

# **Replikacja katalogu Active Directory Usługa DNS**

**Tomasz Onyszko**

*CTO*

*[tonyszko@zero-trust.cloud](mailto:tonyszko@zero-trust.cloud)*

# Zawartość kursu

---

<b>INFRASTRUKTURA FIZYCZNA KATALOGU</b>	<b>8</b>
Partyce katalogu	11
Global Catalog	15
Read Only Domain Controller	22
Typy topologii replikacji	25
 <b>MECHANIKA REPLIKACJI KATALOGU ACTIVE DIRECTORY</b>	 <b>28</b>
Obiekty katalogu związane z replikacją danych	28
Obiekty połączenia (siteLink)	29
Obiekty ustawień lokacji (NTDS Settings)	30
Obiekt serwera (server)	30
Obiekt ustawień replikacji kontrolera domeny – NTDS Settings (nTDSDSA)	31
Obiekty połączenia replikacji (nTDSConnection)	32
Atrybut <i>options</i>	34
Powiązania pomiędzy obiektami i ich rola	36
Knowledge Consistency Checker (KCC)	38
Inter-Site Topology Generator (ISTG)	39
Budowanie topologii replikacji: intra-site	41
Pierścień replikacji	41
Replikacja wielu partycji katalogu	43
Replikacja partycji Global Catalog	44
Budowanie topologii replikacji: inter-site	47
Serwery brzegowe ( <i>bridgehead servers</i> )	47
Preferowane serwery brzegowe ( <i>preferred bridgehead servers</i> )	49
Wykrywanie niedziałających połączeń replikacji	50
Równoważenie obciążenia połączaniami (load balancing)	52
Łączenie połączeń replikacji ( <i>site link bridges</i> )	54
Powiadomienia i opóźnienia w ramach mechanizmu replikacji	57

<b>Urgent replication</b>	<b>59</b>
Replikacja zmiany hasta	59
<b>Partycje i identyfikatory</b>	<b>62</b>
Identyfikatory repliki katalogu	62
repsFrom	64
repsTo	65
<b>Rodzaje aktualnień</b>	<b>66</b>
Originating update	66
Replicating update	67
<b>Mechanika replikacji danych katalogu</b>	<b>67</b>
USN i metadane obiektu	67
Metadane replikacji	68
<b>PROCES REPLIKACJI DANYCH</b>	<b>70</b>
<b>Replikacja danych z użyciem USN</b>	<b>70</b>
<b>High-watermark vector</b>	<b>74</b>
<b>Up-to-dateness vector</b>	<b>76</b>
<b>Atrybuty wielowartościowe</b>	<b>80</b>
Atrybuty niepołączone	80
Linked attributes	80
Replikacja atrybutów wielowartościowych, połączonych i niepołączonych	81
Atrybuty wielowartościowe i limit wielkości transakcji	82
<b>Konflikty danych w ramach replikacji</b>	<b>83</b>
<b>Usuwanie obiektów</b>	<b>84</b>
Obiekty nagrobkowe	84
<b>Funkcjonalność recycle-bin</b>	<b>86</b>
Informacja o usuniętych obiektach połączonych	87
<b>NARZĘDZIA DIAGNOSTYCZNE</b>	<b>91</b>
<b>Repadmin</b>	<b>91</b>
<b>Replmon</b>	<b>92</b>
<b>DCDIAG</b>	<b>93</b>
<b>ADFIN</b>	<b>94</b>
<b>Rozwiązywanie kodu błędów</b>	<b>95</b>

<b>Logowanie diagnostyczne</b>	<b>96</b>
<b>Przegląd metadanych obiektów</b>	<b>96</b>
<b>Propagacja zmian w katalogu, stan replikacji</b>	<b>97</b>
Lista partnerów replikacji wraz ze statusem replikacji	97
Połączenia replikacji	99
Błędy w procesie replikacji	99
<b>Weryfikacja status replikacji</b>	<b>100</b>
Weryfikacja statusu replikacji przy użyciu Repadmin	100
Opóźnienia w replikacji	102
Narzędzia alternatywne – convergeCheck	102
<b>Weryfikacja stanu replikacji pojedynczej zmiany dla kontrolera domeny</b>	<b>104</b>
Kolejka połączenia i oczekujące zmiany	104
<b>TYPOWE PROBLEMY ZWIĄZANE Z REPLIKACJĄ DANYCH KATALOGU</b>	<b>109</b>
<b>Problemy infrastruktury</b>	<b>109</b>
Usługa DNS	109
Konfiguracja połączeń sieciowych	110
<b>Problemy wystepujące w procesie replikacji danych</b>	<b>111</b>
No more endpoints	111
Active Directory replication has been preempted	111
Access denied	111
No inbound neighbors	112
<b>ZAAWANSOWANE PROBLEMY Z PROCESEM REPLIKACJI</b>	<b>114</b>
<b>Lingering objects</b>	<b>114</b>
Mechanika powstawania lingering objects	114
Replikacja z partnerami zawierającymi lingering objects	114
Strict \ loose replication consistency	115
Diagnostyka problemu	115
Rozwiązywanie problemu	116
<b>USN roll-back</b>	<b>117</b>
Schemat powstawania problemu	117
Diagnostyka	117
Rozwiązywanie problemu	117
<b>INTEGRACJA DNS Z USŁUGĄ ACTIVE DIRECTORY</b>	<b>120</b>
<b>Strefy DNS usługi katalogowej Active Directory</b>	<b>120</b>

<b>REKORDY DNS USŁUGI KATALOGOWEJ</b>	<b>121</b>
Rekordy DNS rejestrowane przez kontroler domeny	121
Wpisu <i>domain wide</i> i <i>site specific</i>	123
Konfiguracja rekordów DNS w scenariuszach branch office	124
<b>DOSTĘP DO DANYCH DNS Z POZIOMU LDAP</b>	<b>126</b>
<b>KOPIE ZAPASOWE I ODZYSKWIANIE DANYCH DNS</b>	<b>130</b>

# Replikacja katalogu Active Directory

---

## **Moduł I**

### **Pojęcia, infrastruktura fizyczna katalogu**



## INFRASTRUKTURA FIZYCZNA KATALOGU

Usługa katalogowa Active Directory zapewnia usługi w oparciu o fizyczną infrastrukturę kontrolerów domeny. Infrastruktura ta z założenia może być rozproszona w sieci. Każda z instancji katalogu (kontroler domeny) zawiera informację o utrzymywanej przez ten kontroler części katalogu (domena).

W celu zapewnienia ciągłości dostępu do danych i usług Active Directory wspiera w ramach jednej usługi katalogowej wiele instancji katalogu, czyli kontrolerów domeny. Redundancja w tym zakresie wynika z konieczności zapewnienia:

- **Odporności usługi na awarię (ang. fault tolerance)**

Awaria pojedynczego kontrolera domeny w przypadku konfiguracji z wieloma replikami katalogu nie wpływa na działanie i dostęp do danych ze strony klientów działających w sieci. W przypadku awarii pojedynczej instancji, replika danych oraz usługi katalogu dostępne są na innych kontrolerach domeny.

- **Rozłożenia obciążenia pomiędzy wieloma replikami (ang. load balancing)**

Wiele replik katalogu w ramach pojedynczej lokacji sieciowej może równoważyć obciążenie zarówno ze strony klientów jak i obciążenie związane z obsługą ruchu replikacji w lokalizacjach centralnych.

- **Optymalizacji dostępu do zasobów usługi z punktu widzenia klienta**

Mechanizmy usługi katalogowej i klienta (*DC locator*) zapewniają możliwość lokalizacji przez klienta najbliższej, z punktu widzenia topologii sieci i usługi katalogowej repliki katalogu.

W celu zapewnienia poprawnego działanie poszczególnych replik katalogu w ramach usługi wymagany jest mechanizm replikacji danych pomiędzy poszczególnymi replikami. Replikacja usługi katalogowej Active Directory charakteryzuje się następującymi cechami:

- **Multimaster**

Replikacja usługi katalogowej Active Directory działa w trybie ***multimaster***. Oznacza to, że każdy z kontrolerów domeny (replik) może niezależnie od innych wprowadzać zmiany do zawartości katalogu. Zmiany te podlegają procesowi replikacji do pozostałych kontrolerów domeny a w przypadku konfliktów związanych z modyfikacją danych katalog stosuje odpowiednie mechanizmy związane z rozwiązyaniem konfliktu.

- **Loosely consistent**

Model replikacji usługi katalogowej zakłada, że dane na poszczególnych replikach katalogu mogą się różnić, co do zawartości w danym momencie czasu. Ze względu na to, że każdy z kontrolerów domeny może wprowadzać zmiany do lokalnej repliki katalogu oraz proces replikacji podlega określonym harmonogramowi, w danym momencie w czasie poszczególne repliki mogą zawierać różniące się pomiędzy sobą dane.

Mechanizm replikacji usługi katalogowej zapewnia jednak, że po pewnym czasie dane zostaną propagowane do poszczególnych replik. W wyniku tego procesu, po określonym czasie (***convergence***) osiągnięty zostanie spójny stan danych we wszystkich replikach katalogu.

Replikacja katalogu Active Directory odbywa się w oparciu o porównanie stanu (**state based**) danych katalogu, z uwzględnieniem stanu poszczególnych obiektów i ich atrybutów pomiędzy dwoma replikami katalogu – źródłową i docelową.

W celu określenia zakresu danych podlegających replikacji kontrolery domeny posługują się wymienianą pomiędzy sobą informacją o stanie replikacji. Stan obiektów podlegających replikacji w ramach każdej z replik określany jest na podstawie metadanych (**metadata**) replikacji. Metadane replikacji dostępne są dla każdego obiektu i atrybutu w ramach katalogu.

Mechanizm replikacji usługi katalogowej jest mechanizmem typu ***pull***. Poszczególne repliki katalogu replikują zmiany z **partnerami replikacji**. W przypadku zmian w lokalnej replice katalogu, które nie zostały jeszcze zreplikowane, partner replikacji jest powiadamiany (**change notification**) o istniejących zmianach.

Po powiadomieniu, partner replikacji odpowiada na powiadomienie inicjuje proces replikacji danych poprzez prośbę o przesłanie zmian w katalogu (***pull***).

#### Reciprocal replication

Standardowo, replikacja usługi Active Directory działa w modelu *notify and pull*, w którym w ramach pojedynczego połączenia replikacji jednej z partnerów wysyła powiadomienie, po którym partner replikacji żąda replikacji zmienionych danych.

W przypadku połączeń replikacji, zdefiniowanych, jako połączenia wzajemne (ang. *reciprocal*) w ramach pojedynczego połączenia możliwe jest wykonanie dwustronnej replikacji danych, poprzez pojedynczy obiekt połączenia. W takim przypadku, kontroler, który inicjuje połączenie replikacji, po otrzymaniu zmian i zakończeniu obsługi replikacji danych do partnera, sam wysyła powiadomienie o zmianach do partnera replikacji.

Scenariusz taki, ma za zadanie zaadresowanie sytuacji, w których połączenie replikacji może być nawiązane tylko z jednej strony, na przykład, gdy jeden z kontrolerów domeny pracuje na połączeniu dial-up.

Mechanizm replikacji usługi katalogowej działa w trybie ***store and forward***. Każdy z kontrolerów domeny po otrzymaniu zmiany zapisuje ją w lokalnej bazie danych i replikuje do wszystkich swoich partnerów replikacji. Zmiana otrzymana od jednego z partnerów replikacji, jest następnie replikowana (o ile zachodzi taka potrzeba) do kolejnych partnerów replikacji.

Dzięki takiemu podejściu pojedynczy kontroler domeny, wprowadzający zmianę do danych katalogu nie musi kontaktować się i dokonywać replikacji zmiany z każdym z kontrolerów domeny utrzymującym replikę danej części katalogu. Replikacja danych wykonywana jest tylko z bezpośrednimi partnerami replikacji (***store***), którzy propagują dalej informacje o zmianach (***forward***) do kolejnych partnerów replikacji w ramach katalogu.

Replikacja odbywa się w ramach infrastruktury fizycznej usługi katalogowej. Infrastruktura fizyczna katalogu Active Directory definiowana jest na podstawie następujących elementów:

- **Kontrolery domeny (ang. Domain controller)**

Kontrolery domeny są to serwery utrzymujące replikę danych katalogu. Kontroler domeny udostępnia dane katalogu klientom oraz dokonuje replikacji tych danych z partnerami replikacji.

- **Lokacje (ang. site)**

Lokacje w ramach usługi katalogowej pozwalają definiować administratorowi usługi obiekty odzwierciedlające lokalizacje fizyczne w ramach sieci. Lokacje w ramach usługi katalogowej mają dwa podstawowe zadania:

- Optymalizację procesu logowania użytkownika, poprzez zapewnienie obsługi klienta przez najbliższy (z punktu widzenia usługi katalogowej) kontroler domeny
- Zdefiniowanie topologii replikacji danych katalogu w środowisku sieciowym.

- **Łącza replikacji (ang. site links)**

Łącza odzwierciedlają w ramach konfiguracji usługi katalogowej topologię sieci z punktu widzenia połączeń pomiędzy poszczególnymi lokalizacjami, reprezentowanymi przez obiekty lokacji. Łącza oraz ich parametry (koszt) pozwalają mechanizmom katalogu na zbudowanie optymalnej, z punktu widzenia fizycznej topologii katalogu, ścieżki replikacji danych pomiędzy poszczególnymi lokacjami.

W oparciu o te elementy definiujące strukturę fizyczną katalogu Active Directory mechanizmy katalogu tworzą i utrzymują topologię replikacji danych usługi.

## Partycje katalogu

Proces replikacji danych usługi katalogowej ma za zadanie zapewnienie spójności danych w ramach poszczególnych *replik* katalogu (kontrolerów domeny). Replikacja pomiędzy poszczególnymi replikami katalogu odbywa się w ramach **partyjki katalogu** (ang. *partition*).

Partycja katalogu jest podstawową jednostką replikacji, czyli definiuje zakres obiektów w katalogu, które są replikowane pomiędzy poszczególnymi replikami katalogu. Repliki katalogu jest to kopia danej partycji katalogu, zestawu partycji na poszczególnych kontrolerach domeny.

W ramach katalogu Active Directory wyróżniamy następujące typy partycji:

- **Schemat (ang. schema partition)**
- **Konfiguracji (ang. configuration partition)**
- **Domenowa (ang. domain)**
- **Aplikacyjna (ang. application partition).**

Typ partycji	Ilość partycji w domenie \ lesie	Opis
Schemat	Jedna w ramach lasu, replikowana do wszystkich kontrolerów domeny w ramach lasu	<p>Partycja schematu zawiera definicję wszystkich klas obiektów oraz atrybutów możliwych do utworzenia w ramach danego lasu usługi katalogowej.</p> <p>Pełna replika tej partycji(definicja schematu) utrzymywana jest na wszystkich kontrolerach domeny w ramach lasu. Zmiany do partycji schematu można wprowadzać tylko na kontrolerze domeny pełniącym rolę <i>Schema FSMO</i> w ramach lasu.</p> <p>DN partycji schematu w ramach każdego z kontrolerów domeny: CN=Schema,CN=Configuration,&lt;DN partycji głównej lasu&gt;</p>
Konfiguracja	Jedna w ramach lasu, replikowana do wszystkich kontrolerów domeny w ramach lasu	<p>Partycja zawierająca dane konfiguracji usługi katalogowej, definicję uprawnień rozszerzonych oraz informacje o konfiguracji usług wspólnych dla całego lasu AD (np. Exchange). Partycja ta zawiera między innymi obiekty definiujące topografię fizyczną usługi katalogowej oraz topografię replikacji danych usługi.</p> <p>Każdy z kontrolerów domeny w ramach lasu utrzymuje pełną replikę danych partycji konfiguracji. Zmiany do danych partycji konfiguracji mogą być wprowadzane na każdym z kontrolerów domeny w ramach usługi katalogowej.</p> <p>DN partycji schematu w ramach każdego z kontrolerów domeny: CN=Configuration,&lt;DN partycji głównej lasu&gt;</p>
Domenowa	Jedna dla każdej domeny w ramach lasu. Pełna replika replikowana jest pomiędzy wszystkimi kontrolerami w ramach danej domeny	<p>Każda z partycji domenowych utrzymuje zestaw obiektów specyficzny dla danej domeny usługi katalogowej (np. użytkowników, grupy, kontenery, OU itp.).</p> <p>Każdy kontroler danej domeny utrzymuje pełną replikę danych partycji własnej domeny.</p> <p>Zmiany do partycji domenowej mogą być wprowadzane na dowolnym kontrolerze domeny utrzymującym pełną replikę</p>
Domenowa (częściowa) –	Częściowa replika danych partycji domenowej, utrzymywana na kontrolerach	Partycja domenowa, utrzymywana na kontrolerach innych domen pełniących rolę <i>Global Catalog</i> , zawierająca częściową kopię danych

Global Catalog	domeny innych domen. Partycja tylko do odczytu ( <i>read only</i> ).	oryginalnej partycji domenowej. Partycja Global Catalog zawiera informacje o wszystkich obiektach z oryginalnej partycji, ograniczoną do zestawy atrybutów wchodzących w skład <i>Partial Attribute Set (PAS)</i> . Częściowa replika każdej partycji domenowej z całego lasu utrzymywana jest na każdym z kontrolerów domeny w ramach lasu, pełniącym role Global Catalog.
Aplikacyjna	Dowolna ilość replik w ramach lasu, ograniczona do ilości kontrolerów domeny. Każdy z kontrolerów domeny w ramach lasu może utrzymywać replikę partycji aplikacyjnej.	Partycje aplikacyjne tworzone są w celu utrzymywania w katalogu wydzielonych partycji zawierających dane aplikacji korzystających z usługi katalogowej. Partycje aplikacyjne mogą być replikowane do dowolnych kontrolerów domeny w ramach lasu, dzięki czemu partycja taka może być replikowana do dowolnych lokacji w sieci rozległej, gdzie wymagany jest dostęp do danych aplikacji i znajduje się kontroler domeny. Zaletą jest fakt, że kontrolery utrzymujące partycje aplikacyjne mogą należeć do różnych domen w ramach lasu. W ramach partycji aplikacyjnych mogą być tworzone obiekty zgodne ze zdefiniowanym schematem usługi katalogowej, z wyjątkiem obiektów będących podmiotami zabezpieczeń (ang. <i>security principal</i> ), czyli na przykład użytkowników i grup. Przykładem partycji aplikacyjnych w ramach usługi katalogowej są partycje usługi DNS: Domenowa: <i>DC=DomainDNSZones,&lt;DN partycji głównej lasu&gt;</i> W ramach lasu: <i>DC=ForestDNSZones,&lt;DN partycji głównej lasu&gt;</i> Partycje aplikacyjne dostępne są w ramach usługi katalogowej od wersji Windows Server 2003. Partycje aplikacyjne określane są, jako NDNC (Non-domain naming context).

Partycje katalogu fizycznie reprezentowane są w ramach danych katalogu poprzez obiekty klasy **domainDNS** ([http://msdn.microsoft.com/en-us/library/ms682204\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms682204(VS.85).aspx)).

### Partycja vs kontekst nazewniczy

W ramach terminologii usługi katalogowej Active Directory terminy partycja (ang. *partition*) oraz kontekst nazewniczy (ang. *naming context*) są równoważne i odnoszą się do partycji usługi katalogowej. W związku z tym można ich używać zamiennie i odnoszą się one do tych samych obiektów.

Partycje katalogu reprezentowane są w ramach konfiguracji katalogu poprzez obiekty klasy **crossRef** ([http://msdn.microsoft.com/en-us/library/ms681007\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms681007(v=VS.85).aspx)) jako obiekty potomne obiektu klasy **crossRefContainer** o DN: *CN=Partitions,CN=Configuration,<DN DN partycji głównej lasu>*

Wszystkie partycje utrzymywane w ramach lasu usługi katalogowej można wylistować używając zapytania LDAP z następującym filtrem:

```
(& (objectClass=crossRef) (objectCategory=crossRef))
```

Typ partycji określany jest na podstawie wartości atrybutu **systemFlags** ([http://msdn.microsoft.com/en-us/library/ms680022\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms680022(VS.85).aspx)) obiektu klasy *crossRef*.

Nazwa	Wartość	Opis
FLAG_CR_NTDS_NC	0x00000001	Partycja katalogu
FLAG_CR_NTDS_DOMAIN	0x00000002	Partycja domenowa
FLAG_CR_NTDS_NOT_GC_REPLICATED	0x00000004	Partycja nie jest replikowana w ramach zestawu partycji Global Catalog.

Typ partycji można określić na podstawie zapytania LDAP o atrybut *systemFlags* obiektu *crossRef*:

Typ partycji	Filtr LDAP
Partycja katalogu	(&(objectClass=crossRef)(systemFlags:1.2.840.113556.1.4.803:=1))
Partycja domenowa	(&(objectClass=crossRef)(systemFlags:1.2.840.113556.1.4.803:=3))
Partycja aplikacyjna	(&(objectClass=crossRef)(systemFlags:1.2.840.113556.1.4.803:=5))

Nazwę partycji domenowej oraz partycji schematu i konfiguracji utrzymywanych w ramach danej repliki katalogu można uzyskać na podstawie informacji uzyskanych z obiektu **rootDSE** ([http://msdn.microsoft.com/en-us/library/ms684291\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms684291(VS.85).aspx)) udostępnianego w ramach każdego kontrolera domeny. RootDSE zgodnie z definicją standardu LDAPv3 jest udostępniany przez każdy serwer usługi i reprezentuje podstawę (ang. *root*) danych drzewa katalogu.

W ramach atrybutów obiektu *rootDSE* dostępne są następujące atrybuty określające partycje katalogu:

Nazwa atrybutu	Opis
schemaNamingContext	<i>Distinguished name (DN)</i> partycji schematu
configurationNamingContext	<i>Distinguished name (DN)</i> partycji konfiguracji
rootDomainNamingContext	<i>Distinguished name</i> partycji domenowej głównej domeny lasu. W lesie z jedną domeną tożsamy z kontekstem domenowym
defaultNamingContext	<i>Distinguished name</i> domyślnej partycji domenowej, domeny danego kontrolera
namingContexts	Wielowartościowy atrybut zawierający listę <i>distinguished name</i> wszystkich partycji katalogu utrzymywanych w ramach danej repliki katalogu.

