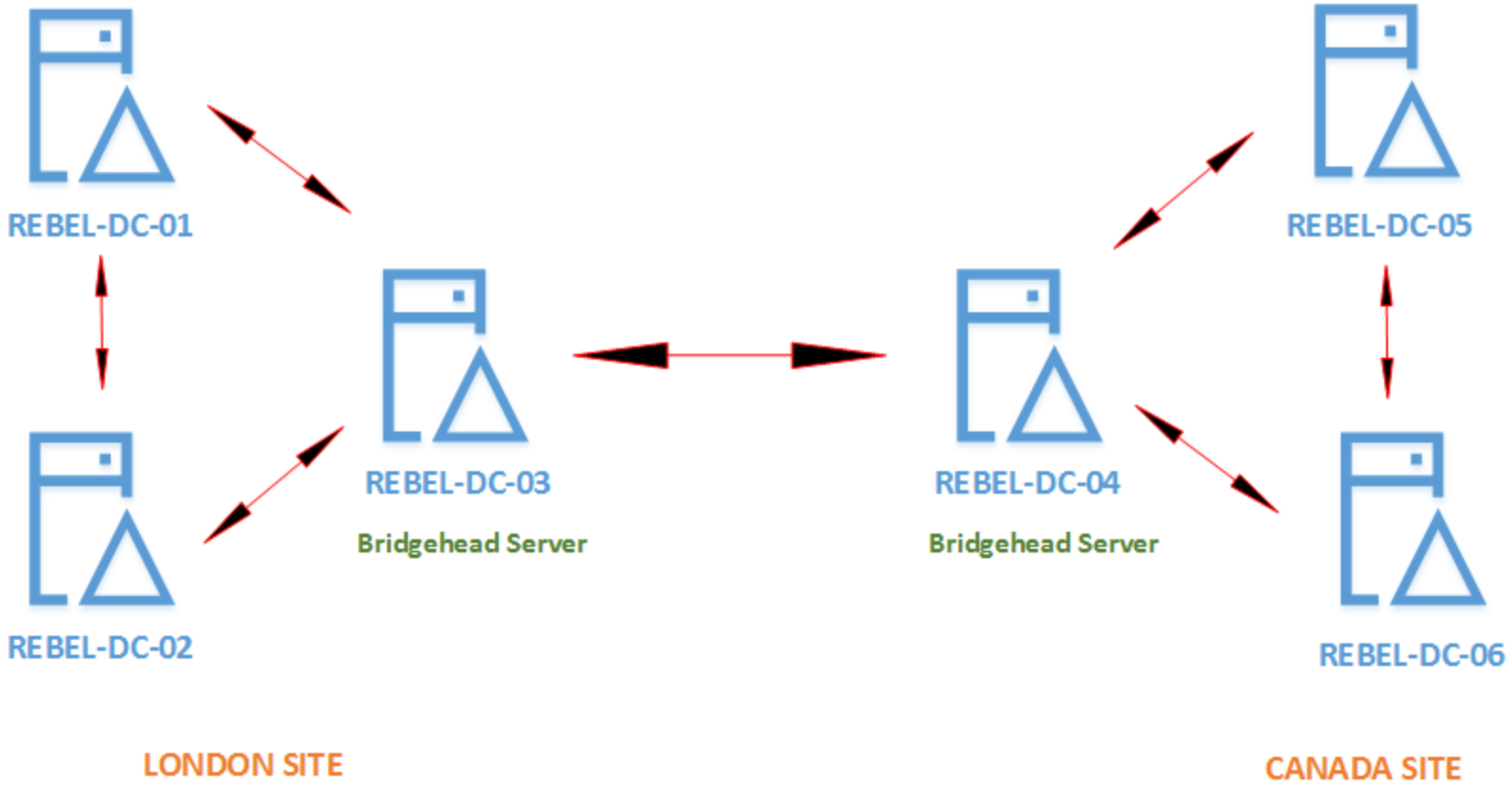
Коли відбувається міжсайтова реплікація:

для міжсайтової реплікації можна задавати **розклад** (наприклад, такий, аби реплікація відбувалася не в період найбільш інтенсивних операцій - скажімо, у неробочі години).

Протокол для міжсайтової реплікації можна обрати:

- RPC over IP (у більшості випадків)
- SMTP (іноді, для старих мереж)

1. Реплікація. Види реплікації



Джерело схеми: https://www.rebeladmin.com/2018/02/active-directory-replication-works/

2. Гарні практики, пов’язані з реплікацією

- Узгодженість бази даних Active Directory є одним з **ключових факторів** нормального функціонування всієї Active Directory.
- Для забезпечення узгодженості (*consistency*) бази даних здійснюється **реплікація**.
- **KCC** (*Knowledge Consistency Checker*) - компонент Microsoft Active Directory, який автоматично генерує топологію для внутрішньосайтової реплікації, а також виконує частину операцій з міжсайтової реплікації.
- KCC забезпечує, щоб між будь-якими двома контролерами домену всередині сайту було **не більше трьох стрибків** (hops).
- У межах **окремого сайту** KCC автоматично генерує топологію і контролює її оптимальність. Втручання адміністраторів тут не потрібне.
- Топологію **між сайтами** розробляють адміністратори AD, коли створюють сайти та з’єднання між ними. До цього процесу треба ставитися з високою відповідальністю, щоб уникнути зайвих затримок.

2. Гарні практики, пов’язані з реплікацією

- Необхідно регулярно здійснювати **моніторинг реплікації** (переглядати загальний звіт — двічі на день, моніторинг реплікації - раз на день).
- Звіти краще зберігати (можна автоматизувати за допомогою скриптів PowerShell або спеціалізованого ПЗ). Зберігання краще зробити централізованим.
- Найпоширеніша причина помилки реплікації — **недоступність контролера домену** через проблему мережі, обладнання чи неправильні налаштування фаєрволу. Але причина може бути серйознішою, тому помилки реплікації не можна ігнорувати.
- Використовуйте налаштування **строгої узгодженості реплікацій** (*Strict Replication Consistency*) на всіх контролерах домену.
- Не варто лишати контролер домену вимкненим протягом тривалого часу (більше 160 днів). Інакше можуть з’являтися **застарілі об’єкти** (*lingering objects*).

2. Гарні практики, пов’язані з реплікацією

Застарілі об’єкти (*lingering object*) — це об’єкти Active Directory, які було видалено з бази, але які знову з’явилися на одному з контролерів AD, коли той було відновлено.

Якщо контролер довго не працював, його екземпляр бази даних може відрізнятися від актуальної бази AD. Якщо у базі щось видалялося, вимкнений контролер про це “не знає”.

Щоб інформувати всі контролери про те, що певний об’єкт видалено, в AD існують спеціальні сутності — **меморіальні об’єкти** (*tombstone objects*). Але ці об’єкти з часом видаляються (зазвичай через 160 днів).

Застарілі об’єкти виникають через те, що меморіальні об’єкти, які мали засвідчити, що цих об’єктів у базі вже не має бути, видалилися до початку відновлення контролера.