Przywracanie DC

USN (Update Sequence Number) to lokalny licznik zmian w bazie Active Directory, prowadzony przez każdy kontroler domeny oddzielnie.

Główne cechy i zastosowanie:

1. **Indywidualny dla każdego DC**
    - Każdy kontroler domeny posiada własne, niezależne USN, które rośnie za każdym razem, gdy dokonuje się jakakolwiek modyfikacja danych w AD na tym kontrolerze (np. utworzenie użytkownika, modyfikacja obiektu).
2. **Mechanizm śledzenia replikacji**
    - W trakcie replikacji kontrolery domeny porównują m.in. swoje USN, aby ustalić, które zmiany są nowsze i powinny zostać przesłane/przyjęte.
    - Dzięki temu system wie, które wpisy w bazie należy zreplikować, a które są już aktualne.
3. **Ryzyko „USN rollback”**
    - W pewnych sytuacjach, np. przy przywróceniu kontrolera domeny z przestarzałego snapshotu lub kopii, USN może ulec cofnięciu do wartości sprzed replikowanych zmian.
    - Inne kontrolery nie oczekują cofnięcia licznika i może dojść do niespójności danych (błędnej replikacji).
    - Dlatego bardzo ważne jest stosowanie wspieranego modelu przywracania (np. VM Generation ID, nieautorytatywne przywracanie w trybie DSRM czy całkowite odbudowanie DC).

Przykładowy scenariusz :

Przy dwóch kontrolerach domeny (DC1 i DC2), w sytuacji gdy DC1 uległ awarii i chcemy go odtworzyć z backupu maszyn wirtualnych, należy wziąć pod uwagę ryzyko tzw. „USN rollback" (błędna replikacja) oraz zalecane praktyki Microsoft. Poniżej ogólny, bezpieczny scenariusz:

<u>Środowiska fizyczne</u>

1. **Rozważ alternatywę „zbuduj od nowa"**

   Z punktu widzenia prostoty i bezpieczeństwa często zaleca się nie przywracać „starego" DC1 z backupu, lecz całkowicie go usunąć z Active Directory i doinstalować nowy kontroler (pod tą samą nazwą lub inną).

   - Na działającym DC2 usuń wpisy DC1 (np. poprzez metadata cleanup).
   - Przywróć system/maszynę z kopii zapasowej (jeśli to konieczne – opis w dalszych krokach), albo szybciej „postaw" nowy serwer i zainstaluj na nim rolę AD DS (promuj do kontrolera).

Jest to często najłatwiejsze i najbardziej rekomendowane podejście, jeśli mamy drugi poprawnie działający kontroler domeny.

2. **Jeśli jednak MUSISZ przywrócić DC1 z backupu**

   - **Upewnij się, że backup nie jest starszy niż okres przechowywania obiektów usuniętych (tombstone lifetime)** – standardowo 180 dni.
   - **Odłącz przywracany DC1 od sieci** (lub uruchom w izolowanej sieci), by uniknąć konfliktów replikacji.
   - Przywróć maszynę DC1 z backupu.
   - Po uruchomieniu w Trybie Przywracania Usług katalogowych (DSRM) wykonaj **przywracanie nieautorytatywne** (non-authoritative restore) bazy AD z poziomu kopii zapasowej system state (jeśli jest taka możliwość). W przypadku przywrócenia całej VM, jeżeli jest wspierana funkcja VM Generation ID (Windows Server 2012+ na hypervisorze wspierającym tę technologię), to system powinien automatycznie wykryć odtworzenie z „migawki" i wyzerować numery USN – minimalizuje to ryzyko USN rollback.
   - Po poprawnym przywróceniu, **włącz replikację** z DC2 (podłącz DC1 do tej samej sieci). DC1 pobierze najnowsze zmiany z DC2.

3. **Weryfikacja**
    - Sprawdź stan replikacji (polecenie repadmin /replsummary lub w konsoli Active Directory Sites and Services).
    - Przejrzyj dzienniki zdarzeń (Event Viewer) na DC1 i DC2 pod kątem błędów replikacji (NTDS Replication, DS) czy DNS.
    - Upewnij się, że rola FSMO, DNS, DHCP itp. działają poprawnie, jeśli były skonfigurowane na DC1.

Najważniejsze wnioski:

- Przy istnieniu drugiego kontrolera domeny najbezpieczniej i najszybciej jest **usunąć uszkodzony DC1** z AD i postawić na nowo.
- Jeśli jednak z jakichś powodów kluczowe jest przywrócenie z backupu, należy zadbać o **uniknięcie USN rollback** (czyli wykonanie nieautorytatywnego przywracania bazy AD w trybie DSRM lub użycie technologii VM Generation ID).
- Po przywróceniu konieczna jest **pełna synchronizacja** z działającym DC2 i weryfikacja poprawności replikacji.