Wszystkie partie katalogu fizycznie przechowywane są w bazie danych usługi Active Directory przechowywana jest na dysku kontrolera domeny w pliku NTDS.DIT. Plik ten zawiera dane bazy danych zarządzanej przez silnik **Extensible Storage Engine** (ESE). ESE jest to transakcyjny silnik bazy danych, który w celu zachowania integralności danych na wypadek awarii dysku posługuje się dziennikami transakcji

W folderze zawierającym bazę danych usługi katalogowej znajdują się następujące pliki:

- **NTDS.DIT** – główny plik bazy danych usługi Active Directory. W pliku tym przechowywane są wszystkie informacje usługi dostępne na danym kontrolerze domeny. Plik ten zawiera również informacje o schemacie i konfiguracji katalogu.
- **EDB.LOG** – plik dziennika transakcji zawierający wszystkie transakcje wykonywane na głównej bazie danych. Transakcje zapisywane są do dziennika transakcji, przed ich próbą zapisy do głównego pliku NTDS.DIT. Pliki dziennika transakcji ESE w przypadku Active Directory mają rozmiar 10 MB.
- **EDBxxxxx.LOG** – dodatkowe pliki dziennika transakcji, tworzone w przypadku, gdy rozmiar transakcji przekracza wielkość pojedynczego logu transakcji. W chwili zapełnienia logu EDB.LOG tworzony jest nowy, tymczasowy plik, który przemianowany jest następnie na EDB.LOG a dotychczasowy plik przemianowywany jest na EDB00001.LOG. Numeracja plików może rosnąć w miarę potrzeby.
- **EDB.CHK** – plik przechowujący informację o znaczniku (*checkpoint*) transakcji bazy danych ESE. Znacznik ten pokazuje, które transakcje z EDB.LOG zostały już przetworzone i zapisane do bazy danych NTDS.DIT. W przypadku awarii plik EBD.CHK zawiera informacje o tym, które z transakcji muszą jeszcze zostać zapisane do bazy danych usługi. Plik znacznika jest na bieżąco uaktualniany w miarę, gdy poszczególne transakcje są potwierdzane, jako zapisane w bazie danych NTDS.DIT.
- **RES1.LOG, RES2.LOG** – pliki te są to rezerwowe pliki mające na celu jedynie zarezerwowanie dodatkowej przestrzeni dyskowej na potrzeby plików dzienników transakcji, w przypadku gdyby dysk ten uległ przepełnieniu. W praktyce zalecane jest niedopuszczanie do takiej sytuacji oraz wprowadzenie dodatkowych środków zabezpieczeń.
- **TEMP.EDB** – jest to tymczasowa przestrzeń bazy danych używana w celu przechowywania danych roboczych silnika, w przypadku, gdy jest przetwarzana jakaś operacja względem NTDS.DIT.

## Global Catalog

**Serwer Global Catalog** to rola pełniona przez kontroler domeny w ramach infrastruktury usługi katalogowej. Celem *Global Catalog* jest zapewnienie możliwości wyszukania informacji o każdym obiekcie istniejącym w ramach lasu usługi katalogowej, niezależnie od kontrolera domeny i domeny, do której on należy w ramach lasu.

W tym celu każdy serwer GC przechowuje oprócz domyślnych partycji katalogu (schemat, konfiguracja, własny kontekst domenowy) również częściowe repliki danych wszystkich innych partycji domenowych istniejących w ramach lasu.

Zawartość GC udostępniana jest klientom na kontrolerze domeny pełniącym rolę GC na porcie TCP/3268, TCP/3269 (SSL). Zapytania LDAP wysyłane na ten port mogą dotyczyć zarówno partycji katalogu dla domeny, do której należy dany kontroler jak i replik częściowych innych domen istniejących w ramach lasu.

Zawartość GC udostępniana jest poprzez następujące protokoły:

Protokół	Opis
LDAP	Dostęp do zawartości Global Catalog poprzez protokół LDAP – jest to podstawowy interfejs dostępu do zawartości GC dla klientów katalogu.
RPC	Protokół RPC jest używany do komunikacji z GC w ramach mechanizmów replikacji oraz interfejsów dostępu dla klientów MAPI\SAM.
SMTP	Protokół SMTP jest używany tylko w ramach replikacji danych katalogu z użyciem protokołu SMTP.

Dostęp klientów do zawartości GC możliwy jest poprzez jeden z następujących interfejsów:

Interfejs	Protokół	Opis
LDAP	LDAP	Podstawowy interfejs LDAP umożliwiający dostęp do danych katalogu z użyciem protokołu LDAP.
REPL	RPC \ SMTP	Interfejs zarządzania związany z mechanizmami replikacji danych katalogu.
NSPI \ MAPI	RPC	Name Service Provider Interface (NSPI) jest to interfejs, przez który dostęp do danych katalogu i GC uzyskują klienci korzystający z protokołu Messaging API (MAPI).
SAM	RPC	Interfejs dostępu do danych Global Catalog dla klientów opartych o starsze wersje systemów operacyjnych (NT / 9x). Starsze wersje systemów operacyjnych uzyskują dostęp do danych katalogu poprzez interfejs SAM, Zachowującą się analogicznie jak w przypadku dostępu do danych domen NT.

Partycje w ramach GC zawierają częściową kopię danych obiektów istniejących w ramach poszczególnych partycji. Lista atrybutów dostępnych w ramach *Global Catalog* definiowana jest poprzez przynależność atrybutu do zestawu **Partial Attribute Set**.

**Partial Attribute Set (PAS)** jest to zestaw atrybutów, które są replikowane w ramach częściowej repliki partycji domenowej utrzymywanej przez serwery pełniące rolę Global Catalog w ramach lasu usługi katalogowej.

Atrybut należy do zestawu atrybutów PAS w przypadku, gdy spełniony jest jeden z warunków:

- Atrybut został oznaczony, jako należący do PAS poprzez ustawienie bitu w ramach wartości atrybutu ***systemFlags*** na obiekcie definicji atrybutu w schemacie.
- Atrybut został oznaczony, jako należący przez do PAS poprzez wartość opcjonalnego atrybutu ***isMemberOfPartialAttributeSet*** na obiekcie definicji atrybutu w schemacie.

#### Wynikowy zestaw atrybutów w PAS

W przypadku, gdy atrybut oznaczony jest, jako przynależący do PAS poprzez wartość atrybutu ***systemFlags*** jest on replikowany w ramach replik Global Catalog niezależnie od wartości atrybutu ***isMemberOfPartialAttributeSet***.

Listę atrybutów zidentyfikowanych w ramach danej repliki katalogu, jako wchodzące w skład PAS można uzyskać poprzez zapytanie o atrybut ***partialAttributeSet*** ([http://msdn.microsoft.com/en-us/library/ms679107\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms679107(VS.85).aspx)) danej repliki partycji domenowej.

W przypadku atrybutu ***systemFlags*** ([http://msdn.microsoft.com/en-us/library/ms680022\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms680022(VS.85).aspx)), drugi bit (od prawej) w ramach wartości atrybutu ***systemFlags*** definiuje przynależność danego atrybutu do zestawu PAS. W oparciu o wartość atrybutu ***systemFlags*** listę atrybutów wchodzących w skład PAS można określić używając następującego zapytania LDAP:

```
(&(objectClass=attributeSchema)(systemFlags:1.2.840.113556.1.4.803:=2))
```

Wartości atrybutu ***systemFlags*** dla klasy **attributeSchema** mające związek z replikacją danych katalogu:

Nazwa	Wartość	Opis
FLAG_ATTR_NOT_REPLICATED	0x00000001	Atrybut nie jest replikowany
FLAG_ATTR_REQ_PARTIAL_SET_MEMBER	0x00000002	Atrybut wchodzi w skład zestawu PAS

W oparciu o wartość atrybutu opcjonalnego atrybutu ***isMemberOfPartialAttributeSet*** ([http://msdn.microsoft.com/en-us/library/ms676807\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms676807(VS.85).aspx)) przynależność atrybutu do zestawy PAS można określić używając następującego filtru LDAP:

```
(&(objectClass=attributeSchema)(isMemberOfPartialAttributeSet=TRUE))
```

#### Przynależność do PAS i replikacja atrybutów

W ramach katalogu możliwe jest zdefiniowanie atrybutu oznaczonego, jako atrybut wchodzący w skład PAS oraz atrybut, który nie jest replikowany do innych replik w ramach katalogu (FLAG\_ATTR\_NOT\_REPLICATED). W przypadku takiego atrybutu, gdy jego wartość zostanie zmodyfikowana w ramach danego kontrolera domeny, jest ona dostępna w ramach GC danego kontrolera domeny, jednak nie zostanie ona zreplikowana do innych replik utrzymujących partycje GC w ramach lasu.

Zmiany w przynależności atrybutów do zestawu PAS mogą wymagać przeprowadzenia dodatkowej replikacji danych w celu odbudowania zawartości GC. Po zmianie związanej z dodaniem nowego atrybutu

do zestawu PAS, kontroler domeny, który otrzymał już informację o zmianie w schemacie powiadamia swojego partnera replikacji o zmianie definicji PAS. W odpowiedzi na to powiadomienie, partner replikacji inicjuje replikację mającą na celu dobudowanie zawartości PAS.

W przypadku kontrolerów domeny działających w oparciu o system operacyjny Windows 2003 lub późniejszy, zmiana w definicji PAS powoduje replikację w trybie aktualnień – nie jest wymagana pełna przebudowa zawartości GC.

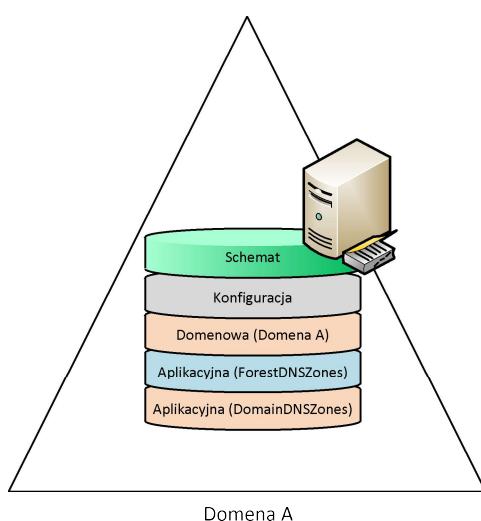
W przypadku replikacji kontrolerów Windows 2000 lub kontrolerów domeny działających w oparciu o Windows 2003 lub późniejszy z partnerami działającymi w oparciu o Windows 2000 zmiana PAS powoduje usunięcie poprzedniej zawartości replik partycji w trybie read-only i pełną odbudowę zawartości GC na kontrolerach domeny.

Usunięcie atrybutu z zestawu PAS wykonywane jest lokalnie na każdym z kontrolerów domeny pełniących rolę kontrolera domeny i nie wymaga dodatkowej replikacji danych. W przypadku, gdy kontroler domeny otrzyma w ramach replikacji informację o tym, że zmieniona została zawartość PAS usunie on odpowiednie atrybuty, których dotyczyła zmiana z lokalnej repliki partycji GC.

W przypadku lasu usługi katalogowej składającej się z jednej domeny w ramach lasu istnieje pięć partycji katalogu:

- Schemat
- Konfiguracja
- Domenowa (Domena A)
- Aplikacyjna: DomainDNSZone (Domena A)
- Aplikacyjna: ForestDNSZone

Standardowo, kontroler domeny w ramach tego lasu, przy założeniu, że jest on również serwerem DNS będzie utrzymywał wszystkie pięć partycji w ramach lasu.



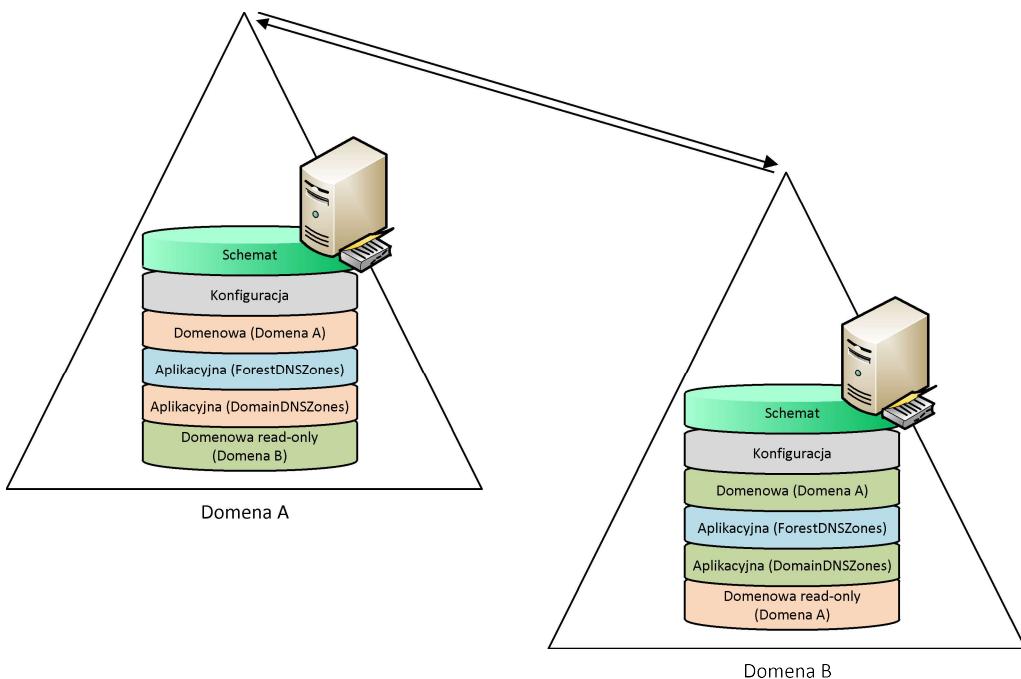
Rysunek 1 Zestaw partycji utrzymywany przez DC w ramach lasu z jedną domeną

Dodanie do lasu dodatkowej domeny (Domena B) powoduje utworzenie dwóch dodatkowych partycji aplikacyjnych:

- Domenowa: (Domena B)
- Aplikacyjna: DomainDNSZone (Domena B).

W przypadku kontrolera domeny pełniącego role Global Catalog w każdej z domen oznacza to, że każdy z nich będzie utrzymywał dodatkową partycję Global Catalog, dla partycji domenowej dodatkowej domeny. W przypadku kontrolera domeny w domenie A, oznacza to, że utrzymywał on będzie następujący zestaw partycji katalogu:

- Schemat
- Konfiguracja
- Domenowa (Domena A)
- Aplikacyjna: DomainDNSZone (Domena A)
- Aplikacyjna: ForestDNSZone
- Domenowa (Domena B) – partycja w trybie tylko do odczytu, GC.



Rysunek 2 Zestaw partycji utrzymywanych przez DC będących GC w ramach lasu z dwoma domenami

Z replikacji w ramach Global Catalog wykluczone są partycje aplikacyjne (NDNC) i partycje te nie są replikowane pomiędzy kontrolerami domeny pełniącymi role Global Catalog.

Domyślnie, Global Catalog udostępnia swoje usługi klientom po zakończeniu replikacji wszystkich partycji, które powinny znaleźć się w zestawie partycji GC w danym środowisku. Warunki związane z ilością zreplikowanych partycji przed udostępnieniem przez Global Catalog usług klientom kontrolowane są przez wpis w rejestrze systemu na każdym z kontrolerów domeny:

Gałiąz rejestru	Klucz	Typ	Wartość
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters	Global Catalog Partition Occupancy	DWORD	0 – brak wymagań, kontroler ogłasza się, jako GC bez ukończonej replikacji danych 1 – wymagana jest dodanie do zestawy replik, co najmniej jednej partycji w trybie read-only w obrębie jednej lokacji (site). 2 – wymagana jest pełna synchronizacja, co najmniej jednej partycji katalogu 3 – wymagane jest, aby wszystkie, wymagane partycje w trybie read-only w ramach danej lokacji zostały dodane do zestawu replik, w tym co najmniej jedna została w pełni zsynchronizowana 4 – wymagane jest, aby wszystkie partycje katalogu w ramach lokacji zostały w pełni zsynchronizowane. 5 – wymagane jest, aby wszystkie, wymagane partycje w trybie read-only w ramach lasu zostały dodane do zestawu replik, w tym co najmniej jedna została w pełni zsynchronizowana 6 – wymagane jest, aby wszystkie partycje w ramach lasu zostały w pełni zsynchronizowane (domyślne)

Brak spełnienia wymaganego poziomu w zakresie stanu replik powoduje, że nowo wypromowany kontroler domeny nie podejmą roli Global Catalog.

Dostępność GC w ramach usług kontrolera domeny można sprawdzić poprzez atrybut obiektu *rootDSE*:

Nazwa atrybutu	Opis
isGlobalCatalogReady	Atrybut typu Boolean. Określa stan usługi <i>Global Catalog</i> w ramach danej repliki katalogu, przyjmuje wartości: <ul style="list-style-type: none"> <li>■ TRUE: GC jest dostępny</li> <li>■ FALSE: GC nie jest dostępny.</li> </ul>

Listę kontrolerów domeny pełniących rolę *Global Catalog* na podstawie danych katalogu można określić używając zapytania LDAP na podstawie wartości atrybutu **options** ([http://msdn.microsoft.com/en-us/library/ms679082\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms679082(VS.85).aspx)) obiektu klasy **nTDSDSA** reprezentującej kontroler domeny w ramach konfiguracji katalogu. Atrybut ten jest maską bitową, w ramach, której pierwszy bit od prawej określa w przypadku kontrolerów domeny, czy dany kontroler pełni rolę GC:

Nazwa	Wartość	Opis
(NTDSDSA_OPT_IS_GC	0x00000001	Kontroler domeny pełni rolę GC

Obiekty *nTDSDSA* reprezentujące kontrolery domeny pełniące role Global Catalog można zidentyfikować używając zapytania LDAP z następującym filtrem:

```
(& (objectClass=nTDSDSA) (options:1.2.840.113556.1.4.803:=1))
```

Od Windows Server 2008 w katalogu dostępny jest konstruowany atrybut ***msDS-isGC*** ([http://msdn.microsoft.com/en-us/library/cc223409\(PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc223409(PROT.10).aspx)), który tworzony jest na podstawie wartości atrybutu *options* dla danego obiektu. Atrybut ten ma wartość TRUE w przypadku, gdy dany kontroler domeny pełni również rolę Global Catalog.

#### **Zapytania z użyciem atrybutów konstruowanych**

Atrybuty konstruowane (and. *constructed attributes*) nie istnieją bezpośrednio w katalogu i są wyliczane przez katalog w chwili zapytania o ich wartość. Z tego powodu nie jest możliwe tworzenie zapytań LDAP w oparciu o tego typu atrybuty.

Możliwość zadania zapytania o kontrolery domeny pełniące rolę kontrolerów domeny posiada również narzędzie DSQUERY:

```
Dsquery server -isgc  
Dsquery server -isgc -domain <FQDN domeny>  
Dsquery server -isgc -site <nazwa lokacji>
```

W środowisku usługi katalogowej Global Catalog używany jest między innymi w następujących scenariuszach:

#### **■ Wyszukiwanie obiektów w ramach całego lasu**

Głównym zadaniem Global Catalog jest umożliwienie zlokalizowanie dowolnego obiektu istniejącego w ramach lasu usługi katalogowej, niezależnie od kontrolera domeny, z którym komunikuje się klient. GC umożliwia wyszukanie informacji o obiekcie a następnie określenie jego docelowej domeny.

Global Catalog wspiera również zapytania, bez określonej podstawy zapytania (ang. *query base*), dzięki czemu możliwe jest jednoczesne przeszukanie informacji we wszystkich partycjach utrzymywanych w ramach danego kontrolera domeny.

W oparciu o tą funkcję GC budowany jest szereg funkcjonalności zarówno w ramach usługi katalogowej, od strony klienta jak i aplikacji zewnętrznych

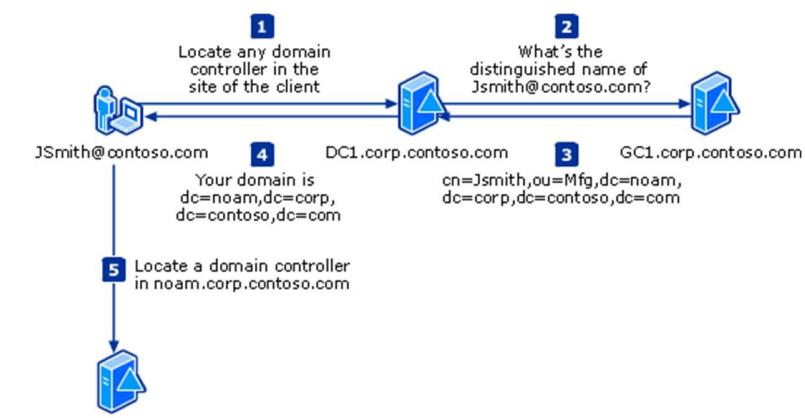
#### **■ Rozwiązywanie członkostwa w grupach uniwersalnych w trakcie logowania**

Grupa uniwersalna może zawierać użytkowników z dowolnej domeny w ramach lasu usługi katalogowej. Ze względu na to, że obiekty będące członkami grup uniwersalnych należą do różnych domen zawartość atrybutu *member* tych grup przechowywana jest w partycji GC. GC zawiera informację o wszystkich obiektach, we wszystkich partycjach, dzięki temu możliwe jest stworzenie referencji pomiędzy obiektami użytkownika i grupy.

Z tego powodu uzyskanie pełnej informacji o członkostwie użytkownika w grupach, ramach lasu Active Directory składającej się z więcej niż jednej domeny wymaga kontaktu z Global Catalog.

## ■ Logowanie z użyciem UPN

W przypadku, gdy użytkownik poda nazwę logowania w formacie UPN Global Catalog jest odpowiedzialny za wyszukanie odpowiedniego obiektu w ramach wszystkich partycji lasu. Wynika to z faktu, że pomimo, iż UPN podawany jest w formacie *użytkownik@suffix*, to suffix atrybutu UPN nie musi odpowiadać nazwie domeny, z której pochodzi użytkownik (chociaż tak jest domyślnie).



Rysunek 3 Schemat rozwiązania nazwy UPN w procesie logowania użytkownika

Zapytanie skierowane do Global Catalog pozwala określić domenę, która jest autorytywna dla podanych poświadczeń użytkownika.

Dodatkowo GC używany jest w ramach mechanizmy Global Group Membership Caching czy rozwiązywanie zapytań dotyczących książek adresowych Exchange.

W ramach pojedynczej domeny, Global Catalog nie udostępnia informacji innych niż informacja o własnej domenie, ponieważ nie ma innych partycji domenowych katalogu, w których mogłyby istnieć obiekty w katalogu. W związku z tym, w ramach lasu składającego się z pojedynczej domeny Global Catalog działa jak każdy inny kontroler domeny, rozwiązuje dodatkowo zapytania kierowane bezpośrednio do usługi GC (zapytania dla całego lasu).

