Migawka – tworzenie, montowanie i usuwanie migawek AD DS

1. Wprowadzenie

Migawka (ang. snapshot) w kontekście Active Directory Domain Services (AD DS) to funkcjonalność pozwalająca na wykonanie punktu w czasie (point-in-time) kopii bazy danych katalogowej Active Directory. Nie jest to pełna kopia zapasowa, lecz mechanizm służący do przeglądania, analizy i przywracania pojedynczych obiektów lub ich atrybutów bez wpływania na działający katalog. Mechanizm migawek pojawił się od systemu Windows Server 2008 i bazuje na technologii Volume Shadow Copy Service (VSS).

2. Lokalizacja bazy AD DS

Domyślna lokalizacja bazy AD DS: C:\Windows\NTDS\ntds.dit

Dodatkowo istotne są pliki dzienników (*.log) oraz plik punktu kontrolnego edb.chk.

3. Cel i zastosowanie migawek

Migawek używa się do analizy stanu katalogu AD w przeszłości, odzyskiwania obiektów przy użyciu dsamain, porównania danych katalogowych w czasie, testowania i audytu zmian.

4. Narzędzia używane do obsługi migawek

1. ntdsutil.exe – zarządzanie bazą AD DS (tworzenie, listowanie, usuwanie migawek).

2. dsamain.exe – uruchamianie instancji AD DS z migawki pod innym portem LDAP.

3. LDP.exe lub ADUC – przeglądanie zawartości migawki.

5. Tworzenie migawki AD DS

1. Uruchom wiersz poleceń jako Administrator: cmd.exe (Run as Administrator).
2. Uruchom narzędzie: ntdsutil.
3. Przejdź do trybu snapshot: snapshot.
4. Utwórz nową migawkę: create.

Po utworzeniu migawki system zwróci identyfikator np. {abc12345-6789-0abc-def0-1234567890ab}.

6. Wyświetlanie dostępnych migawek

Polecenie: list all

7. Montowanie migawki

Polecenie: mount <ID>. Przykład: mount 2 → migawka dostępna np. jako C:\$SNAP_20251106$.

8. Uruchamianie instancji AD DS z migawki

dsamain -dbpath "C:\$SNAP_20251106$\Windows\NTDS\ntds.dit" -ldapport 38999

9. Przeglądanie migawki

W konsoli ADUC wybierz „Change Domain Controller” i podaj: localhost:38999. Pozwala to przeglądać dane z migawki bez wpływu na bieżący katalog.

10. Odmontowanie i usunięcie migawki

Odmontowanie: unmount <ID>. Usunięcie: delete <ID> lub delete all.

11. Dobre praktyki i uwagi

• Migawki nie zastępują pełnej kopii zapasowej AD DS.

• Z migawek można eksportować obiekty przez ldifde.

• Migawki mogą zajmować dużo miejsca – usuwaj niepotrzebne.

• Sprawdzaj poprawność działania ntdsutil po zmianach konfiguracji.

12. Przykładowa sekwencja poleceń

ntdsutil
snapshot
activate instance ntds
create
list all
mount 1
dsamain -dbpath "C:\$SNAP_20251106$\Windows\NTDS\ntds.dit" -ldapport 38999
unmount 1
delete 1
quit
quit

13. Podsumowanie

Etap	Narzędzie	Komenda / czynność	Efekt
1	ntdsutil	create	Tworzy migawkę bazy AD
2	ntdsutil	list all	Wyświetla listę migawek
3	ntdsutil	mount <ID>	Montuje migawkę

			jako dysk
4	dsamain	-dbpath ... -ldapport	Uruchamia instancję AD z migawki
5	ADUC / LDP	localhost:port	Przeglądanie danych z migawki
6	ntdsutil	unmount, delete	Usuwa migawkę

Rysunek poglądowy (opisowy):

AD DS → migawka → dsamain → ADUC (przeglądanie danych historycznych)