Środowiska wirtualne

W środowiskach **Windows Server 2012 i nowszych** działających na **hypervisorach wspierających VM Generation ID** (m.in. nowsze wersje VMware, Hyper-V) można przywrócić całą maszynę wirtualną kontrolera domeny z backupu i – o ile spełnione są określone warunki – uniknąć ręcznego wykonywania przywracania nieautorytatywnego i ryzyka USN rollback.

Jak to działa?

- **VM Generation ID**: To mechanizm wprowadzony w Windows Server 2012, dzięki któremu system operacyjny (kontroler domeny) rozpoznaje, że został odtworzony ze „starego” stanu (snapshot/backup).
- W takiej sytuacji DC automatycznie **resetuje numer USN**, co powoduje, że jest traktowany jakby został przywrócony nieautorytatywnie. Innymi słowy:
    - Odczytuje swój stan AD z momentu backupu.
    - Natychmiast po uruchomieniu wymusza replikację z innymi kontrolerami, aby „dogonić” bieżący stan bazy katalogowej.

Dzięki temu procedura jest znacznie uproszczona i bezpieczniejsza w porównaniu do czasów przed 2012 r., kiedy wymagane było np. **ręczne przywracanie bazy AD w trybie DSRM (non-authoritative)**.

Zalecana procedura przywrócenia całej VM DC:

1. **Upewnij się, że spełnione są warunki**:
    - Kontroler domeny to **Windows Server 2012+** (im nowszy, tym lepiej).
    - Hypervisor (np. Hyper-V, VMware ESXi) **obsługuje VM Generation ID**.
    - Backup jest **nowszy niż tombstone lifetime** (domyślnie 180 dni).
    - W domenie istnieje co najmniej jeszcze jeden sprawny DC (aby było skąd „dograć" aktualne zmiany).
2. **Odtwórz maszynę z backupu** (plików VM).
    - Najlepiej w środowisku testowym/izolowanym w celu weryfikacji (jeśli to możliwe) – przynajmniej na czas pierwszego rozruchu.
    - Jeżeli mamy zaufanie do systemu VM Generation ID i wiemy, że wszystko jest wspierane, w praktyce większość firm przywraca bezpośrednio w produkcji.
3. **Uruchom odzyskaną maszynę**.
    - Przy pierwszym starcie kontroler sprawdzi, czy zmienił się VM Generation ID, co jednoznacznie wskazuje na przywrócenie z wcześniejszego stanu.
    - Jeśli tak – automatycznie rozpoczyna się procedura „bezpiecznego przywrócenia" (safe restore).
4. **Sprawdź replikację**.
    - Upewnij się, że DC replikuje się poprawnie z innymi kontrolerami, np. komendą:

    repadmin /replsummary

    - Przejrzyj logi w **Event Viewer** → **Directory Service** / **NTDS Replication**, czy nie pojawiają się ostrzeżenia/błędy replikacji.
5. **Potwierdź poprawność usług** (DNS, DHCP, rola FSMO itp.).

Kiedy może być problem?

1. **Brak wsparcia VM Generation ID**
    - Jeżeli mamy starszy hypervisor lub Windows Server 2008 R2 i wcześniejsze wersje kontrolerów – automatyczny „safe restore" nie zadziała.
    - Wówczas zalecane jest ręczne przywracanie **nieautorytatywne** (DSRM) albo (najczęściej prościej) **postawienie nowego DC** i wyczyszczenie metadanych starego.
2. **Zbyt stary backup**
    - Jeśli kopia jest starsza niż tombstone lifetime (standardowo 180 dni), to przywracanie DC z takiej kopii jest ryzykowne, bo w międzyczasie obiekty usunięte i zreplikowane na innych DC już nie istnieją w bazie i dojdzie do niespójności.
    - Lepiej wtedy zrobić **metadata cleanup** uszkodzonego DC i dodać nowy.
3. **Brak innego DC** w domenie
    - Jeśli był to jedyny kontroler domeny, wtedy i tak przywracamy z backupu, ale wówczas opłaca się znać procedurę autorytatywnego przywracania (a to osobny, bardziej złożony temat).

Podsumowanie

W środowiskach wirtualnych z obsługą VM Generation ID (Windows Server 2012+ i zgodny hypervisor) **można bezpiecznie odtworzyć całą maszynę wirtualną** kontrolera domeny z backupu. System sam wykryje, że została cofnięta w czasie i automatycznie wymusi replikację nieautorytatywną, zapobiegając problemom typu USN rollback.

Gdy warunki nie są spełnione, nadal trzeba wykonać albo **ręczne nieautorytatywne przywracanie z system state** (DSRM), albo – w praktyce najczęściej – **usunąć stary DC z domeny i zainstalować nowy** (jeśli mamy wciąż działający inny DC).