## Read Only Domain Controller

*Read-Only Domain Controller (RODC)* jest to nowa rola wprowadzona w ramach usługi katalogowej w wersji Windows Server 2008 i późniejszych. Z punktu widzenia replikacji danych katalogu RODC charakteryzuje się następującymi cechami:

- Może utrzymywać taki sam zestaw partycji jak każdy inny kontroler domeny w ramach katalogu
- Może pełnić rolę Global Catalog.
- Przechowuje w ramach lokalnej bazy danych katalogu zestaw atrybutów obiektów, nie zawierający danych wchodzących w skład **Filtered Attribute Set (FAS)**.
- Nie pozwala na dokonywanie zmian w danych katalogu (*originating update*) i przekierowuje klientów dokonujących zmiany do kontrolera domeny utrzymującego kopię danej partycji w trybie do zapisu.
- Jednokierunkową replikację zarówno danych katalogu jak i danych SYSVOL.

Kontrolery domeny w trybie tylko do odczytu replikują pełną replikę danych katalogu pozbawioną atrybutów wchodzących w skład *Filtered Attribute Set (FAS)*.

Do zestawu atrybutów zdefiniowanych, jako FAS nie mogą należeć atrybuty spełniające następujące kryteria:

- Atrybut oznaczony jest, jako atrybut niereplikowany poprzez flagę FLAG\_ATTR\_NOT\_REPLICATED w ramach wartości *systemFlags* atrybutu w definicji schematu
- Atrybut oznaczony jest, jako należący do PAS poprzez flagę FLAG\_ATTR\_REQ\_PARTIAL\_SET\_MEMBER w ramach wartości *systemFlags* atrybutu
- Atrybut oznaczony jest, jako atrybut konstruowany, poprzez flagę FLAG\_ATTR\_IS\_CONSTRUCTED (0x00000004) w ramach wartości *systemFlags* atrybutu w definicji schematu
- Atrybut oznaczony jest, jako systemowy poprzez wartość TRUE atrybutu *systemOnly* w definicji schematu
- Atrybut oznaczony jest, jako atrybut konstruowany, poprzez flagę FLAG\_ATTR\_IS\_CRITICAL (0x00000004) w ramach wartości *schemaFlagsEx* atrybutu w definicji schematu.
- Atrybut jest jednym z wymienionych atrybutów: *currentValue*, *dBCSPwd*, *unicodePwd*, *ntPwdHistory*, *priorValue*, *supplementalCredentials*, *trustAuthIncoming*, *trustAuthOutgoing*, *lmPwdHistory*, *initialAuthIncoming*, *initialAuthOutgoing*, *msDS-ExecuteScriptPassword*, *displayName*, *codePage*, *creationTime*, *lockoutDuration*, *lockOutObservationWindow*, *logonHours*, *lockoutThreshold*, *maxPwdAge*, *minPwdAge*, *minPwdLength*, *nETBIOSName*, *pwdProperties*, *pwdHistoryLength*, *pwdLastSet*, *securityIdentifier*, *trustDirection*, *trustPartner*, *trustPosixOffset*, *trustType*, *rid*, *domainReplica*, *accountExpires*, *nTMixedDomain*, *operatingSystem*, *operatingSystemVersion*, *operatingSystemServicePack*, *fSMORoleOwner*, *trustAttributes*, *trustParent*, *flatName*, *sIDHistory*, *dNSHostName*, *lockoutTime*, *servicePrincipalName*, *isCriticalSystemObject*, *msDS-TrustForestTrustInfo*, *msDS-SPNSuffixes*, *msDS-AdditionalDnsHostName*, *msDS-AdditionalSamAccountName*, *msDS-AllowedToDelegateTo*, *msDS-KrbTgtLink*, *msDS-AuthenticatedAtDC*, *msDS-SupportedEncryptionTypes*.

W przypadku pozostałych atrybutów, niespełniających powyższych kryteriów, przynależność do FAS determinowana jest poprzez wartość atrybutu *systemFlags* w definicji atrybutu w schemacie katalogu (9-bit).

Wartości atrybutu *searchFlags* dla klasy *attributeSchema* mające związek z replikacją danych katalogu:

Nazwa	Wartość	Opis
fRODCFilteredAttribute,	0x00000200	Atrybut wchodzi w skład zestawu fas

W oparciu o wartość atrybutu *searchFlags* listę atrybutów wchodzących w skład FAS można określić używając następującego zapytania LDAP:

```
(& (objectClass=attributeSchema) (searchFlags:1.2.840.113556.1.4.803:=512))
```

Atrybuty wchodzące w skład FAS usuwane są również z danych katalogu w przypadku przygotowywania zestawu danych do promocji kontrolera domeny używając opcji *Install From Media*.

W przypadku operacji zapisu danych do katalogu kontroler domeny RODC przekazuje do klienta referencję (ang. *referral*) do kontrolera domeny utrzymującego kopię danej partycji w trybie tylko do zapisu. Aplikacja wykonująca zmianę jest odpowiedzialna za odwołanie do instancji katalogu zwróconej w ramach referencji i wykonanie odpowiednich zmian.

Schemat ten stosowany jest do wszystkich obiektów oraz atrybutów z wyjątkiem wybranych atrybutów mających znaczenie dla działania mechanizmów uwierzytelnienia usługi katalogowej. Zmiany do tych atrybutów przekazywane są przez RODC poprzez bezpośrednie uaktualnienia wysyłane przez RODC do DC posiadającego pełną replikę danej partycji:

- Zmiany hasła użytkownika,
- Uaktualnienia wartości atrybutu *ServicePrincipalname* przez stację roboczą uwierzytelnioną przez RODC (przekazanie zmiany poprzez wywołanie RPC).
- Uaktualnienia atrybutów stacji roboczej, takich jak *DnsHostName*, *OsVersionInfo*, *OsName*, *Supported Encryption Types*,
- Zmiany atrybutu *lastLogonTimestamp* (przekazanie danych przez wywołanie LDAP).

#### Zapis atrybutów w ramach bazy danych RODC

Pomimo, że RODC przechowuje bazę danych katalogu w trybie tylko do odczytu możliwe jest na nim wykonanie zapisu do bazy danych niektórych atrybutów wymaganych do działania usługi katalogowej. Zapis danych do bazy danych katalogu na RODC możliwy jest dla atrybutów, związanych z procesem logowania użytkownika. Zestaw tych atrybutów obejmuje: *LastLogon*, *LogonCount*, *BadPwdCount*, *BadPwdTime*, *BadPwdStamp*, *lockoutTime*, *LastLogonTimeStamp*, *ms-DS-Site-Affinity*.

RODC pozwala również na zapis danych wymaganych dla działania mechanizmów replikacji w ramach własnego obiektu NTDSA.

### **RODC i lastLogonTimeStamp**

Zmiany do atrybutu *lastLogonTimeStamp* na RODC traktowane są odrębnie od zmian w ramach innych atrybutów – atrybut ten należy do zestawu atrybutów replikowanych pomiędzy kontrolerami domeny. W przypadku logowania obsługiwanej przez RODC wartość atrybutu *lastLogonTimestamp* jest aktualniana lokalnie, a następnie RODC podejmuje próbę aktualnienia tej wartości na kontrolerze domeny utrzymującym kopię danej partycji w trybie do zapisu.

Próba aktualnienia wartości atrybutu *lastLogonTimeStamp* jest próbą bez gwarancji powodzenia (ang. *best effort*). W przypadku powodzenia, w następnym cyklu replikacji wartość atrybutu *lastLogonTimeStamp* zostanie nadpisana przez wartość z pełnego kontrolera domeny, na którym wykonany został zapis.

Zmiany w atrybutach przekazane przez RODC lub wykonanie po przekazaniu referencji do innego kontrolera domeny replikowane są do RODC w ramach następnej replikacji danych katalogu. W niektórych przypadkach RODC wykonuje replikację poza zaplanowanym harmonogramem używając mechanizmu *Replicate Single Object*.

Z punktu widzenia topologii replikacji kontroler domeny RODC, nie jest widoczny przez inne kontrolery domeny w ramach usługi katalogowej. Kontrolery RODC tworzone są w oparciu o inną kategorię obiektów w ramach katalogu – NTDA-DSA-RO (pełne DC to obiekty kategorii NTDS-DSA).

Kontroler domeny w trybie RODC tworzy w ramach swojej własnej repliki katalogu połączenia replikacji, pozwalające na przeprowadzenie replikacji danych katalogu z innego kontrolera domeny (*inbound replication*). Kontroler taki tworzy dwa osobne obiekty połączeń, jeden dla replikacji danych katalogu, drugi dla replikacji danych FRS.

Obiekty te nie są nigdy replikowane poza lokalną bazę danych RODC w związku z tym nie istnieją z punktu widzenia pozostałych kontrolerów domeny biorących udział w replikacji.

Z punktu widzenia mechanizmów tworzenia topologii replikacji pozostałych kontrolerów domeny RODC nie jest brany pod uwagę przy wyznaczaniu topologii replikacji (brane są pod uwagę tylko obiekty klasy NTDS-DSA). Z tego powodu, kontrolery domeny utrzymujące pełne kopie danych katalogu nie będą tworzyć przychodzących połączeń replikacji, umożliwiających replikację danych katalogu z kontrolerów w trybie RODC.

Kontrolery domeny w trybie tylko do odczytu tworzą połączenia replikacji tylko do kontrolerów domeny w wersji Windows Server 2008 lub wyższej. Wynika to z faktu, że tylko te kontrolery są w stanie zapewnić replikację danych bez atrybutów wchodzących w skład FAS. Kontrolery spełniające te wymagania mogą być zidentyfikowane przy pomocnym następującego filtra LDAP:

```
(& (objectClass=nTDSDSA) (objectCategory=nTDS-DSA) (ms-DS-behaviorVersion>=3))
```

## Typy topologii replikacji

W ramach mechanizmów replikacji usługi katalogowej wyróżniamy dwa podstawowe typy replikacji:

- **Intrasite**

Replikacja danych pomiędzy partnerami replikacji (kontrolerami domeny) w ramach pojedynczej lokacji usługi katalogowej. Ze względu na definicję lokacji zakłada się, że replikacja ta odbywa się pomiędzy partnerami replikacji połączonymi dobrymi łączami w ramach sieci lokalnej lub szybkiej sieci WAN.

- **Intersite**

Replikacja danych pomiędzy partnerami replikacji (kontrolerami domeny) znajdującymi się, w ramach różnych lokacji zdefiniowanych w ramach usługi katalogowej. Poszczególne lokacje połączone

Replikacja może odbywać się przy pomocy jednej z następujących metod transportu danych:

- RPC
- IP
- SMTP

Nazwa	Protokół	Zastosowanie
RPC	RPC over IP	Replikacja danych wewnętrz lokacji (intrasite). Replikacja dowolnych danych katalogu.
IP	RPC over IP	Replikacja danych pomiędzy lokacjami (intersite). Replikacja dowolnych danych katalogu.
SMTP	Simple Mail Transport Protocol	Replikacja danych pomiędzy lokacjami (intersite). Replikacja danych w zakresie: <ul style="list-style-type: none"><li>■ Partyj schematu</li><li>■ Partyj konfiguracji</li><li>■ Danych Global Catalog</li><li>■ Partyj aplikacyjnych</li></ul> Replikacja SMTP nie może być użyta do replikacji danych partyj domenowych.

Replikacja informacji usługi katalogowej w oparciu o protokół SMTP została przewidziana dla scenariuszy, w których nie ma bezpośredniego połączenia pomiędzy lokacjami zawierającymi kontrolery usługi katalogowej działające w ramach jednego lasu. W takim wypadku, replikacja danych wspólnych dla całego lasu teoretycznie może odbywać się w oparciu o wiadomości przesyłane przez usługę SMTP.

Wdrożenie replikacji opartej o SMTP wymaga wdrożenia usług certyfikatów, w celu zapewnienia certyfikatów wymaganych do szyfrowania komunikacji pomiędzy kontrolerami domeny.

### **Praktyczne zastosowanie replikacji SMTP**

Replikacja danych usługi katalogowej z użyciem protokołu SMTP została zaimplementowana w celu zaadresowania sytuacji, w których replikacja odbywa się bez bezpośredniego połączenia pomiędzy lokacjami usługi katalogowej lub poprzez niestabilne łącza WAN.

W chwili obecnej replikacji z zastosowaniem protokołu SMTP wydaje się nie mieć praktycznego zastosowania, dlatego w ramach zakresu szkolenia temat ten nie jest dalej poruszany.

# Replikacja katalogu Active Directory

---

## **Moduł II**

### Topologia replikacji

## **MECHANIKĄ REPLIKACJI KATALOGU ACTIVE DIRECTORY**

### **Obiekty katalogu związane z replikacją danych**

Topologia replikacji danych usługi katalogowej tworzona jest w sposób automatyczny przez procesy działające w ramach systemu lub definiowana samodzielnie przez administratora usługi. Od strony mechanizmów działania usługi katalogowej, topologia replikacji reprezentowana jest przez zestaw obiektów katalogu istniejących w partycji konfiguracji, które reprezentują topologię sieci, rozmieszczone w niej kontrolery domeny oraz połączenia pomiędzy nimi. Na podstawie tych informacji, wyznaczana jest topologia replikacji danych katalogu, której reprezentacją są obiekty połączenia replikacji.

Klasa obiektu	Opis
Site	Obiekt reprezentujący lokację Active Directory. Lokacje tworzone są samodzielnie przez administratora usługi
siteLink	Obiekt reprezentujący połączenie pomiędzy dwoma lub więcej lokalizacjami. Używany do odzwierciedlenia topologii połączeń w sieci rozległej
nTDSiteSettings	Obiekt reprezentujący ustawienia związane z replikacją katalogu dla pojedynczej lokalizacji.
Server	Obiekt reprezentujący w ramach partycji konfiguracji serwer pełniący role kontrolera domeny
nTDSDSA	Obiekt reprezentujący konfiguracje i ustawienia replikacji dla pojedynczego kontrolera domeny
nTDSDSARO	Obiekt o znaczeniu takim samym jak obiekt klasy nTDSDSA tworzony dla kontrolerów działających w trybie tylko do odczytu (RODC)
nTDSConnection	Obiekt reprezentujący połączenie replikacji danych pomiędzy dwoma partnerami replikacji.

## Obiekty połączenia (siteLink)

Celem tworzenia obiektów połączeń (ang. *site links*) w ramach konfiguracji usługi katalogowej jest odzwierciedlenie w konfiguracji usługi topologii połączeń WAN pomiędzy poszczególnymi lokacjami usługi katalogowej.

Obiekty te tworzone są przez administratora usługi katalogowej, w celu wskazania topologii połączeń pomiędzy poszczególnymi lokacjami utworzonymi w ramach usługi. Obiekt połączenia może łączyć dwie lub więcej lokacje usługi katalogowej.

### Liczba lokacji i obiekty połączeń

Jako dobrą praktykę przy projektowaniu i zarządzaniu usługą katalogową należy przyjąć, że w ramach konfiguracji usługi każdy z obiektów połączeń łączy tylko dwie lokacje usługi katalogowej.

Założenie takie umożliwia procesom odpowiedzialnym za generowanie topologii replikacji poprawne określenie ścieżek replikacji w ramach topologii replikacji.

Każdy z obiektów połączeń definiowany jest w ramach jednej z możliwych metod transportu danych katalogu – IP lub SMTP, odpowiednio w kontenerach:

- **IP:** CN=IP,CN=Inter-Site Transports,CN=Sites,<DN partycji konfiguracji>
- **SMTP:** CN=SMTP,CN=Inter-Site Transports,CN=Sites,<DN partycji konfiguracji>

Dla każdego z obiektów połączenia określone są następujące atrybuty, które mają wpływ na działanie mechanizmów replikacji danych:

Atrybut	Opis
Cost	Określany arbitralnie koszt połączenia. Koszt ten ustalany jest przez administratora. Domyślna wartość to 100.
replInterval	Częstotliwość replikacji danych katalogu poprzez dany obiekt, w ramach ustalonego harmonogramu replikacji. Częstotliwość replikacji określana jest wartością podawaną w minutach. Minimalna wartość to 15 minut.
Schedule	Harmonogram replikacji danych katalogu poprzez dany obiekt połączenia
siteList	Wielowartościowy atrybut, który zawiera linki do obiektów lokacji, które są połączone przez dany obiekt połączenia

### Koszt łączy

Wartość atrybutu *cost* obiektów połączeń w ramach konfiguracji usługi katalogowej określana jest arbitralnie przez administratora usługi. Nie ma jednolitego wzorca pozwalającego na wyliczenie kosztu połączenia, chociaż w dokumentacji usługi można znaleźć różne przykłady wzorów, pozwalających wyliczyć koszt łącza w zależności od jego prędkości.

Koszt łącza może być jednak modyfikowany przez administratora usługi nie tylko ze względu na to, jaka jest przepustowość danego łącza, ale również ze względu na takie czynniki jak utylizacja łącza, opóźnienia na łączu itp.

Ważne jest przyjęcie jednolitej zasady określania kosztu w ramach całej konfiguracji, która pozwoli na odzwierciedlenie poprzez wartość kosztu, jakości i preferencji, co do użycia danego łącza w ramach połączenia pomiędzy lokacjami.

## Obiekty ustawień lokacji (NTDS Settings)

Obiekt nazwany *NTDS Settings* istniejący, jako obiekt potomny dla lokacji jest to obiekt klasy *nTDSSiteSettings* i definiuje on ustawienia związane z replikacją dla danej lokacji.

Obiekt ten zawiera następujące atrybuty istotne z punktu widzenia działania mechanizmów replikacji danych usługi:

Atrybut	Opis
interSiteTopologyGenerator	Informację o aktualnym kontrolerze domeny pełniącym rolę ISTG w ramach lokacji (rola ISTG omówiona zostanie dalej w ramach modułu)
msDS-Preferred-GC-Site	W przypadku użycia mechanizmu buforowania informacji o grupach uniwersalnych, atrybut ten określa lokację, z której informacja taka powinna być odświeżana.
Schedule	Domyślny harmonogram replikacji danych katalogu w ramach danej lokacji

Dla każdej lokacji istnieje jeden tego typu obiekt.

## Obiekt serwera (server)

Obiekty klasy reprezentują w ramach partycji konfiguracji serwery istniejące w ramach katalogu, w tym przypadku kontrolery domeny. Obiekt ten jest tworzony w trakcie promocji kontrolera domeny, w ramach kontenera odpowiadającego lokacji, w której umieszczony został dany kontroler domeny.

Obiekty tego typu są kontenerem, w ramach którego tworzone powiązane z danym kontrolerem domeny kolejne obiekty związane z działaniem mechanizmów replikacji katalogu.

W ramach obiektów klasy serwer, należy zwrócić uwagę na następujące atrybuty związane z działaniem mechanizmów replikacji:

Atrybut	Opis
dnsHostName	Nazwa FQDN kontrolera domeny
serverReference	Link (DN) do obiektu komputera w partycji domenowej reprezentującego dany kontroler domeny
bridgeHeadTransportLists	Atrybut wielowartościowy, zawierający linki (DN) do obiektów odpowiadającym metodom transportu (IP, SMTP), dla których dany kontroler domeny jest preferowanym serwerem brzegowym w ramach danej lokacji.

## Obiekt ustawień replikacji kontrolera domeny – NTDS Settings (nTDSDSA)

Obiekt tej klasy utworzony dla obiektu klasy serwer oznacza, że dany obiekt serwera reprezentuje kontroler domeny. Obiekt ten zawiera ustawienia związane z replikacją dla danego kontrolera domeny oraz jest kontenerem, w ramach którego tworzone są następnie obiekty połączeń związane z poszczególnymi partnerami replikacji.

Obiekt ten tworzony jest w trakcie promocji kontrolera domeny i nie powinien być następnie usuwany ręcznie przez administratora usługi. Obiekt ten usuwany jest w trakcie usuwania roli kontrolera domeny z serwera.

### Obiekt klasy server bez obiektu klasy nTDSDSA

Obiekty klasy *server* istniejące w ramach partycji konfiguracji, umieszczone w kontenerze odpowiadającym lokacji usługi katalogowej, które nie posiadają obiektu *NTDS Settings* są to w normalnym wypadku pozostałości po kontrolerze domeny, który istniał i rola kontrolera domeny została z niego usunięta.

Każdy z kontrolerów domeny posiada w ramach partycji konfiguracji tylko jeden obiekt klasy nTDSDSA.

### Kontrolery RODC

Jak to zostało już wspomniane w ramach poprzedniego modułu, odpowiednikiem obiektu klasy *nTDSDSA* dla kontrolerów domeny, w trybie tylko do odczytu (RODC) są obiekty klasy *nTDSDSARO*.

Istotne atrybuty obiektu nTDSDSA w kontekście działania mechanizmów replikacji danych katalogu:

Atrybut	Opis
invocationID	Identyfikator GUID bazy danych (NTDS.DIT) usługi katalogowej w ramach danej repliki. Rola tego identyfikatora w procesie replikacji przedstawiona jest w module III.
hasMasterNCs	Wielowartościowy atrybut zawierający linki (DN) do partycji schematu, konfiguracji oraz partycji domenowej katalogu, dla których dany kontroler domeny utrzymuje kopię w trybie do zapisu. Atrybut ten nie istnieje na obiekcie odpowiadającym RODC.
hasPartialReplicaNCs	Wielowartościowy atrybut zawierający linki (DN) do wszystkich partycji katalogu, dla których dany kontroler domeny utrzymuje kopię w trybie tylko do odczytu (GC). Atrybut ten będzie posiadał te wartości, tylko w przypadku, gdy dany kontroler domeny pełni rolę Global Catalog.
msDS-Behaviour-Version	Atrybut odpowiadający najwyższemu poziomowi funkcjonalnemu domeny i lasu, jaki dany kontroler domeny jest w stanie obsługi. Atrybut ten uaktualniany jest przez system w trakcie uaktualnień kontrolera domeny. Możliwe wartości to: <ul style="list-style-type: none"><li>■ DS_BEHAVIOR_WIN2000</li><li>■ DS_BEHAVIOR_WIN2003</li><li>■ DS_BEHAVIOR_WIN2008</li><li>■ DS_BEHAVIOR_WIN2008R2</li></ul>
msDS-HasDomainNCs	Link (DN) do partycji domenowej w trybie zapisu utrzymywanej na danym kontrolerze domeny.
msDS-hasInstantiatedNCs	Atrybut przechowujący w postaci binarnej (DN-Binary) informacje o partycjach utrzymywanych w ramach danej repliki katalogu, połączony z informacją o wartości atrybutu <i>instanceType</i> dla danej partycji.
msDS-hasMasterNCs	Wielowartościowy atrybut zawierający linki (DN) do wszystkich partycji katalogu wraz z partycjami aplikacyjnymi,

	dla których dany kontroler domeny utrzymuje kopię w trybie do zapisu.
queryPolicyObject	Link (DN) do obiektu definiującego zasady przetwarzania zapytań (query policy) obowiązujące dla danego serwera. Zasady te określają między innymi takie parametry jak maksymalna liczba połączeń, domyślny rozmiar strony w zapytaniu. Parametry te mogą mieć wpływ na wydajność kontrolera domeny.
msDS-hasFullReplicaNCs	Atrybut występuje tylko w ramach kontrolerów RODC. Zawiera linki (DN) do wszystkich partycji, dla których dany kontroler domeny utrzymuje pełne kopie w trybie tylko do odczytu. Zawiera linki do partycji schematu, konfiguracji, partycji domenowej oraz wszystkich partycji aplikacyjnych utrzymywanych na danym kontrolerze domeny.

## Obiekty połączenia replikacji (*nTDSConnection*)

W oparciu o elementy topologii fizycznej katalogu (lokacje, łącza), procesy odpowiedzialne za tworzenie topologii replikacji danych pomiędzy kontrolerami domeny tworzą połączenia replikacji (ang. *connections*). Połączenia, to obiekty katalogu klasy ***nTDSConnection***, które definiują faktyczne połączenie pomiędzy dwoma partnerami replikacji.

W ramach każdego konfiguracji każdego z kontrolerów domeny obiekt połączenia tworzony jest dla każdego z partnerów replikacji, z którym dany kontroler replikuje dane katalogu. Obiekt ten definiuje parametry połączenia, sposób transportu oraz częstotliwość wykonywania połączenia.

Replikacja katalogu działa w trybie *pull*, w którym kontroler domeny powiadamia swoich partnerów replikacji o zmianach, replikowanych następnie przez odpowiedniego partnera. Obiekt połączenia definiuje w ramach replikacji jednokierunkowe połączenie (ang. *one way*) przychodzące (ang. *inbound*) pozwalające na replikację danych z kontrolera źródłowego (ang. *source*) do kontrolera docelowego (ang. *target*). Kontrolerem docelowym jest kontroler domeny, dla którego utworzony został obiekt połączenia.

Obiekty połączenia tworzone są, jako obiekty potomne dla obiektu klasy *nTDSDSA* reprezentujące w ramach topologii replikacji kontrolery domeny. Każdy z kontrolerów domeny będzie posiadał jeden obiekt połączenia dla każdego z kontrolerów, z którym replikuje dane katalogu.

Ponieważ obiekty połączenia definiowane są, jako obiekty jednokierunkowe, w celu stworzenia pełnej topologii replikacji, zapewniającej dwustronną wymianę danych pomiędzy dwoma kontrolerami domeny wymagane jest stworzenie dwóch obiektów połączeń, po jednym dla każdego z kontrolerów domeny biorących udział w ramach replikacji.

Istotne atrybuty obiektu *nTDSConnection* w kontekście działania mechanizmów replikacji danych katalogu:

Atrybut	Opis
parent	Link (DN) do nadziednego obiektu nTDSADSA reprezentującego kontroler domeny
fromServer	Link (DN) do źródłowego obiektu nTDSDSA, który jest źródłem danych w ramach tego połączenia
Schedule	Harmonogram replikacji. W ramach połączenia w jednej lokacji, harmonogram ustalany jest na podstawie harmonogramu lokacji. W połączeniach pomiędzy lokacjami, harmonogram ustalany jest na podstawie harmonogramu łącza pomiędzy lokacjami.
transportType	Link (DN) do obiektu odpowiadającego metodzie transportu (IP, SMTP) używanej w ramach połączenia.
mS-DS-	Dodatkowe informacje o stanie połączenia. Wartość tego atrybutu zostanie omówiona w części szkolenia

---

ReplicatesNCReason dotyczącej budowania topologii replikacji.

---

W przypadku kontrolerów domeny RODC, dostępnych od Windows 2008 tworzony jest tylko pojedynczy zestaw połączeń dla kontrolera RODC pozwalający na replikację danych z pełnego kontrolera domeny, do kontrolera RODC. Definiuje to jednostronne połączenie przychodzące, pozwalające kontrolerowi RODC na replikację danych z pełnego kontrolera domeny (RWDC).

W przypadku kontrolerów domeny w trybie tylko do odczytu, po stronie kontrolera domeny RODC tworzone są dwa połączenia replikacji dla pojedynczego kontrolera będącego partnerem replikacji. W przypadku replikacji SYSVOL z użyciem FRS do kontrolera RODC mechanizmy FRS wymagają osobnego obiektu połączenia na potrzeby działania FRS. Standardowe kontrolery domeny w celu zapewnienia działania mechanizmów replikacji FRS używają standardowych połączeń replikacji katalogu istniejących po obu stronach. W przypadku kontrolerów domeny RODC w celu zapewnienia działania mechanizmów FRS tworzony jest dodatkowy obiekt połączenia po stronie RODC.

Replikacja danych katalogu oraz replikacja danych SYSVOL w ramach danego obiektu RODC musi być wykonywana z tym samym partnerem replikacji. W przypadku zmiany partnera replikacji danych katalogu, atrybut *fromServer* na odpowiednim połączeniu przeznaczonym dla replikacji FRS zostanie synchronizowana tak, aby oba połączenia wykonywane były z konkretnym kontrolerem domeny.

#### **Replikacja SYSVOL z użyciem DFSR**

Jeżeli replikacja SYSVOL w środowisku odbywa się z użyciem DFSR dodatkowy obiekt połączenia nie jest wymagany.

Obiekt połączenia przeznaczony dla replikacji FRS dla kontrolera domeny RODC wyróżniony jest poprzez ustawioną wartość bitową w ramach atrybutu *options* połączenia:

Nazwa	Wartość	Opis
NTDSCONN_OPT_RODC_TOPOLOGY	0x00000040	Ustawienie tej flagi wskazuje na to, że obiekt połączenia powinien być używany tylko do replikacji FRS

## Atrybut *options*

W ramach atrybutów obiektów należących do jednej z klas:

- **nTDSSiteSettings**
- **nTDSDSA**
- **nTDSCConnection**
- **siteLink**

występuje atrybut *options*, który przechowuje wartość odpowiadającą 32-bitom. Poszczególne bity w ramach tej wartości, dla których w ramach danej klasy obiektów zdefiniowane zostało znaczenie, dostarczają informacji znaczących z punktu widzenia działania mechanizmów replikacji usługi katalogowej lub pozwalają na modyfikowanie działania tych mechanizmów.

Bitы w ramach flagi *options* ustawiane są począwszy od najmniej znaczącego bitu, od lewej strony.

W zależności od klasy obiektu, dla którego flaga ta jest modyfikowana, poszczególne bity mają inne znaczenie.

Atrybut *options* dla obiektów klasy *nTDSSiteSettings*:

Nazwa*	Wartość	Opis
NTDSSETTINGS_OPT_IS_AUTO_TOPOLOGY_DISABLED	0x00000001	Ustawienie tej flagi powoduje wyłączenie mechanizmów automatycznego generowania topologii replikacji (KCC) wewnątrz lokacji
NTDSSETTINGS_OPT_IS_TOPL_CLEANUP_DISABLED	0x00000002	Ustawienie tej flagi powoduje wyłączenie mechanizmów automatycznego czyszczenia topologii replikacji
NTDSSETTINGS_OPT_IS_TOPL_MIN_HOPS_DISABLED	0x00000004	Ustawienie tej flagi powoduje, że wyłączone zostaje generowanie topologii replikacji z zachowaniem minimalnej liczby przejść pomiędzy poszczególnymi kontrolerami domeny.
NTDSSETTINGS_OPT_IS_TOPL_DETECT_STALE_DISABLED	0x00000008	Ustawienie tej flagi powoduje wyłączenie mechanizmu wykrywania nieaktywnych kontrolerów domeny
NTDSSETTINGS_OPT_IS_INTER_SITE_AUTO_TOPOLOGY_DISABLED	0x00000010	Ustawienie tej flagi powoduje wyłączenie mechanizmów automatycznego generowania topologii replikacji (ISTG) pomiędzy lokacjami.
NTDSSETTINGS_OPT_IS_GROUP_CACHING_ENABLED	0x00000020	Ustawienie tej flagi włącza mechanizm buforowania informacji o grupach uniwersalnych w ramach lokacji
NTDSSETTINGS_OPT_FORCE_KCC_WHISTLER_BEHAVIOR	0x00000040	Flaga ta włącza działanie mechanizmów KCC w oparciu o algorytm dostępny w Windows 2003 i późniejszych
NTDSSETTINGS_OPT_IS_RAND_BH_SELECTION_DISABLED	0x00000100	Ustawienie tej flagi wyłącza mechanizm losowego wyboru serwera przyzółkowego w ramach lokacji
NTDSSETTINGS_OPT_IS_REDUNDANT_SERVER_TOPOLOGY_ENABLED	0x00000400	Ustawienie tej flagi powoduje włączenie trybu generowania redundantnej topologii połączeń replikacji dla lokacji. Generowane połączenia są statyczne, flaga ta wymaga równoczesnego wyłączenia mechanizmów KCC (NTDSSETTINGS_OPT_IS_INTER_SITE_AUTO_TOPOLOGY_DISABLED)

\* – Wybrane flagi, pełny opis w dokumentacji protokołu MS-ADTS

Flagi w ramach wartości atrybutu *options* mogą być ustawiane równocześnie i tak w celu wyłączenia mechanizmów automatycznego generowania połączeń replikacji wewnętrz i pomiędzy lokacjami należy ustawić wartości 1 (0x00000001) oraz 16 (0x00000010) co daje razem 17 (0x00000011).

Atrybut *options* dla obiektów klasy *nTDSDSA*:

Nazwa*	Wartość	Opis
NTDSDSA_OPT_IS_GC	0x00000001	Kontroler domeny pełni rolę Global Catalog

\*) – Wybrane flagi, pełny opis w dokumentacji protokołu MS-ADTS

Atrybut *options* dla obiektów klasy *nTDSCollection*:

Nazwa*	Wartość	Opis
NTDSCONN_OPT_IS_GENERATED	0x00000001	Ustawiona flaga oznacza obiekt połączenia wygenerowany automatycznie
NTDSCONN_OPT_TWOWAY_SYNC	0x00000002	Ustawiona flaga wskazuje na połączenie wzajemne pomiędzy partnerami replikacji (reciprocal replication)
NTDSCONN_OPT_USE_NOTIFY	0x00000008	Ustawiona flaga włącza mechanizm powiadomień o zmianach pomiędzy partnerami replikacji
NTDSCONN_OPT_USER OWNED_SCHEDULE	0x00000020	Ustawiona flaga oznacza, że harmonogram replikacji dla danego połączenia zarządzany jest ręcznie przez administratora i nie powinien być modyfikowany przez mechanizmy KCC.

\*) – Wybrane flagi, pełny opis w dokumentacji protokołu MS-ADTS

Atrybut *options* dla obiektów klasy *siteLink*:

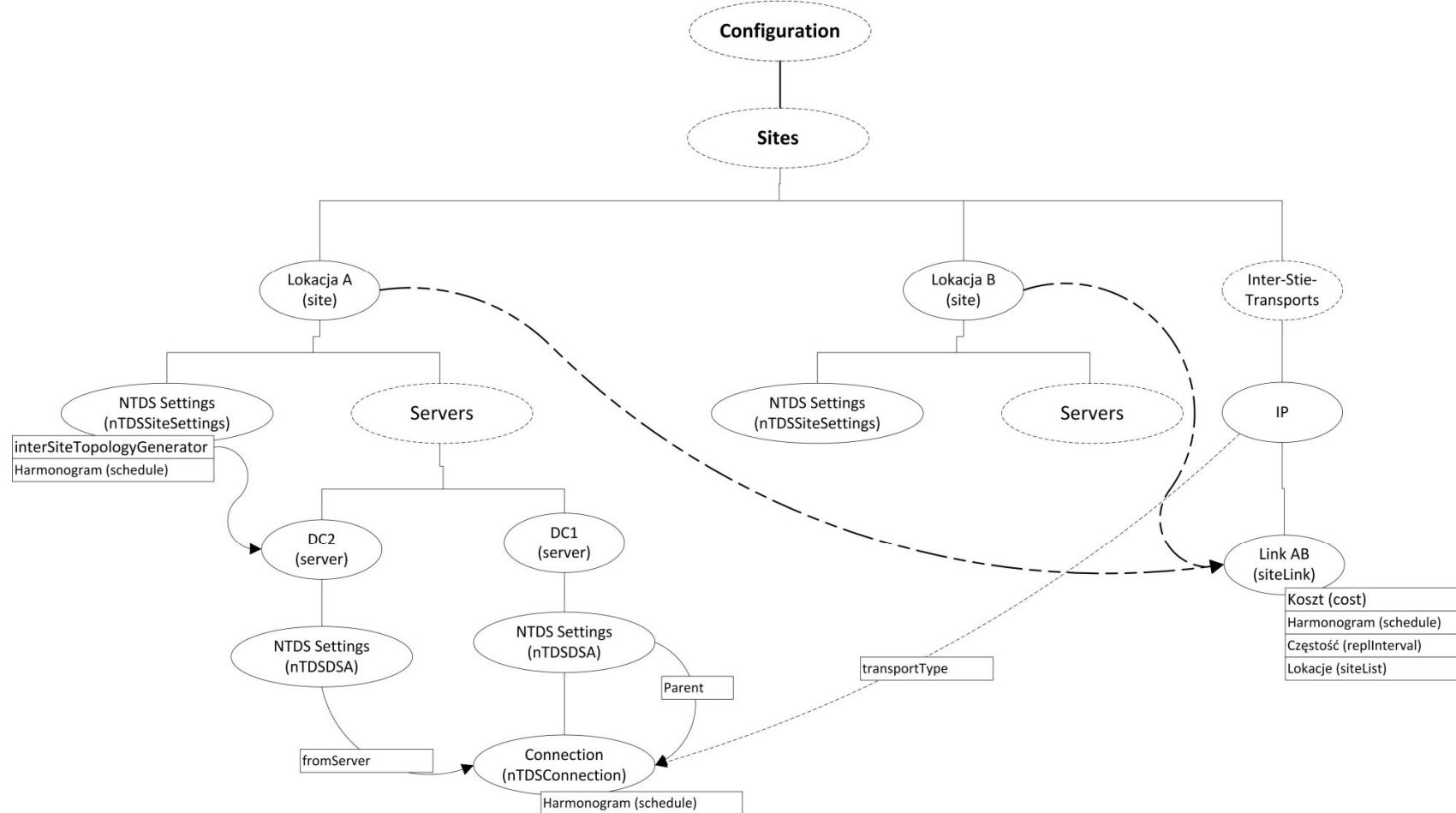
Nazwa*	Wartość	Opis
NTDSSITELINK_OPT_USE_NOTIFY	0x00000001	Ustawiona flaga włącza w ramach danego połączenia mechanizm powiadomień o zmianach pomiędzy partnerami replikacji
NTDSSITELINK_OPT_TWOWAY_SYNC	0x00000002	Ustawiona flaga powoduje, że w ramach danego połączenia używany jest mechanizm wzajemnej replikacji (reciprocal replication)

\*) – Wybrane flagi, pełny opis w dokumentacji protokołu MS-ADTS

## **Powiązania pomiędzy obiektami i ich rola**

Na następnej stronie przedstawiony został uproszczony schemat zależności pomiędzy obiektami definiującymi topologię replikacji danych usługi katalogowej. Schemat ten obrazuje powiązanie pomiędzy obiektami poszczególnych klas wraz z powiązaniami pomiędzy nimi w ramach konfiguracji mechanizmów replikacji.

Schemat nie obejmuje odniesień do obiektów istniejących poza partycją konfiguracji, takich jak np. przykład obiektu komputera reprezentujący kontroler domeny w ramach partycji domenowej czy obiekty powiązane z replikacją wolumenu SYSVOL, również umieszczone w ramach partycji domenowej.



## Knowledge Consistency Checker (KCC)

Topologia replikacji budowana jest poprzez proces *Knowledge Consistency Checker (KCC)*. KCC działa na każdym kontrolerze domeny w celu zweryfikowania informacji o topologii katalogu, obiektach wpływających na działanie replikacji katalogi i dostępnych kontrolerach domeny. Gdy KCC wykryje zmiany w konfiguracji katalogu, obejmujące elementy związane z topologią katalogu zadaniem tego procesu jest obliczenie optymalnej ścieżki replikacji danych i dostosowanie topologii połączeń tak, aby proces replikacji danych zachodził w sposób optymalny.

KCC odpowiedzialne jest za generowanie ścieżek replikacji wewnętrz lokacji (*intra-site*) jak i pomiędzy lokacjami (*inter-site*). Metoda wyznaczania ścieżek replikacji w poszczególnych scenariuszach omówiona dalej w ramach materiałów szkoleniowych.

Rezultatem działania KCC w ramach lokacji (*intra-site*) jest topologia replikacji w postaci *ringu*, w przypadku replikacji jest drzewo (*spanning tree*).

Działanie algorytmu KCC ma za zadanie spełnienie następującego zestawy wymagań:

- W topologii replikacji istnieje ścieżka połączenia pomiędzy każdą z pełnych replik partycji a dowolną inną repliką tej partycji (*read-only*, częściowa, pełna)
- Połączenie pomiędzy dwiema pełnymi (*writable*) replikami danej partycji nie prowadzi przez replikę w trybie *read-only*.
- Wszystkie, pełne (*writable*) repliki danej partycji domenowej połączone są z pozostałymi replikami tej partycji (dowolnego typu) z użyciem protokołu RPC.
- W ramach jednej lokacji replikacja powinna zapewniać szybką propagację danych (nawet kosztem zwiększenia ruchu związanego z replikacją). Pomiędzy lokacjami replikacja powinna zapewniać jak najmniejszy ruch związany z replikacją danych (nawet kosztem zwiększeniu opóźnienia w replikacji danych).

W wyniku działania procesu KCC w ramach konfiguracji katalogu tworzone są lub uaktualniane obiekty połączeń (*nTDSCollection*) oraz atrybuty *repsFrom* i *repsTo* dla poszczególnych replik partycji katalogu.

### **repsFrom, repsTo**

Atrybuty te, przechowują dla każdej z replik partycji katalogu lokalną strukturę danych, w ramach której dostępne są informacje o stanie replikacji dla danej repliki i poszczególnych partnerów replikacji. Informacje te obejmują takie dane jak czas ostatniej próby replikacji, czas ostatniej udanej replikacji, czas ostatniej replikacji GUID repliki itp.

KCC utrzymuje też i uaktualnia w ramach każdego z kontrolerów domeny informację o próbach replikacji danych z poszczególnymi partnerami replikacji, które zakończyły się błędem i nie powiodły się.

Dzięki działaniu KCC, przy prawidłowym zdefiniowaniu topologii fizycznej katalogu, w postaci definicji lokacji, połączeń pomiędzy lokacjami i rozmieszczeniu kontrolerów domeny, utrzymanie topologii replikacji katalogu jest zadaniem automatycznym. W większości przypadków, zadanie to nie wymaga interwencji administratora w postaci tworzenia ręcznych połączeń replikacji pomiędzy poszczególnymi replikami katalogu.

Proces KCC uruchamiany jest po raz pierwszy 5 minut po starcie kontrolera domeny. Następnie KCC uruchamiane jest konsekwentnie zweryfikowania topologii replikacji co 15 minut. Czas pomiędzy uruchomieniami KCC można zmienić modyfikując rejestr kontrolera domeny.

#### Czas uruchamiania procesu KCC

Czas pierwszego uruchomienia procesu KCC po starcie systemu kontrolowanego jest przez wartość wpisu ***Repl topology update delay (secs)*** w ramach klucza HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters. Wartość ta określa okres podany w sekundach, po którym po starcie systemu nastąpi uruchomienie KCC w celu weryfikacji topologii replikacji.

Okres kolejnych uruchomień KCC w celu weryfikacji topologii replikacji kontrolowanego jest przez wartość rejestru ***Repl topology update period (secs)*** w kluczu HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters. Wartość ta określana jest w sekundach.

## Inter-Site Topology Generator (ISTG)

Generowanie topologii replikacji w relacjach pomiędzy lokacjami wykonywane jest również przez proces KCC jednak działający na konkretnym serwerze w ramach lokacji. Kontroler domeny, który w ramach danej lokacji jest odpowiedzialny za generowanie połączeń definiujących topologie replikacji pomiędzy poszczególnymi lokacjami pełni rolę ***inter-site topology generator (ISTG)***.

W ramach każdej lokacji działa jeden kontroler domeny pełniący rolę ISTG. Domyslnie, rolę tę pełni pierwszy kontroler domeny wypromowany w ramach danej lokacji. Aktualny kontroler domeny pełniący rolę ISTG w ramach danej lokacji wskazywany jest przez link do obiektu klasy *nTDSDSA* tego kontrolera w ramach atrybutu *interSiteTopologyGenerator* obiektu *NTDS Settings* (*nTDSSiteSettings*) dla danej lokacji. W razie potrzeby administrator usługi może przypisać rolę ISTG innemu kontrolerowi domeny poprzez modyfikację tego atrybutu.

W przypadku awarii kontrolera domeny pełniącego rolę ISTG w ramach lokacji, w przypadku gdy w danej lokacji istnieje więcej niż jeden kontroler domeny, rolę ISTG może przejąć jeden z pozostałych kontrolerów. Fakt działania ISTG określany jest poprzez uaktualnienie przez kontroler domeny pełniący tę rolę informacji skierowanej do pozostałych kontrolerów w ramach lokacji. Częstotliwość uaktualniania informacji określana jest przez atrybut *interSiteTopologyRenew* obiektu *NTDS Settings* (*nTDSSiteSettings*) dla danej lokacji.

#### Informacja o dostępności ISTG

W Windows 2000, serwer pełniący rolę ISTG w ramach lokacji co 30 minut uaktualnia wartość atrybutu *InterSiteTopologyGenerator*. Zmiana ta jest replikowana w ramach lokacji i pełni rolę informacji o dostępności ISTG.

W Windows 2003 i późniejszych konieczność wykonywania tych uaktualnień została wyeliminowana. Dostępność serwera pełniącego rolę ISTG w ramach lokacji określana jest na podstawie informacji o ostatnim połączeniu kontrolera domeny z partnerami replikacji. Informacja ta przechowywana jest w ramach *up-to-dateness-vector*. Pozwala to na wyeliminowanie uaktualnienia atrybutu w ramach obiektu lokacji, jako sposobu potwierdzenia dostępności ISTG.

Czas bez uaktualnień, po którym wybierany jest nowy ISTG w ramach lokacji, określany jest poprzez wartość atrybutu *interSiteTopologyFailover* obiektu *NTDS Settings* (*nTDSSiteSettings*) dla danej lokacji. Domyślny czas, po którym nastąpi wybór nowego kontrolera pełniącego rolę ISTG to 2 godziny.

#### Lokacje z RODC i ISTG

Lokacje, w których zainstalowany będzie tylko kontroler RODC nie będą miały zarejestrowanego ISTG. Związane jest to z tym, że serwer pełniący rolę RODC pełni tą rolę tylko dla siebie samego i nie rejestruje tej informacji dla lokacji (atrribut *interSiteTopologyGenerator*).

#### Uaktualnienia wartości ISTG dla lokacji

Wartość atrybutu *interSiteTopologyGenerator* dla obiektu lokacji generowana jest przez kontroler domeny, który wybrany został jako pełniący rolę ISTG dla lokacji. Uaktualnienia te jednak nie następują gdy:

- ostatni kontroler domeny został przeniesiony z lokacji do innej lokacji. W takim wypadku ISTG dla danej lokacji nadal będzie wskazywał na ostatni, wybrany jako ISTG dla danej lokacji kontroler domeny.
- Ostatni kontroler domeny dla danej lokacji został skasowany. W takim wypadku wartość ISTG będzie wskazywała na skasowany obiekt kontrolera domeny

Kontroler domeny pełniący rolę ISTG zawsze tworzy obiekty połączeń w ramach danej lokacji, dla których kontroler domeny w danej lokacji jest serwerem docelowym (*destination*) w ramach połączenia, a kontrolery domeny w innych lokacjach stanowią źródło danych. Pomimo, że ISTG w ramach danej lokacji tworzy jedynie część połączeń wymaganych do stworzenia pełnej topologii replikacji (połączenia po jednej ze stron) to decyzje te oparte są na topologii katalogu i konfiguracji dla całego lasu.

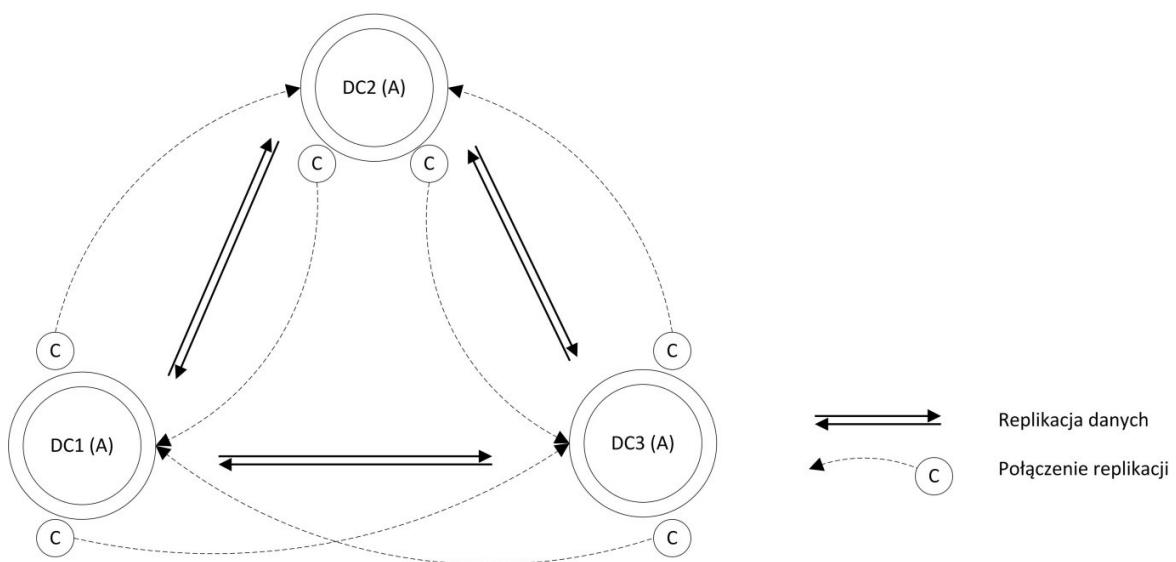
## Budowanie topologii replikacji: intra-site

### Pierścień replikacji

Topologia replikacji wewnętrz lokacji wyznaczana jest przez proces KCC w postaci pierścienia (*ring*) łączącego wszystkie kontrolery domeny w ramach lokacji. W ramach tego okręgu, każdy kontroler domeny w ramach lokacji tworzy obiekty połączeń (przychodzące) z dwoma innymi kontrolerami domeny (o ile istnieje ich wystarczająca liczba by spełnić to wymaganie).

Kolejność kontrolerów domeny w ramach okręgu wyznaczana jest na podstawie wartości atrybutów *objectGUID* kontrolerów domeny biorących udział w replikacji. Wartości *objectGUID* kontrolerów domeny sortowane są w porządku rosnących wartości i dwa skrajne kontrolery domeny na liście (pierwszy i ostatni) tworzą początek i koniec pierścienia replikacji

Założeniem procesu KCC w przypadku tworzenia połączeń pomiędzy DC w ramach jednej lokacji jest to, aby pomiędzy dowolnymi dwoma kontrolerami domeny w ramach lokacji, nie było więcej niż 3 przejścia w ramach pierścienia replikacji.



W przypadku, gdy liczba kontrolerów domeny w ramach lokacji przekracza liczbę (7), umożliwiającą stworzenie topologii pomiędzy wszystkimi DC spełniającymi to założenie w oparciu o tylko dwa połączenia dla każdego DC, tworzone są dodatkowe połączenia zapewniające spełnienie wymagania maksymalnej liczby przejść pomiędzy DC.

### **ms-DS-ReplicatesNCReason**

Obiekt połączenia (*nTDSCollection*) posiada atrybut ms-DS-ReplicatesReason, który przechowuje informacje związane z topologią replikacji generowaną przez KCC. W ramach wartości tego atrybutu, dla każdej z partycji katalogu replikowanej poprzez dane połączenie istnieje wpis, zawierający DN danej partycji oraz wartość binarną opisującą stan danego połączenia dla tej partycji. W ramach tej wartości binarnej, następujące wartości mają powiązanie z tworzeniem topologii replikacji wewnątrz lokacji:

- NTDSCONN\_KCC\_RING\_TOPOLOGY, 0x00000002: obiekt połączenia stworzony w celu zamknięcia pierścienia replikacji
- NTDSCONN\_KCC\_MINIMIZE\_HOPS\_TOPOLOGY, 0x00000004: obiekt połączenia stworzony, w celu zminimalizowania liczby przejść pomiędzy partnerami replikacji.

### **Atrybuty opisujące listę partnerów replikacji**

Od systemu Windows Server 2003 dostępne są dwa atrybuty konstruowane *msDS-NCRepInboundNeighbors* oraz *msDS-NCRepOutboundNeighbors* dla obiektu partycji katalogu, prezentujące informacje o partnerach replikacji dla danej repliki katalogu w ramach tej partycji katalogu.

Dodatkowo dostępne są również atrybuty konstruowane *msDS-RepAllInboundNeighbors* oraz *msDS-RepAllOutboundNeighbors* obiektu rootDSE prezentujące listę wszystkich partnerów replikacji dla danej repliki katalogu.

Proces KCC znając liczbę kontrolerów domeny w ramach lokacji oblicza minimalną, wymaganą liczbę połączeń dla każdego DC zapewniającą stworzenie pierścienia replikacji z zachowaniem maksymalnej liczby przejść pomiędzy partnerami replikacji. Następnie porównuje liczbę obiektów połączeń (*nTDSCollection*) posiadanych przez każdy z kontrolerów, i jeżeli posiada on mniej połączeń niż zakładane minimum tworzy dodatkowe połączenia przychodzące z losowo wybranymi kontrolerami w ramach lokacji.

### **Czas generowania topologii replikacji**

W przypadku konieczności utworzenia dodatkowych połączeń pomiędzy kontrolerami domeny w ramach jednej lokacji wystąpić może opóźnienie w czasie, w którym topologia zostanie ustalona w ramach lokacji. Opóźnienie to wynika z rozproszonej struktury katalogu oraz opóźnień w powiadomianiu partnerów replikacji o zmianach.

Proces KCC w ramach każdego z kontrolerów domeny uruchamiany jest asynchronicznie w cyklach 15 minutowych. Czas ten nie jest jednak synchronizowany pomiędzy poszczególnymi kontrolerami domeny, w związku z czym, w skrajnym wypadku różnica w czasie uruchomienia procesu KCC na poszczególnych kontrolerach domeny może wynieść 15 minut.

Dodatkowo, kontroler domeny musi uzyskać informacje niezbędne do wygenerowania nowej topologii replikacji (nowy kontroler domeny, usunięty link itp.) w ramach procesu replikacji danych. Powiadomienie o zmianach pomiędzy poszczególnymi kontrolerami domeny może wynosić w zależności od wersji systemu operacyjnego o 15 sekund do 5 minut pomiędzy dwoma partnerami. W związku z tym maksymalne opóźnienie w ramach pierścienia replikacji wynosi of 45 sekund do 15 minut.

Ponieważ do ustalenia topologii replikacji wymagane jest zajście cyklu, na który składa się:

- Replikacja o zmianie
- Uruchomienie KCC w celu wygenerowania nowych połączeń
- Replikacja informacji o nowych połączeniach do partnerów replikacji

Pełne ustalenie się topologii replikacji w ramach lokacji może wymagać zależnego od ilości kontrolerów domeny okresu czasu.

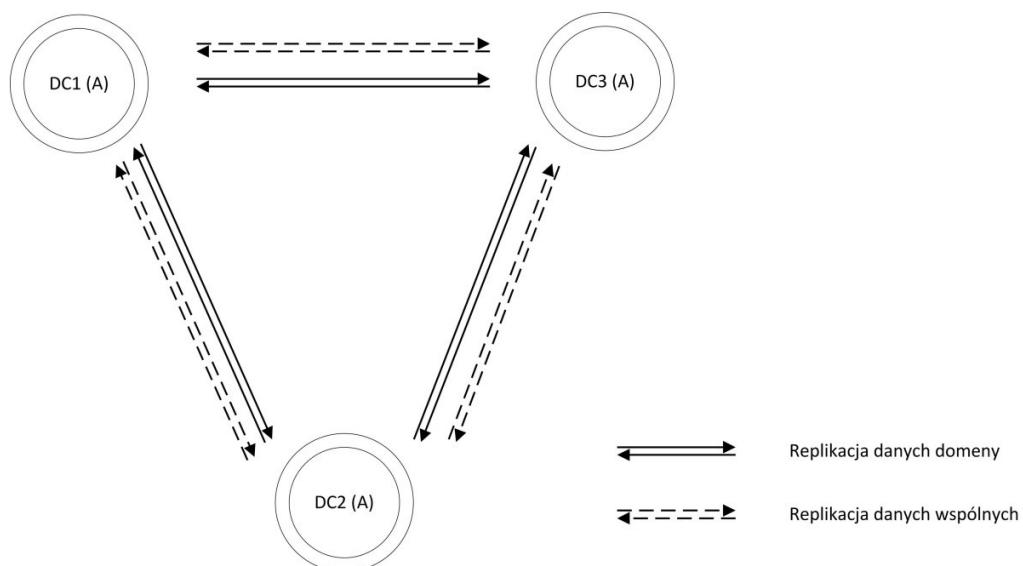
Mechanizm opóźnień w powiadomianiu partnerów replikacji o czekających zmianach opisany jest dalej w ramach materiałów szkoleniowych w rozdziale „Powiadomienia i opóźnienia w ramach mechanizmu replikacji”.

## Replikacja wielu partycji katalogu

Jak to zostało powiedziane w ramach Modułu I partycja katalogu, jest podstawową jednostką replikacji danych w ramach usługi katalogowej. Z tego powodu, w ramach każdej lokacji kontrolery domeny będą tworzyły osobną topografię replikacji dla każdej z partycji katalogu. W szczególności, gdy w ramach lokacji występują tylko kontrolery jednej domeny, istnieć będą co najmniej trzy, osobno wyznaczane pierścienie w ramach topologii replikacji, dla poszczególnych partycji:

- Schematu,
- Konfiguracji,
- Domenowej.

W przypadku, gdy w ramach katalogu utrzymywane są również partycje aplikacyjne (np. ForestDNSZones lub DomainDNSZones), kontrolery domeny utrzymujące dane tych partycji utworzą osobne topologie replikacji danych tych partycji.



W przypadku, gdy w lokacji występują kontrolery domeny z różnych domen, kontrolery te w ramach pojedynczej lokacji utworzą wspólną topografię replikacji dla danych wspólnych katalogu:

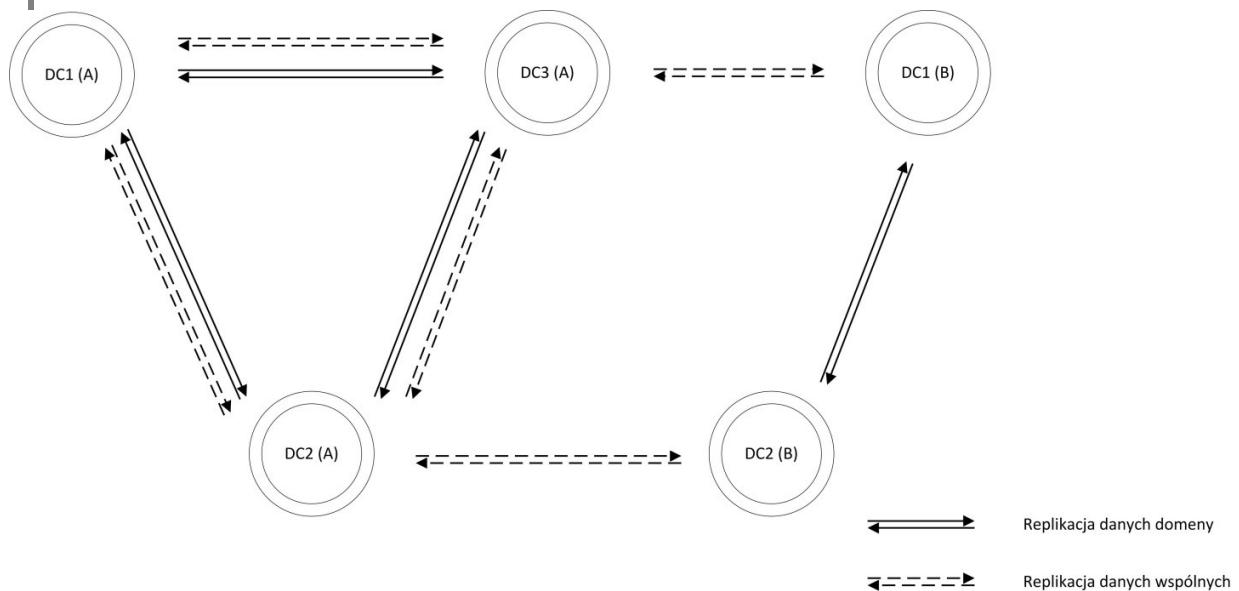
- Schemat
- Konfiguracja.

oraz osobne pierścienie replikacji, dla każdej z partycji domenowych.

### Połączenia używane w ramach replikacji wielu partycji

W ramach jednej domeny, te same połączenia replikacji używane są do replikacji danych zarówno partycji domenowej jak i partycji wspólnych w ramach lasu. Dla replikacji danych schematu i konfiguracji w ramach jednej domeny nie są wymagane więc dodatkowe połączenia replikacji.

Połączenia te pojawiają się, w przypadku gdy w ramach jednej lokacji pracują kontrolery domeny z różnych domen. W takim wypadku, w celu replikacji danych z partycji wspólnych wymagane są nowe połączenia replikacji.



Jeżeli w ramach lokacji pracują kontrolery domeny, utrzymujące partycje aplikacyjne, na przykład wspólną partycję DNS ForestDNSZones, dla tej partycji również utworzona zostanie odpowiednia topologia replikacji w ramach lokacji.

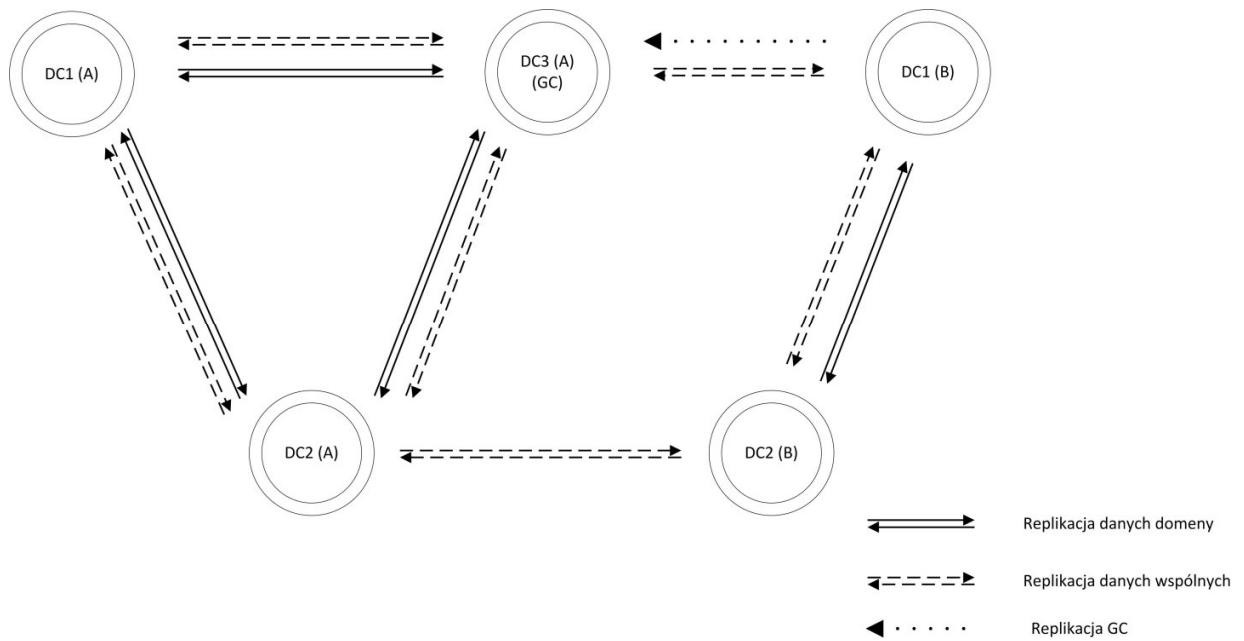
## Replikacja partycji Global Catalog

Kontrolery domeny pełniące rolę serwerów Global Catalog przechowują dane o wszystkich obiektach w ramach lasu, niezależnie od domeny, w której obiekty te są przechowywane.

W przypadku replikacji danych w ramach jednej domeny, dane potrzebne do zbudowania partycji GC replikowane są w ramach tych samych połączeń replikacji, które używane są do replikacji danych wspólnych lasu i partycji domenowych.

W przypadku, gdy w ramach jednej lokacji występują kontrolery domeny więcej niż jednej domeny istniejącej w ramach lasu, replikacja danych wymaganych do utworzenia partycji GC pomiędzy kontrolerami domeny różnych domen wymaga dodatkowego, jedno-kierunkowego połączenia pozwalającego kontrolerowi domeny na replikację danych innej partycji domenowej.

Replikacja danych wymaganych do utworzenia partycji GC zawsze wykonywana jest z partnerem replikacji, z którym wymieniane są informacje dotyczące partycji wspólnych w ramach lasu (schemat, konfiguracja).

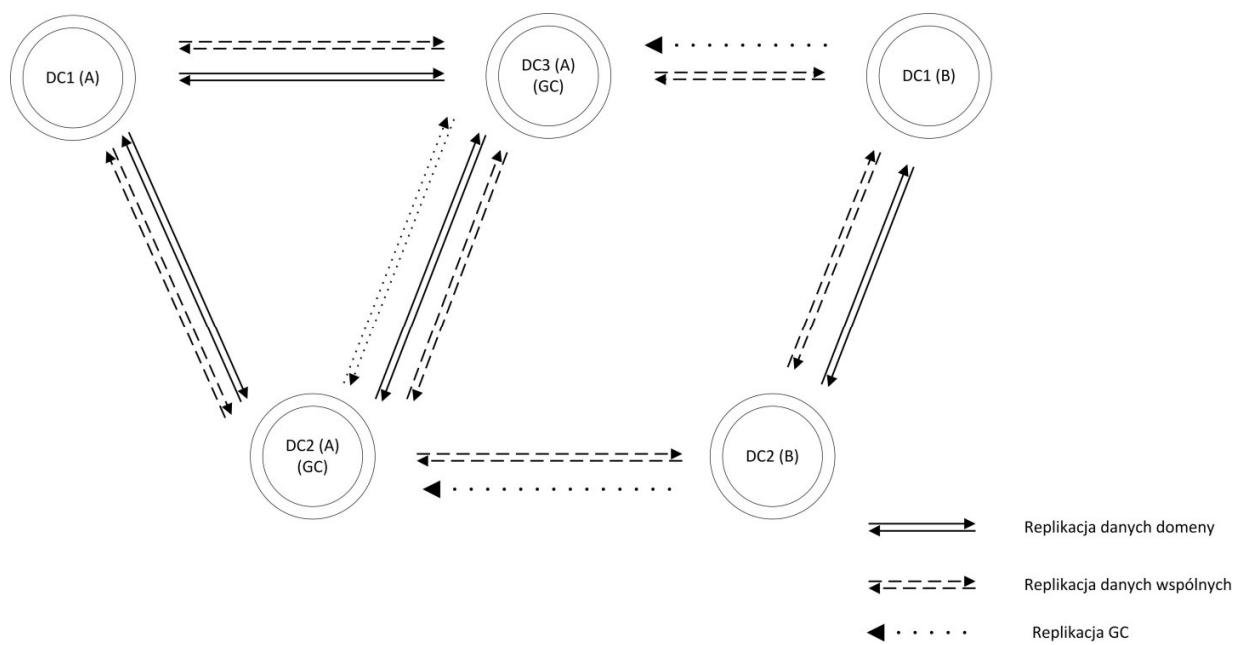


#### Replikacja danych GC a połączenia

Replikacja danych wymaganych do zbudowania partycji GC zawsze jest wykonywana z partnerami replikacji, z którymi replikowane są dane dotyczące partycji wspólnych katalogu.

Replikacja danych wymaganych do zbudowania partycji GC pomiędzy kontrolerem utrzymującym pełną replikę danych a kontrolerem utrzymującym tylko częściową replikę na potrzeby GC jest zawsze jednokierunkowa.

W ramach replikacji danych pomiędzy dwoma kontrolerami domeny, pełniącymi rolę GC i utrzymującymi częściowe repliki danych możliwa jest sytuacja, w której takie kontrolery domeny są dla siebie wzajemnie źródłem informacji.



## Budowanie topologii replikacji: inter-site

### Serwery brzegowe (*bridgehead servers*)

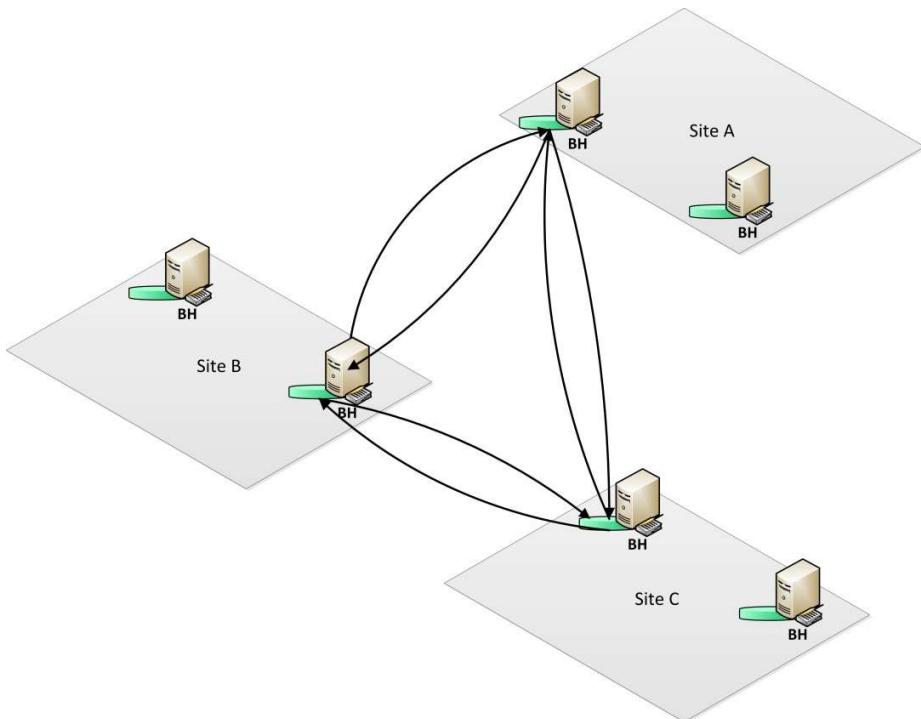
Replikacja pomiędzy lokacjami usługi Active Directory odbywa się pomiędzy serwerami brzegowymi (ang. *bridgehead servers, BH*). Serwer pełniący rolę *bridgehead* replikuje dane z innymi partnerami replikacji, pełniącymi taką samą rolę w innych lokalizacjach.

W ramach każdej z lokalizacji, posiadającej lokalny kontroler domeny, w środowisku z wieloma lokalizacjami i kontrolerami domeny istniał będzie, co najmniej jeden serwer brzegowy dla każdej z partycji katalogu. Serwer brzegowy musi zapewnić replikację w ramach danej lokalizacji wszystkich partycji, które wymagane są w ramach danej lokalizacji.

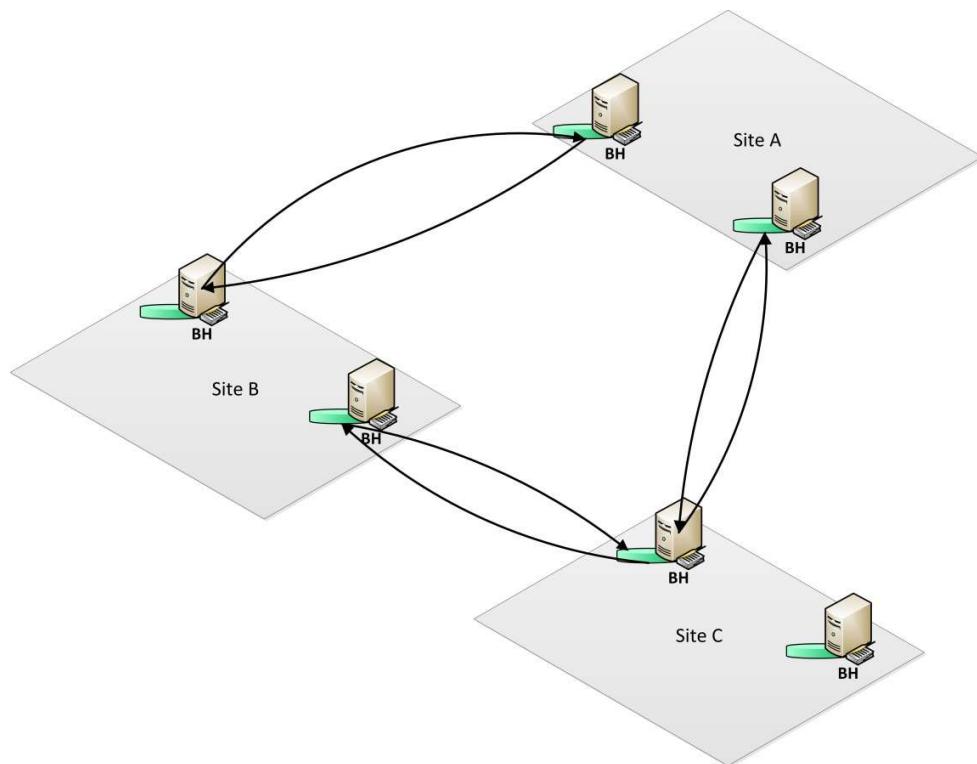
W ramach każdej z lokalizacji musi istnieć jeden serwer pełniący rolę *bridgehead* dla danej partycji katalogu.

Serwer pełniący rolę *bridgehead* wybierany jest automatycznie przez proces KCC działający na kontrolerze domeny pełniącym rolę ISTG w ramach lokalizacji. Domyślnie każdy z kontrolerów domeny w ramach lokalizacji może być wybrany, jako *bridgehead* i wybór ten następuje automatycznie.

W Windows 2000, w ramach jednej lokalizacji może istnieć tylko jeden kontroler domeny pełniący rolę *bridgehead* dla danej partycji katalogu i sposobu replikacji.



W systemach Windows 2003 i późniejszym w ramach jednej lokalizacji różne kontrolery domeny mogą pełnić rolę *bridgehead* dla różnych lokalizacji, z którymi następuje replikacja danych w ramach katalogu.



W ramach Windows 2000 Server wybór serwera, pełniącego rolę *bridgehead* w danej lokacji wykonywany był pomiędzy DC w oparciu o listę kontrolerów domeny uszeregowaną według GUID.

W Windows 2003 i 2008 późniejszych, wybór serwera pełniacego rolę *bridgehead* dla danej partycji stosowany jest losowy algorytm wyboru serwera brzegowego w ramach lokacji (zarówno źródłowej jak i docelowej).

#### **Wyłączenie losowego wyboru serwera *bridgehead* w ramach lokacji**

Losowy wybór serwera *bridgehead* w ramach lokacji może zostać wyłączony poprzez ustawienie bitu `NTDSSETTINGS_OPT_IS_RAND_BH_SELECTION_DISABLED` (0x00000100) w ramach wartości atrybutu `options` obiektu opcji dla lokacji (`nTDSSiteSettings`). W przypadku wyłączenia tego mechanizmu, kontrolery domeny sortowane są w listę według GUID, gdzie na początku listy umieszczone są kontrolery pełniące rolę Global Catalog.

#### **Windows 2008 RODC i wybór serwera brzegowego**

W Windows 2008 wprowadzona została rola serwera RODC, która implementuje zmodyfikowany algorytm wyboru serwera brzegowego. W przypadku RODC, przy wyborze serwera źródłowego brana jest pod uwagę ilość istniejących na DC w lokacji źródłowej obiektów połączeń. Dzięki temu zapewnione jest równoważenie obciążenia kontrolerów domeny w lokacji źródłowej połączeniami z RODC.

Zachowanie to kontrolowane jest przez wartość ***Random BH Loadbalancing Allowed*** w kluczu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters` rejestru kontrolera domeny. Wartość 1 (domyślna) oznacza włączony mechanizm rozłożenia obciążenia, wartość 0 oznacza wyłączenie tego mechanizmu.

W ramach systemu Windows Server 2008 R2 wprowadzono mechanizm automatycznego rozłożenia połączeń pomiędzy serwerami *bridgehead* w ramach replikacji jednej partycji katalogu, pomiędzy dwoma lokacjami. Algorytm ten nie zmienia zachowania w przypadku generowania połączeń replikacji w ramach jednej lokacji.

## Preferowane serwery brzegowe ( *preferred bridgehead servers* )

Proces KCC dokonuje wyboru serwera brzegowego w ramach lokacji w sposób automatyczny, uwzględniając wszystkie dostępne w ramach lokacji kontrolery domeny. W ramach wyboru serwera przez KCC, każdy z serwerów jest potencjalnym serwerem brzegowym.

W ramach lokacji, istnieje możliwość wskazania preferowanych serwerów brzegowych dla wybranego rodzaju transportu danych katalogu (IP, SMTP). Serwer wskazany, jako serwer brzegowy, dla danego rodzaju transportu posiada wartość odpowiadającą DN do obiektu reprezentującego dany protokół w atrybucie ***bridgeheadTransportList***. Ponieważ atrybut ten należy do pary atrybutów połączonych, na odpowiadającym mu atrybucie ***bridgeheadTransportListBL***, na odpowiednim kontenerze transportu znajduje się lista wszystkich serwerów, skonfigurowanych jako preferowane serwery brzegowe.

Jeżeli w ramach wartości ***bridgeheadTransportListBL*** występuje, co najmniej jeden kontroler domeny dla danej lokacji KCC przy wyborze serwera brzegowego dla tej lokacji bierze pod uwagę tylko te serwery, które znajdują się na tej liście. Jeżeli w danej lokacji zdefiniowane zostały preferowane serwery brzegowe, to należy upewnić się, że serwery te są w stanie replikować wszystkie partycje katalogu wymagane dla danej lokacji.

### Serwery preferowane a awarie kontrolerów domeny

Wskazanie serwerów preferowanych, jako serwery przyczółkowe dla danej lokacji powoduje, że proces KCC nie uwzględnia w ramach swojej pracy żadnych innych serwerów niż te, które zostały wskazane na liście serwerów preferowanych. W przypadku awarii wszystkich serwerów, wskazanych jako serwery preferowane w ramach lokacji, proces KCC nie wybierze więc nowego serwera przyczółkowego dla danej lokacji.

Sytuacja taka może prowadzić do przerwania ciągłości replikacji danych katalogu.

### Serwery preferowane a istniejące obiekty połączeń

Jeżeli w ramach danej lokacji usługi katalogowej wskazany zostanie preferowany serwer przyczółkowy, konfiguracja ta odnosi się zarówno do nowych jak i do istniejących obiektów połączeń. W ramach wykonywanych uaktualnień, po wskazaniu serwera(ów) preferowanych proces KCC skonfiguruje zarówno nowe połączenia używając tych serwerów jak i przekonfiguruje automatycznie zarządzane, już istniejące połączenia tak, aby korzystały z serwerów preferowanych.

Zachowanie takie należy uwzględnić planując obciążenie serwerów przyczółkowych.

## Wykrywanie niedziających połączeń replikacji

Proces KCC działający wewnątrz lokacji, jak i proces KCC działający na serwerze pełniącym rolę ISTG mają za zadanie utrzymać topologię połączeń uwzględniającą aktualnie dostępne kontrolery domeny. W tym celu, KCC używa kryteriów w celu określenia, czy partnerzy replikacji są nadal dostępni. Jeżeli stwierdzona zostanie niedostępność partnera replikacji, KCC próbuje utworzyć połączenie replikacji z innym partnerem replikacji. Jako kryteria istnienia połączenia z danym kontrolerem domeny przyjmowane są dwa parametry:

- Liczba nieudanych prób replikacji
- Czas od ostatniej nieudanej próby replikacji.

W przypadku połączeń replikacji w ramach jednej lokacji:

- Dla połączeń bezpośrednich w ramach lokacji, z bezpośredniimi partnerami replikacji:
  - Minimalna liczba nieudanych prób połączeń: 0 (natychmiast)
  - Czas od ostatniego udanego połączenia: 2 godziny
- Dla połączeń w ramach lokacji, wynikających z potrzeby skrócenia pierścienia replikacji:
  - Minimalna liczba nieudanych prób połączeń: 1
  - Czas od ostatniego udanego połączenia: 12 godziny

W przypadku połączeń replikacji w ramach jednej lokacji:

- Minimalna liczba nieudanych prób połączeń: 1
- Czas od ostatniego udanego połączenia: 2 godziny

Wartości tych parametrów mogą być kontrolowane poprzez wpisy w rejestrze w gałęzi HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:

Klucz	Wartość domyślna	Opis
<b>Połączenia pomiędzy lokacjami</b>		
IntersiteFailuresAllowed	1	Liczba nieudanych prób replikacji
MaxFailureTimeForIntersiteLink (secs)	7200 (sek)	Czas od ostatniego udanego połączenia
<b>Połączenia w ramach lokacji</b>		
<b>Bezpośredni partnerzy replikacji</b>		
CriticalLinkFailuresAllowed	0	Liczba nieudanych prób replikacji
MaxFailureTimeForCriticalLink	7200 (sek)	Czas od ostatniego udanego połączenia
<b>Połączenia skracające pierścień replikacji</b>		
NonCriticalLinkFailuresAllowed	1	Liczba nieudanych prób replikacji
MaxFailureTimeForNonCriticalLink	43200 (sec)	Czas od ostatniego udanego połączenia

## **Połączenia domeny związane z usuniętymi kontrolerami domeny**

W środowiskach opartych o system Windows Server 2003 przed SP1 lub wcześniejszych, w ramach partnerów replikacji danego kontrolera domeny mogą występować kontrolery domeny, które nie istnieją już w ramach organizacji. W przypadku poprawnego usunięcia kontrolera domeny z organizacji wykonywane są operacje związane z procesem usunięciem informacji o tym kontrolerze domeny.

W przypadku systemów działających w oparciu o Windows Server 2003 przed SP1, w ramach tego procesu:

- Usuwany jest obiekt „NTDS Settings” reprezentujący dany kontroler domeny
- Z atrybutu *repsFrom* obiektu reprezentującego daną partycję (kontekst nazewniczy) katalogu nie są usuwane wpisy dotyczące danego kontrolera domeny, jeżeli nie upłynął okres określony przez atrybut *repTopologyStayOfExecution*. Wpisy te usuwane są przez KCC automatycznie po upływie czasu określonego w tym atrybutie.

Atrybut *repTopologyStayOfExecution* definiuje okres pomiędzy usunięciem kontrolera domeny, a jego całkowitym usunięciem z topologii replikacji dla danej partycji. Domyslnie wynosi on 14 dni, maksymalna wartości to  $\frac{1}{2}$  czasu *tombstoneLifetime*.

W ramach Windows Server 2003 SP1 i późniejszych wersji systemu operacyjnego zachowanie to zostało zmienione, i w ramach procedury usunięcia kontrolera domeny:

- Usuwany jest obiekt „NTDS Settings” reprezentujący dany kontroler domeny
- Z atrybutu *repsFrom* obiektu reprezentującego daną partycję (kontekst nazewniczy) usuwana jest informacja o obiekcie kontrolera domeny.

Mechanizm uwzględniający okres definiowany przez *repTopologyStayOfExecution* w systemach tych został wyłączony z użycia.

## Równoważenie obciążenia połączaniami (load balancing)

W ramach połączeń pomiędzy lokacjami Active Directory algorytm KCC ma za zadanie zapewnić replikację danych wszystkich wymaganych partycji do docelowych kontrolerów domeny. W tym celu algorytm ten tworzy połączenia pomiędzy serwerami brzegowymi w poszczególnych lokacjach.

Ze względu na specyfikę działania algorytmu KCC i mechanizm wyboru brzegowych kontrolerów domeny w ramach lokacji, w przypadku dużej liczby kontrolerów domeny biorących udział w procesie replikacji z daną lokacją (na przykład lokacja centralna w ramach topologii hub-n-spoke) istnieje możliwość przypisania do jednego z kontrolerów domeny zbyt duże liczby połączeń przychodzących lub wychodzących. Powodować to może problemy z wydajnością danego kontrolera domeny, co może prowadzić do problemów z replikacją danych katalogu.

Aby uniknąć nadmiernego obciążenia kontrolerów domeny przez dużą liczbę partnerów replikacji konieczne jest zapewnienie mechanizmów równoważenia obciążenia pomiędzy kontrolerami domeny.

### **Windows 2000**

W Windows 2000 KCC zakładało tylko jeden serwer brzegowy dla danej partycji w lokacji, co oznaczało, że w przypadku wielu kontrolerów domeny będących partnerami replikacji w relacji z daną lokacją wszystkie połączenia replikacji, będą tworzone przez KCC w ramach tego kontrolera domeny.

Windows 2000 nie posiada żadnych automatycznych mechanizmów równoważenia obciążenia pomiędzy kontrolerami domeny w ramach jednej lokacji. W celu zapewnienia równoważenia obciążenia w ramach lokacji wymagających tego typu konfiguracji, wymagane jest w Windows 2000 wyłączenie mechanizmów KCC i tworzenie ręcznie połączeń replikacji pomiędzy poszczególnymi kontrolerami domeny.

### **Windows 2003**

Algorytm KCC implementuje w procesie wyboru serwera brzegowego, z którym zostanie nawiązane połączenie mechanizm losowego wyboru serwera spośród dostępnych w ramach lokacji kandydatów. Mechanizm ten zapewnia rozłożenie połączeń pomiędzy wiele kontrolerów domeny w ramach lokacji w sposób losowy, lecz nie zapewnia równego rozłożenia obciążenia pomiędzy nimi.

Mechanizm ten nie zapewnia jak wspomniane zostało równomiernego rozłożenia obciążenia pomiędzy kontrolerami domeny, jak i nie uwzględnia nowo dodanych kontrolerów domeny w ramach lokacji. Dodatkowo KCC nie wykonuje zmian w utworzonych obiektach połączeń, jeżeli nie jest to wymagane ze względu na zmiany w katalogu wpływające na dany obiekt połączenia (na przykład usunięcie kontrolera domeny). W sytuacji, gdy do przedstawionej powyżej konfiguracji w lokacji A dodany zostanie dodatkowy kontroler domeny, nie zmieni to konfiguracji już istniejących połączeń.

W celu zapewnienia równoważenia obciążenia połączaniami kontrolerów domeny w ramach jednej lokacji w środowisku Windows 2003 można skorzystać z następujących opcji:

- Ręcznie zarządzać obiektami połączeń
- Zastosować narzędzie ADLB pochodzące z Windows 2003 Branch Office Guide

ADLB jest to dodatkowe narzędzie, którego zadaniem jest utworzenie połączeń, zapewniając równomierne rozmieszczenie tych połączeń pomiędzy kontrolerami domeny znajdującym się w ramach danej lokacji. Mechanizm KCC działa w jednej lokalizacji optymalizując połączenia w ramach tej lokacji. ADLB obchodzi to ograniczenie, i pozwala na zarządzanie połączonymi pomiędzy lokacjami, modyfikując połączenia przychodzące jak i wychodzące w ramach połączonych lokacji.

#### Liczba połączeń przetwarzanych przez ADLB

W ramach pojedynczego uruchomienia ADLB przetwarza jedynie 10 obiektów połączeń. Jeżeli w ramach danej lokacji istnieje więcej niż 10 obiektów połączeń, w celu ich zrównoważenia konieczne jest wielokrotne uruchomienie ADLB.

#### ADLB vs KCC

W środowisku, w którym w celu uzyskania równomiernego obciążenia kontrolerów domeny w ramach lokacji stosowane jest ADLB nadal mogą pracować mechanizmy KCC. KCC nadal może działać w ramach lokacji w celu aktualizacji informacji o połączeniach. Ponieważ KCC nie modyfikuje istniejących połączeń, tak dugo jak połączenia te działają poprawnie

## Windows Server 2008 i Windows 2008 R2

W ramach systemu operacyjnego Windows Server 2008:

- W przypadku kontrolerów domeny utrzymujących pełną replikę danych katalogu (RWDC) w ramach katalogu działają takie same mechanizmy jak w przypadku rozwiązania opartego na Windows 2003. Standardowo, w ramach lokalizacji nie jest zapewniane zrównoważenie połączeń pomiędzy poszczególne kontrolery domeny w lokacji. Zapewnienie takiej konfiguracji wymaga ręcznego zarządzania połączonymi lub użycia ADLB.
- W przypadku kontrolerów domeny, w trybie tylko do odczytu (RODC) stosowany jest algorytm zapewniający rozłożenie obciążenia pomiędzy poszczególne kontrolery domeny w ramach lokacji, z którą dane replikuje RODC. Algorytm ten opiera się na złożeniach prawdopodobieństwa przypisania kontrolera domeny do danego serwera brzegowego i powinien zapewnić zrównoważenie połączeń tworzonych przez RODC w sposób równy, pomiędzy kontrolerami domeny.

W ramach systemu Windows Server 2008 R2 algorytm zaimplementowany dla kontrolerów domeny w trybie tylko do odczytu został zaimplementowany również w przypadku pełnych kontrolerów domeny. W przypadku zmiany liczby kontrolerów domeny w ramach lokacji proces KCC w ramach Windows 2008 R2 powinien zapewnić równomierne rozłożenie zarówno połączeń RODC jak i RWDC pomiędzy partnerami replikacji, w sposób analogiczny jak w przypadku RODC.

## **Łączenie połączeń replikacji (*site link bridges*)**

### ***Site link bridges***

Obiekt połączenia (*site link*) reprezentuje w ramach konfiguracji usługi katalogowej połączenie sieciowe pomiędzy poszczególnymi lokacjami usługi katalogowej. Pojedynczy obiekt połączenia powinien reprezentować połączenie tylko pomiędzy dwoma lokacjami.

Obiekty połączeń w ramach konfiguracji usługi katalogowej domyślnie tworzone są jako obiekty przechodnie (ang.*transitive*) lub inaczej *bridged*. Oznacza to, że w przypadku gdy lokacja A jest połączona z lokacją B, a lokacja B z lokacją C, to poprzez przechodnie obiekty połączeń pomiędzy lokacjami może zostać ustanowione połączenie pomiędzy lokacją A i C.

Taka konfiguracja obiektów połączeń pozwala w razie awarii kontrolera domeny w lokacji łączącej dwie inne lokacje stworzyć połączenie replikacji pomiędzy poszczególnymi kontrolerami domeny w lokacjach, które nie są ze sobą bezpośrednio połączone z punktu widzenia topologii fizycznej katalogu.

W przypadku, gdy istniejąc trzy lokacje: A, B i C, gdzie A jest połączone obiektem połączenia z lokacją B oraz C jest połączone obiektem połączenia z lokacją B, kontrolery domeny z lokacji A oraz C nawiążą połączenie z kontrolerami domeny w lokacji B.

W przypadku awarii kontrolera domeny w lokacji B proces KCC korzystając z tego, że połączenia pomiędzy lokacjami są przechodnie, będzie mógł stworzyć połączenie bezpośrednio pomiędzy lokacjami A i C.

W takim przypadku koszt połączenia pomiędzy lokacjami, tworzony w oparciu o przechodnie obiekty połączeń, równy jest sumarycznemu kosztowi wszystkich obiektów połączeń tworzących pojedynczą trasę replikacji. Przy założeniu kosztu 100 dla każdego z połączeń pomiędzy lokacjami A, B i C, koszty połączeń przedstawiają się następująco:

- A -> B: 100
- B -> C: 100
- A -> C: 200

W standardowej sytuacji, gdy w każdej z lokalizacji działa kontroler domeny, algorytm KCC zapewni połączenie pomiędzy partnerami replikacji o najniższym koszcie połączenia.

Interwał replikacji w ramach ścieżki replikacji złożonej z wielu obiektów łączy odpowiadającą największemu interwałowi ustalonemu dla łączącego w ramach całej ścieżki replikacji.

Jeżeli dla obiektów łączących się na całość ścieżki replikacji ustalone są wartości atrybutu *options*, w celu określenia wynikowej wartości tego atrybutu wykonywana jest operacja AND dla poszczególnych wartości atrybutów.

## ***Bridge all site-links (BASL)***

Opcja *Bridge all site-links* powoduje, że wszystkie połączenia w ramach usługi katalogowej traktowane są jako połączenia przechodnie. Opcja ta jest domyślnie włączona w ramach konfiguracji katalogu i nie wymaga dodatkowej konfiguracji. Opcja ta znajduje się we właściwościach obiektów, reprezentujących protokoły transportu replikacji – IP, SMTP.

W sieciach w pełni routowanych, w których ruch pomiędzy poszczególnymi lokacjami nie jest blokowany za pomocą firewall nie ma potrzeby wyłączania opcji BASL ponieważ zapewnia ona utworzenie optymalnych połączeń pomiędzy poszczególnymi lokacjami na wypadek awarii kontrolerów domeny w poszczególnych lokacjach.

W przypadku wyłączenia opcji BASL możliwe jest ręczna konfiguracja połączenia pomiędzy poszczególnymi obiektami łączy poprzez manualne stworzenie *site link bridge*. Konfiguracja taka może być wymagana gdy, istnieje potrzeba ścisłego kontrolowania ścieżek replikacji w sieci, ze względu na brak routingu pomiędzy segmentami sieci lub konfiguracje filtrowania ruchu sieciowego.

W większości sytuacji ręczne tworzenie połączeń pomiędzy obiektami łączy nie powinno być wymagane.

### ***Włączona BASL a proces lokalizacja SYSVOL***

Włączona opcja BASL wymagana jest dla poprawnego działania mechanizmu lokalizacji SYSVOL przez klienta usługi katalogowej, w przypadku gdy używany jest mechanizm *Site Costed Reerrals*.

Lokalizacja SYSVOL odbywa się z użyciem innego mechanizmu, niż mechanizm lokalizacji kontrolera domeny. Jeżeli wybór SYSVOL ma być wykonywany z uwzględnieniem informacji o koszcie połączeń pomiędzy lokacjami, w celu określenia najbliższej, z punktu widzenia kosztu połączenia repliki SYSVOL wymagane jest aby w konfiguracji usługi katalogowej włączona była opcja *Bridge all site-links*.

W przypadku, gdy ze względu na konfigurację sieci lub inne wymagania opcja BASL dla mechanizmów replikacji danych katalogu nie jest wskazana a należy zachować mechanizmy lokalizacji repliki SYSVOL ze względu na koszt, możliwe jest wyłączenie mechanizmu przechodniości z punktu widzenia KCC dla danej lokacji. Składania polecenia repadmin dla takiej konfiguracji lokacji przedstawiona została poniżej:

```
repadmin /siteoptions W2K3_BRIDGES_REQUIRED
```

Opcja ta powoduje, że z punktu widzenia procesu KCC łączenie poszczególnych obiektów połączeń nie jest możliwe, jednak nadal jest to możliwe z punktu widzenia kalkulacji kosztu połączenia do repliki SYSVOL (i ogólnie DFS)

## ***Harmonogram połączeń***

Dla poprawnego działania mechanizmów *site link bridging* wymagane jest zapewnienie odpowiedniej konfiguracji harmonogramu replikacji poszczególnych obiektów łączy, które mogą tworzyć pojedynczą ścieżkę replikacji.

W przypadku włączonej opcji *Bridge all site-links* lub ręcznie utworzonych połączeń pomiędzy obiektami łączy, aby replikacja była możliwa przez ścieżkę złożoną z kilku obiektów łączy, muszą one w konfiguracji harmonogramu replikacji zawierać przynajmniej jeden, nakładający się okres czasu.

W konfiguracji, w której mamy trzy lokacje, A, B i C, gdzie istnieje obiekt łączący pomiędzy lokacjami A i B oraz B i C oraz włączona jest opcja BASL, w przypadku niedostępności kontrolera domeny w lokacji B możliwa jest bezpośrednia ścieżka replikacji pomiędzy lokacjami C i A.

Aby połączenie takie mogło powstać i zapewnić replikację danych, dla obiektu połączenia łączącego lokację A z B oraz obiektu łączącego lokację B z C musi istnieć wspólny okres replikacji danych w ramach harmonogramu replikacji.

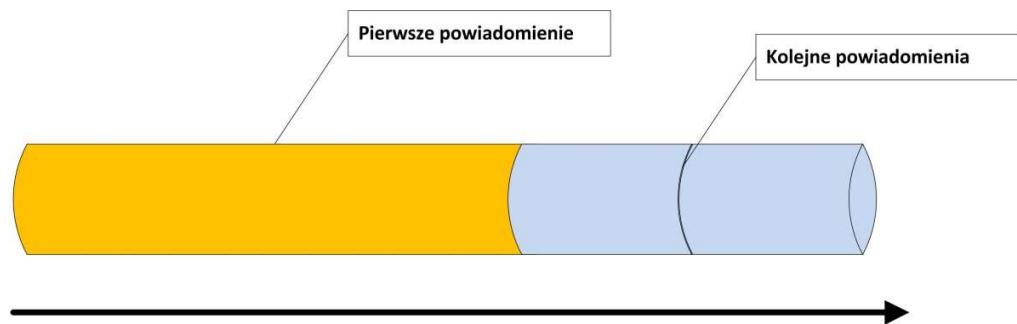
Zależność taka wymagana jest również, w przypadku gdy połączenia pomiędzy obiektami łączy tworzone są ręcznie przy wyłączonym mechanizmie BASL.

## Powiadomienia i opóźnienia w ramach mechanizmu replikacji

Replikacja katalogu Active Directory działa w trybie *notify & pull*, w którym kontroler domeny posiadający uaktualnione informacje wysyła powiadomienie do partnerów replikacji. Partner replikacji następnie inicjuje proces replikacji danych.

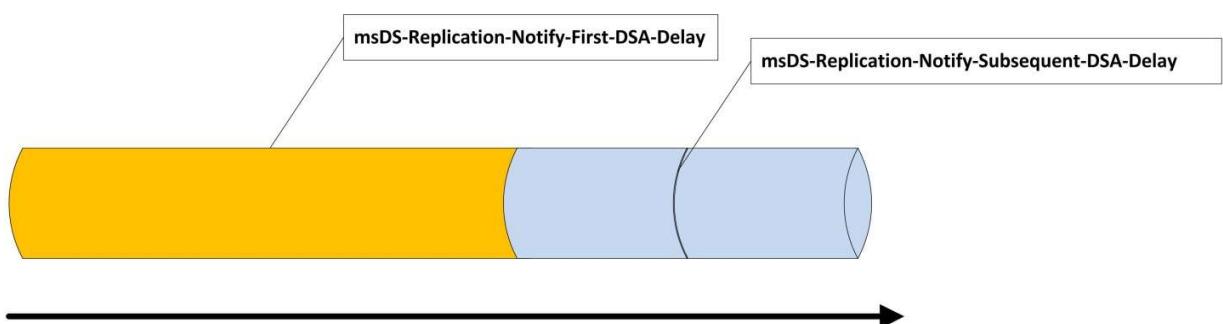
W celu optymalizacji tego procesu oraz zabezpieczeniu kontrolera domeny przed równoczesnymi żądaniami od wielu kontrolerów domeny w ramach mechanizmu replikacji danych został wprowadzony mechanizm opóźnień w powiadomieniach partnerów replikacji. Mechanizm ten wprowadza dwa opóźnienia:

- Opóźnienie w wysłaniu powiadomienia do pierwszego partnera replikacji w ramach danej partycji katalogu po otrzymaniu zmiany
- Opóźnienie w wysłaniu powiadomienia dla kolejnych partnerów replikacji w ramach danej partycji katalogu, po wysłaniu powiadomienia do pierwszego partnera replikacji.



Opóźnienia te określają opóźnienia w wysłaniu kolejnych powiadomień do partnerów replikacji wskazywanych przez wartość atrybutu *repsTo* dla danej partycji katalogu. Wartość tych opóźnień kontrolowana jest odpowiednio poprzez wartość następujących atrybutów obiektu partycji katalogu:

- ***msDS-Replication-Notify-First-DSA-Delay***: opóźnienie w wysłaniu powiadomienia po otrzymaniu zmiany do pierwszego z partnerów replikacji. Wartość wyrażona w sekundach.
- ***msDS-Replication-Notify-Subsequent-DSA-Delay***: opóźnienie w wysłaniu powiadomienia do kolejnych partnerów replikacji po przesłaniu powiadomienia do pierwszego z partnerów.



### **Konfiguracja opóźnień związanych z replikacją poprzez rejestr systemu**

Przedstawione powyżej atrybuty definiowane są dla całej partycji katalogu od systemu Windows 2003. W Windows 2000 konfiguracja ta odbywała się poprzez rejestr systemu dla pojedynczych kontrolerów domeny. W tym wypadku używane są wpisy, odpowiednio:

- Replicator notify pause after modify (sec)
- Replicator notify pause between DSAs (sec)

Obie wartości typu DWORD konfigurowane są w kluczu rejestru  
HKLM\System\CurrentControlSet\Services\NTDS\Parameters.

Wpisy te respektowane są również przez kontrolery domeny działające w oparciu o system wyższy niż Windows 2000.

Domyślna wartość tych opóźnień zależy od wersji systemu operacyjnego:

<b>Wersja OS</b>	<b>Pierwsze powiadomienie</b>	<b>Kolejne powiadomienia</b>
Windows 2000	15 min	5 minut
Windows 2003 i późniejsze	15 sekund	3 sekundy

W przypadku topologii replikacji w ramach jednej lokacji, przy zachowaniu reguły trzech przejść pomiędzy partnerami replikacji opóźnienia te powodują, że czas propagacji w ramach lokacji pomiędzy poszczególnymi partnerami replikacji może wynosić odpowiednia dla Windows 2000 / Windows 2003 45 minut / 45 sekund.

## Urgent replication

W przypadku zmian niektórych, istotnych dla mechanizmu dostępu atrybutów w ramach usługi katalogowej Active Directory stosuje do replikacji tych zmian mechanizm *urgent replication*.

Mechanizm *urgent replication* wyzwalany jest na podstawie następujących zdarzeń:

- Informacji o zablokowaniu konta (*account lockout*)
- Zmiana w polityce blokady kont (*account lockout policy*)
- Zmiana polityki domenowej haseł
- Zmiana hasła komputera pełniącego rolę kontrolera domeny
- Zmiana haseł przechowywanych przez LSA (na przykład hasła relacji zaufania – obiekt klasy *secret*)
- Zmiana właściciela roli RID Master.

Mechanizm *urgent replication* nie oznacza obejścia normalnego trybu replikacji danych. Replikacja w trybie *urgent* oznacza, że kontroler domeny wysyła powiadomienie o zmianach do partnera replikacji, bez wprowadzania dodatkowego opóźnienia, które normalnie istnieje przed powiadomieniem partnerów replikacji. W przypadku zmiany jednego z atrybutów, replikowanych w trybie *urgent* powiadomienia do partnerów replikacji wysyłane są natychmiast, bez dodatkowego opóźnienia.

### FGPP i urgent replication

W Windows 2008 wprowadzono nowy mechanizm pozwalający na definiowanie wielu polityk haseł – *Fine Grained Password Policy*. Zmiany do obiektów definiujących politykę haseł dla mechanizmu FGPP nie są replikowane w trybie *urgent*.

Replikacja w trybie *urgent* zachodzi pomiędzy partnerami replikacji w ramach jednej lokacji, chyba że pomiędzy lokacjami skonfigurowany został mechanizm powiadomień o zmianach. W takim wypadku, powiadomienia w ramach replikacji w trybie *urgent* wysyłane są również do partnerów replikacji w innych lokacjach, dla których włączone został mechanizm powiadomień o zmianach.

Informacja o zablokowaniu konta replikowana jest w trybie *urgent* do:

- Kontrolera domeny pełniącego rolę PDC Emulator
- Wszystkich kontrolerów domeny w ramach lokacji, w której pracuje kontroler, na którym nastąpiła blokada konta
- Wszystkich kontrolerów domeny, w ramach lokacji połączonych z lokacją, w której nastąpiła blokada konta, o ile pomiędzy lokacjami włączony został mechanizm powiadomień o zmianie hasła.

Powiadomienie wysyłane do partnerów replikacji w trybie *urgent* posiada ustawioną odpowiednią flagę identyfikującą je jako powiadomienie wysiane w tym trybie.

## Replikacja zmiany hasła

Zmiana hasła użytkownika podlega dodatkowemu mechanizmowi replikacji poza normalnym trybem replikacji i replikacją w trybie *urgent*. W przypadku zmiany hasła użytkownika na danym kontrolerze domeny, replikacja hasła następuje:

- Natychmiast, poza standardowymi mechanizmami replikacji i harmonogramem, bezpośrednio do kontrolera domeny pełniącego rolę PDC Emulator w ramach domeny
- W ramach normalnych mechanizmów replikacji do kontrolerów domeny w ramach tej samej lokacji i w innych lokacjach.

Replikacja informacji o zmianie hasła, wykonywana bezpośrednio z PDC Emulatorem korzysta z mechanizmu wywołania RPC i jest podejmowana na zasadzie *best effort*. W przypadku, gdy próba taka się nie powiedzie, zmiana hasła replikowana jest do wszystkich kontrolerów domeny (włączając PDC Emulator) w ramach standardowych mechanizmów replikacji. Do replikacji zmiany hasła użytkownika nie jest używany mechanizm powiadomień w trybie *urgent*.

#### AvoidPDConWAN

Administrator może kontrolować zachowanie mechanizmu przekazywania haseł do PDC Emulatora poprzez wpis w rejestrze kontrolera domeny. Wpis AvoidPDConWAN w kluczu HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters z wartością 1 oznacza, że kontroler domeny nie powinien próbować przesyłać hasła do PDC Emulator. Wartość 0 lub brak wpisu oznacza standardowe zachowanie tego mechanizmu.

# Replikacja katalogu Active Directory

## **Moduł III**

### **Model replikacji usługi katalogowej**

## Partycje i identyfikatory

### Identyfikatory repliki katalogu

Każda z replik katalogu identyfikowana jest w ramach mechanizmów replikacji danych unikalnie przez następujące atrybuty:

Klasa obiektu	Opis
FQDN	Nazwa DNS kontrolera domeny utrzymująca replikę katalogu. Nazwa ta nie występuje wewnętrznych danych dotyczących replikacji katalogu, wymagana jest jednak do poprawnej komunikacji z innymi kontrolerami domeny w ramach sieci.
DSA GUID	Wartość atrybutu <i>objectGUID</i> instancji obiektu klasy NTDSDSA reprezentującego dany kontroler domeny w ramach mechanizmów replikacji danych. Wartość tego atrybutu nie zmienia się w trakcie czasu życia kontrolera domeny i jest unikalna pomiędzy innymi replikami katalogu
InvocationID	Identyfikator aktualnej instancji bazy danych NTDS.DIT utrzymywanej w ramach danej repliki katalogu. Baza danych NTDS.DIT przechowuje dane katalogu. Ze względu na działanie mechanizmów replikacji i określania danych wymaganych do replikacji pomiędzy partnerami replikacji identyfikator ten zmienia się w trakcie życia kontrolera domeny.

### DSA GUID

Wartość DSA Guid używana jest do rejestracji rekordu SRV w ramach strefy \_MCDCS usługi DNS powiązanej z usługą katalogową. W oparciu o ten atrybut tworzony jest rekord CNAME dla nazwy kontrolera domeny z wartością:

Nazwa	Typ	Rekord DNS
Nazwa DC	CNAME	<DSAGUID>._msdcs.<Forest root DNS>

W oparciu o tą nazwę, partnerzy replikacji dokonują lokalizacji danego kontrolera domeny w sieci.

W przypadku systemów opartych o Windows Server 2003 przed SP1 i wcześniejszych kontrolerów domeny próbuje rozwiązać nazwę partnera replikacji poprzez rekord CNAME. Jeżeli ta operacja nie powiedzie się, kontroler domeny nie jest w stanie rozwiązać nazwy i próba replikacji kończy się niepowodzeniem.

W przypadku kontrolerów domeny działających w oparciu o Windows Server 2003 z SP1 i późniejszym kontrolerem domeny, w trakcie lokalizacji partnera replikacji próbuje rozwiązać nazwę według następującego schematu:

- Kontroler domeny próbuje rozwiązać nazwę partnera replikacji używając rekordu CNAME opartego o DSA GUID.
- W przypadku niepowodzenia poprzedniego kroku, kontroler domeny próbuje rozwiązać nazwę partnera replikacji używając rekordu A dla danego kontrolera domeny.
- W przypadku niepowodzenia, kontroler domeny próbuje rozwiązać nazwę partnera replikacji używając nazwy NetBIOS i ogłoszenia nazwy NetBIOS w sieci.
- Jeżeli żadna z trzech prób nie zakończyła się powodzeniem próba replikacji danych kończy się niepowodzeniem.

Ze względu na ten schemat rozwiązywania nazw DNS w trakcie lokalizacji partnera replikacji, każdy z kontrolerów domeny biorących udział w replikacji danych powinien mieć poprawnie zarejestrowane co najmniej dwa rekordy DNS:

- Rekord CNAME oparty o DSA GUID w ramach strefy \_MSDCS lasu usługi katalogowej.
- Rekord A w ramach odpowiedniej strefy DNS dla domeny.

### **Invocation ID**

Atrybut *InvocationID* obiektu NTDSDSA identyfikuje aktualnąinstancję bazy danych NTDS.DIT danego kontrolera domeny. Identyfikator ten używany jest, w celu określenia przez partnerów replikacji zakresu zmian wymaganych do replikacji pomiędzy instancjami.

Początkowa wartość *InvocationID* tworzona jest w trakcie promocji kontrolera domeny i jest taka sama jak wartość DSA GUID, czyli objectGUID dla obiektu NTDSDSA kontrolera domeny. Wartość ta może ulegać zmianie w trakcie życia kontroler domeny w następujących przypadkach:

- Odtworzenie bazy danych z kopii zapasowej w poprawny sposób
- Dodania lub usunięcia i ponownego dodania partycji katalogu (*re-host*) w trybie do zapisu do zestawu partycji utrzymywanych w ramach danej repliki katalogu.

#### **Wymuszenie zmiana wartości InvocationID**

Administrator może wymusić zmianę wartości *InvocationID* poprzez zmianę w rejestrze kontrolera domeny wpisując w kluczu **HKLM\System\CurrentControlSet\Services\NTDS\Parameters**, parametr **Database restored from backup** (typ DWORD) z wartością 1 i restartując kontroler domeny.

**Operacja taka nie powinna być wykonywana w odniesieniu do produkcyjnych kontrolerów domeny!!!**

**Użycie tego wpisu w rejestrze wymaga przeprowadzenie odpowiedniej, odrębnej od standardowej, operacji przywrócenia kontrolera domeny!!!**

#### **Odtworzenie danych DC i zmiana InvocationID**

Poprawna metoda odtworzenia danych usługi katalogowej, w szczególności odtworzenia bazy danych w ramach kontrolera domeny musi dokonywać zmiany *InvocationID* w ramach lokalnej instancji NTDS.DIT. Brak tej zmiany powoduje problemy w działaniu mechanizmów replikacji i może prowadzić do poważnych problemów z działaniem usługi katalogowej.

Aktualną wartość atrybutów DSA GUID jak i *InvocationID* dla kontrolera domeny można uzyskać poprzez polecenie repadmin.exe z następującymi parametrami:

```
repadmin /SHOWREPL <FQDN kontrolera domeny>
```

W wyniku polecenia informacje te dostępne są w pozycjach:

- DSA GUID: DC Object GUID
- InvocationID: DC InvocationID

W ramach obiektu klasy NTDSDSA reprezentującego kontroler domeny przechowywane są wszystkie wartości *InvocationID* jakie były używane przez dany kontroler domeny w ramach jego okresu życia. Informacja ta przechowywana jest w ramach wartości atrybutu *retiredRep/DSA Signatures* obiektu „NTDS Settings” (NTDSDSA) dla danego kontrolera domeny.

Każdy z kontrolerów domeny przechowuje informację o obecnych i poprzednich wartościach *InvocationID* dla baz danych, w ramach których przechowywana jest dana partycja katalogu w trybie do zapisu. Informacja ta przedstawia potencjalnych partnerów replikacji, z których mogą pochodzić informacje o zmianach w ramach danej partycji katalogu.

Informacja ta przechowywana jest w ramach *up-to-dateness vector*.

Informacja o wartościach *InvocationID* dla baz danych utrzymujących informacje o danej partycji katalogu w trybie *read-only*, czyli GC lub RODC, nie jest wymagana, ponieważ instancje te nie są źródłem uaktualnień do obiektów i atrybutów.

## repsFrom

Atrybut *repsFrom* jest atrybutem, który może być przechowywany dla każdej z partycji katalogu. Atrybut ten zawiera na kontrolerze domeny będącym celem (*destination*) replikacji informacje o źródłowych partnerach replikacji. Dla każdego z partnerów replikacji, atrybut ten zawiera wpis zawierający następujące dane:

Klasa obiektu	Opis
naDSA	Adres sieciowy źródłowej repliki danych
uuidDSA	DSA GUID źródłowej repliki danych
Options	Wartość zawierająca flagę bitową, której poszczególne wartości odpowiadają wartościami parametrów DRS_OPTIONS ( <a href="http://msdn.microsoft.com/en-us/library/cc228477%28v=PROT.13%29.aspx">http://msdn.microsoft.com/en-us/library/cc228477%28v=PROT.13%29.aspx</a> ): <ul style="list-style-type: none"><li>■ DRS_WRIT_REP (0x00000010): replika w trybie do zapisu</li><li>■ DRS_INIT_SYNC (0x00000020): w celu inicializacji lokalnej kopii repliki wymagana jest replikacja z tym partnerem replikacji</li><li>■ DRS_PER_SYNC (0x00000040): replikacja wykonywana jest okresowo zgodnie z harmonogramem replikacji danych</li><li>■ DRS_MAIL_REP (0x00000080): replikacja wykonywana jest z użyciem protokołu SMTP</li><li>■ DRS_DISABLE_AUTO_SYNC (0x04000000): dla danego partnera replikacji wyłączona jest opcja</li></ul>

---

	replikacji na podstawie powiadomień o zmianach
■	DRS_DISABLE_PERIODIC_SYNC (0x08000000): dla danego partnera replikacji wyłączona jest replikacja oparta o harmonogram
■	DRS_USE_COMPRESSION (0x10000000): w ramach połączenia replikacji używana jest kompresja danych
■	DRS_TWOWAY_SYNC (0x00000200): replikacja wykonywana jest w ramach połączenia przez obie strony
<b>Schedule</b>	Harmonogram replikacji
<b>uuidInvocationID</b>	Wartość invocationID dla danej repliki katalogu
<b>usnVec</b>	Struktura zawierająca informację o numerach USN zreplikowanych od danego partnera replikacji
<b>uuidTransport</b>	Identyfikator GUID odpowiadający obiektywu, reprezentującemu metodę transportu używaną w ramach połączenia
<b>consecutiveFailures</b>	Liczba następujących po sobie niepowodzeń przy próbie połączenia i replikacji danych
<b>timeLastSuccess</b>	Data i czas ostatniego, udanego połączenia replikacji
<b>timeLastAttempt</b>	Data i czas ostatniej podjętej próby replikacji
<b>resultLastAttempt</b>	Rezultat ostatniej próby replikacji
<b>pasData</b>	Lista atrybutów, wchodzących w skład PAS które były replikowane w ramach połączenia replikacji.

---

## repsTo

Atrybut repsFrom jest atrybutem, który może być przechowywany dla każdej z partycji katalogu. Atrybut ten zawiera na kontrolerze domeny będącym źródłem (*source*) replikacji informacje o docelowych partnerach replikacji. Dla każdego z partnerów replikacji, atrybut ten zawiera wpis zawierający następujące dane:

---

Klasa obiektu	Opis
<b>naDSA</b>	Adres sieciowy źródłowej repliki danych
<b>uuidDSA</b>	DSA GUID źródłowej repliki danych
<b>Options</b>	Wartość zawierającą flagę bitową, której poszczególne wartości odpowiadają wartościami parametrów DRS_OPTIONS ( <a href="http://msdn.microsoft.com/en-us/library/cc228477%28v=PROT.13%29.aspx">http://msdn.microsoft.com/en-us/library/cc228477%28v=PROT.13%29.aspx</a> ):
	■ DRS_WRIT_REP (0x00000010): replika w trybie do zapisu
<b>consecutiveFailures</b>	Liczba następujących po sobie niepowodzeń przy próbie połączenia i replikacji danych
<b>timeLastSuccess</b>	Data i czas ostatniego, udanego połączenia replikacji
<b>timeLastAttempt</b>	Data i czas ostatniej podjętej próby replikacji
<b>resultLastAttempt</b>	Rezultat ostatniej próby replikacji

---

## Rodzaje uaktualnień

W ramach zmian zdefiniowanych jako operacje na katalogu LDAP występują następujące typy uaktualnień:

- Dodanie obiektu
- Modyfikacja atrybutów obiektu (*add, delete, replace*)
- Przeniesienie obiektu
- Usunięcie obiektu.

W ramach replikacji danych pomiędzy kontrolerami domeny występują dwa typy uaktualnień:

- Originating update
- Replicating update

### Originating update

Zmiana w katalogu wykonywana na danym kontrolerze domeny w lokalnej bazie danych to zmiana określana jako *originating update*. Originating update to zmiana w bazie danych, która została wykonana i została zakończona sukcesem (*commit*) na lokalnej bazie danych w ramach repliki katalogu.

W ramach katalogu Active Directory występują następujące typy uaktualnień w ramach *originating update*:

Operacja	Opis
Add	Operacja dodania nowego obiektu z unikalną wartością <i>objectGUID</i> . W ramach operacji Add dla wszystkich atrybutów obiektu parametr <i>version</i> ustawiany jest na wartość 1.
Modify	<p>W ramach operacji Modify aktualna wartość atrybutu zastępowana jest przez inną wartość.</p> <p>W przypadku, gdy wartość atrybutu jest usuwana, jest ona zastępowana przez wartość NULL. Wartość NULL nie powoduje przechowywania danych w bazie danych, jednak posiada przypisane atrybuty metadanych replikacji.</p> <p>W przypadku, gdy wartość atrybutu jest dodawana do atrybutu wielowartościowego, mechanizmy katalogu porównują wartości w ramach atrybutu i wynikiem operacji jest aktualna wartość atrybutu + nowa wartość.</p> <p>W przypadku, gdy dla operacji typu Modify nowa wartość odpowiada poprzedniej wartości operacji jest anulowana.</p> <p>W wyniku operacji Modify wartość atrybutu <i>version</i> w metadanych zwiększana jest o 1. W przypadku nowych atrybutów podstawowa wartość <i>version</i> to 0, w związku z tym każdy nowy atrybut będzie posiadał wartość <i>version</i> wynoszącą 1.</p>
Move	Operacja przeniesienia obiektu odbywa się jako operacja zmiany atrybutu <i>name</i> zgodnie z zasadami jak dla operacji <i>Modify</i> .
Delete	Operacja usunięcia obiektu powodująca uaktualnienie atrybutu <i>isDeleted</i> oraz <i>isRecycled</i> (w przypadku Windows 2008 R2) oraz usunięcie atrybutów obiektu i przejście obiektu w stan obiektu nagrobkowego. Usunięty

---

obiekt przenoszony jest do kontenera *Deleted objects*. Zachowanie w tym wypadku różni się dla katalogu działającego w oparciu o Windows 2008 R2 z włączoną opcją *Recycle bin*

---

## Replicating update

Replicating update jest to zmiana w ramach katalogu, wykonywana w lokalnej instancji bazy danych na podstawie informacji replikowanych od partnera replikacji. Zmiana ta nie została zainicjowana w ramach lokalnej instancji bazy danych.

## Mechanika replikacji danych katalogu

### USN i metadane obiektu

**Update Sequence Number (USN)** to lokalny i niezależny dla każdego z kontrolerów domeny, 64-bitowy licznik określający sekwencyjnie numer zmiany wprowadzanej do bazy danych w ramach lokalnej repliki katalogu. Licznik ten jest zwiększany przy każdej transakcji zmiany do katalogu, która zakończyła się powodzeniem. USN zwiększany jest zarówno w przypadku uaktualnienia *originating* jak i *replicated* zapisywanej w lokalnej bazie danych katalogu.

W przypadku, gdy transakcja zapisu danych nie zostanie zakończona sukcesem numer USN nie jest zwiększany.

Numery USN używane są pomiędzy kontrolerami domeny jako uniwersalny znacznik, pozwalający na określenie zmian, które muszą zostać zreplikowane pomiędzy kontrolerami domeny.

Wartości USN w momencie utworzenia lub zmiany obiektu jak i modyfikacji atrybutów przechowywane są wraz z każdym obiektem w ramach *metadanych* replikacji.

Z każdym z obiektów w ramach katalogu Active Directory powiązane są dwa atrybuty przechowujące wartości USN:

Atrybut	Opis
<b>uSNCreated</b>	Atrybut przechowujący lokalną wartość USN w chwili, gdy obiekt został utworzony.
<b>uSNChanged</b>	Atrybut przechowujący wartość USN w chwili dokonania ostatniej zmiany w ramach obiektu. Zmiany do atrybutów niepodlegających replikacji nie powodują uaktualnienia wartości w ramach tego atrybutu. Wartość tego atrybutu powinna odpowiadać najwyższej wartości USN dla numeru zmian w ramach atrybutu obiektu.

Dodatkowo, dla każdego z atrybutów obiektu przechowywane są następujące wartości USN:

Atrybut	Opis
<b>Originating USN</b>	Wartość USN w chwili wykonywania zmiany ( <i>originating update</i> ) na kontrolerze domeny, na którym wykonana została zmiana
<b>Local USN</b>	Lokalna wartość USN w chwili wykonywania zmiany na kontrolerze domeny. W przypadku <i>originating update</i> wartość <i>Originating USN</i> i <i>Local USN</i> jest identyczna. W przypadku <i>replicated update</i> jest to lokalna wartość USN w chwili zapisu replikowanej zmiany.

Wraz z wartościami USN w chwili wykonywania zmiany, w ramach opisu atrybutu przechowywane są dodatkowo następujące informacje:

Atrybut	Opis
Version number	32-bitowy numer opisujący wersję atrybutu. Początkowa wartość tego atrybutu to 1. Jest ona zwiększana o 1 w przypadku każdej zmiany ( <i>originating update</i> ) wykonywanej na obiekcie. Wersja atrybutu nie zmienia się w przypadku replikacji zmiany.  Wersja atrybutu jest w odróżnieniu od wartości USN globalna i replikowana pomiędzy kontrolerami domeny w ramach metadanych atrybutu.  Wersja atrybutu (z wykluczeniem kolizji) odpowiada liczbie zmian wykonywanych na wartości atrybutu.
Timestamp	62-bitowy znacznik czasu (UTC) odpowiadający czasowi zmiany atrybutu.
Originating Domain controller	DA GUID kontrolera domeny, na którym wykonana została ostatnia zmiana atrybutu ( <i>originating update</i> ).

Wartości atrybutu *Local USN* są przechowywane lokalnie, na danym kontrolerze domeny i nie są replikowane pomiędzy kontrolerami domeny. Pozostałe wartości atrybutów:

- Originating USN
- Version number
- Timestamp
- Originating Domain Controller

składają się na opis atrybutu, który replikowany jest wraz ze zmianami w atrybucie w ramach metadanych replikacji.

## Metadane replikacji

Atrybuty opisujące zmiany, przekazywane wraz z każdym obiektem tworzą metadane replikacji tego obiektu. Metadane te, przechowywane są w formie binarnej w atrybucie **repIPropertyMetaData** każdego obiektu. Informacje zawarte w metadanych replikacji pozwalają na stwierdzenie kiedy i gdzie nastąpiła zmiana wartości atrybutu.

Zawartość metadanych w ramach tego atrybutu dodaje około 48 bajtów dodatkowej przestrzeni na dysku wymaganej do składowania danych katalogu na dysku, dla każdego atrybutu obiektu.

W ramach replikacji danych, dla każdej własności atrybutu metadane replikacji dodają 40 bajtów do przesłania pomiędzy partnerami replikacji. Wartość ta jest mniejsza niż ilość danych składowanych na dysku ponieważ wartość Local USN nie jest replikowana pomiędzy kontrolerami domeny.

W systemie Windows Server 2003 dodany został dodatkowy atrybut **msds-ReplAttributeMetaData**, zawierający metadane replikacji atrybutu w postaci XML. Dodatkowy atrybut **msds-ReplValueMetaData** opisują metadane replikacji dla każdej wartości atrybutu wielowartościowego jeżeli replikowany jest on z użyciem mechanizmu LVR.

Metadane replikacji dla danego obiektu można odczytać używając systemowego narzędzia REPADMIN.EXE z następującą składnią:

```
repadmin /SHOWMETA <DN obiektu> <FQDN kontrolera domeny>
```

# PROCES REPLIKACJI DANYCH

## Replikacja danych z użyciem USN

Proces replikacji danych pomiędzy kontrolerami domeny opiera się na określeniu zmian ostatnio zreplikowanych od danego partnera replikacji i pobrania danych, które nie zostały jeszcze zreplikowane. W celu określenia zmian wymaganych do replikacji kontrolery domeny posługują się numerami USN.

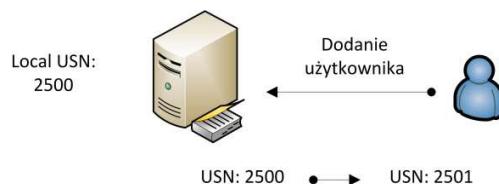
Numerы USN są utrzymywane lokalnie w ramach każdego kontrolera domeny, w ramach metadanych replikacji przekazywana jest wraz z atrybutami informacja o USN ostatniej zmiany aktualizującej dany atrybut i kontrolerze domeny który ją wykonał.

W celu zobrazowania procesu replikacji danych przedstawiony zostanie proces replikacji zmiany w katalogu pomiędzy dwoma kontrolerami domeny – DC1 i DC2, na przykładzie utworzenia nowego obiektu oraz zmian jego atrybutu.

### 1. Utworzenie nowego użytkownika na DC1

Wynik operacji z punktu widzenia metadanych replikacji obiektu na DC1:

- Lokalna wartość USN na DC1 przed operacją: 2500
- Dodanie obiektu i jego atrybutów to pojedyncza transakcja. Lokalny USN zwiększony o 1: 2501.
- Local USN oraz Originating USN dla nowego obiektu to 2501.
- Wersja atrybutu to 1 (nowy obiekt).
- Jeden znacznik czasu ze względu na pojedynczą transakcję



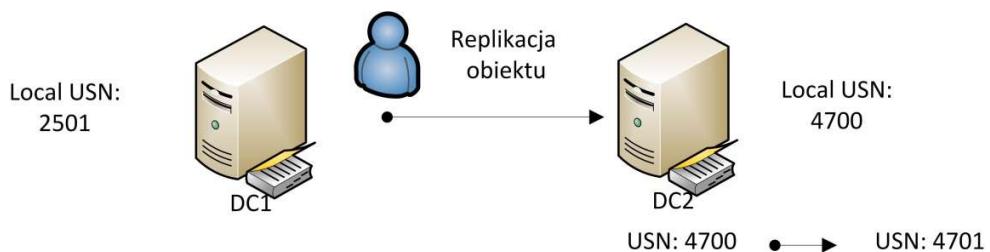
usnCreated = 2501				usnChanged = 2501		
Atrybut	Wartość	Local USN	Version	Timestamp	Originating DSA	OriginatingUSN
Cn	Jan.nowak	2501	1	2010-09-01 11:05:31	<DC1 GUID>	2501
userPassword	P@ssw0rd	2501	1	2010-09-01 11:05:31	<DC1 GUID>	2501
Sn	Nowak	2501	1	2010-09-01 11:05:31	<DC1 GUID>	2501
GivenName	Jan	2501	1	2010-09-01 11:05:31	<DC1 GUID>	2501

SamAccountname	Jnowak	2501	1	2010-09-01 11:05:31	<DC1 GUID>	2501
userPrincipaName	jnowak@w2k.pl	2501	1	2010-09-01 11:05:31	<DC1 GUID>	2501

## 2. Replikacja nowego obiektu pomiędzy DC1 i DC2

Wynik operacji z punktu widzenia metadanych replikacji obiektu na DC2:

- Lokalna wartość USN dla DC 2 przed operacją: 4700
- Dodanie obiektu i jego atrybutów to pojedyncza transakcja. Lokalny USN zwiększyły się o 1: 4701.
- Local USN dla operacji: 4701
- Originating USN dla operacji: 2501 (USN dla operacji na DC1)
- Wersja atrybutu to 1 (nowy obiekt).
- Znacznik czasu bez zmian (czas originating update)
- Originating DSA bez zmian (replicating update)



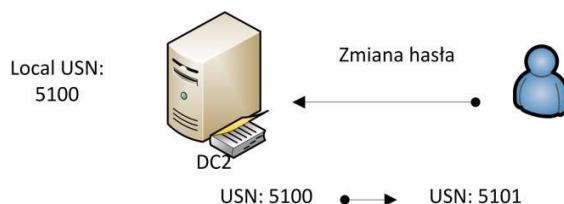
usnCreated = 4701				usnChanged = 4701		
Atrybut	Wartość	Local USN	Version	Timestamp	Originating DSA	OriginatingUSN
Cn	Jan.nowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
userPassword	P@ssw0rd	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
Sn	Nowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
GivenName	Jan	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
SamAccountname	Jnowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
userPrincipaName	jnowak@w2k.pl	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501

## 3. Zmiana atrybutu obiektu na DC2

Wynik operacji z punktu widzenia metadanych replikacji obiektu na DC2:

- Lokalna wartość USN dla DC 2 przed operacją: 5100
- Zmiana hasła użytkownika, aktualizacja jednego atrybutu. Lokalny USN zwiększyły się o 1: 5101.

- Local USN dla operacji: 5010
- Originating USN dla operacji: 5101 (USN dla operacji na DC2)
- Wersja atrybutu to 2.
- Znacznik czasu lokalny dla DC2 w chwili operacji (czas originating update)
- Originating DSA dla atrybutu hasła to DC2 (originating update)

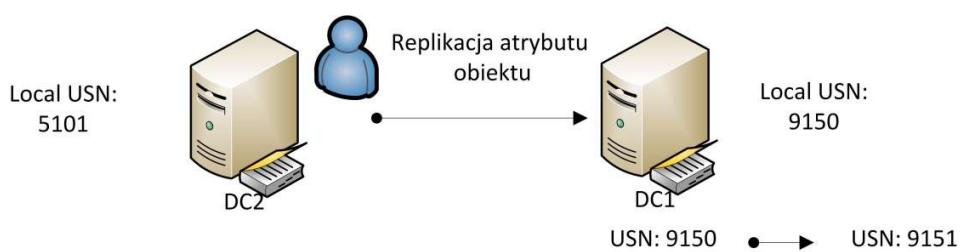


usnCreated = 4701			usnChanged = 5101			
Atrybut	Wartość	Local USN	Version	Timestamp	Originating DSA	OriginatingUSN
Cn	Jan.nowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
<b>userPassword</b>	<b>SecR#%\$%</b>	<b>5101</b>	<b>2</b>	<b>2010-09-01 13:23:11</b>	<b>&lt;DC2 GUID&gt;</b>	<b>5101</b>
Sn	Nowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
GivenName	Jan	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
SamAccountname	Jnowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
userPrincipalName	jnowak@w2k.pl	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501

#### 4. Replikacja zmiana atrybutu obiektu z DC2 do DC1

Wynik operacji z punktu widzenia metadanych replikacji obiektu na DC1:

- Lokalna wartość USN dla DC 1 przed operacją: 9150
- Zmiana hasła użytkownika, uaktualnienie jednego atrybutu. Lokalny USN zwiększyły się o 1: 9151.
- Local USN dla operacji: 9151
- Originating USN dla operacji: 5101 (USN dla operacji na DC2)
- Wersja atrybutu to 2.
- Znacznik czasu lokalny dla DC2 w chwili operacji (czas originating update)
- Originating DSA dla atrybutu hasła to DC2 (originating update)



usnCreated = 2501			usnChanged = 9151			
Atrybut	Wartość	Local USN	Version	Timestamp	Originating DSA	OriginatingUSN
Cn	Jan.nowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
<b>userPassword</b>	<b>SecR#t\$%</b>	<b>9151</b>	<b>2</b>	<b>2010-09-01 13:23:11</b>	<b>&lt;DC2 GUID&gt;</b>	<b>5101</b>
Sn	Nowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
GivName	Jan	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
SamAccountname	Jnowak	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501
userPrincipaName	jnowak@w2k.pl	4701	1	2010-09-01 11:05:31	<DC1 GUID>	2501

### Highest Committed USN

W ramach każdego kontrolera domeny obiekt *rootDSE* danego kontrolera domeny posiada atrybut o nazwie *highestCommittedUSN*. Atrybut ten zawiera najwyższy numer USN, który został użyty w ramach danego kontrolera domeny. Wartość tego atrybutu jest lokalna, dla danego kontrolera domeny.

## High-watermark vector

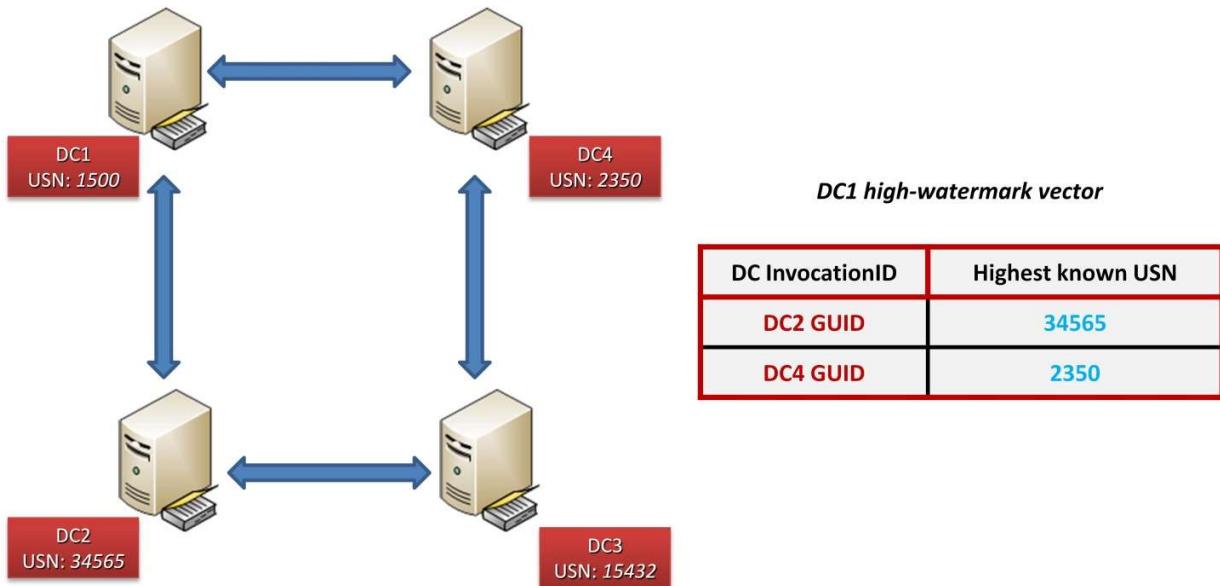
W celu replikacji danych z partnerami replikacji, dany kontroler domeny musi posiadać wiedzę o ostatniej wartości zreplikowanego numeru USN dla danego partnera replikacji. Przy następnej próbie replikacji dany partner replikacji prosi o zmiany o numerze wyższym, niż ostatni zreplikowany od danego partnera replikacji.

W celu przechowywania tej informacji każdy z kontrolerów domeny utrzymuje lokalną tablicę **high-watermark vector**.

*High-watermark vector* zawiera informację o najwyższy, zreplikowanym numerze USN dla każdego partnera replikacji, a w ramach połączenia z partnerem dla każdej replikowanej partycji katalogu.

Tablica ta przechowywana jest w ramach atrybutu *repsFrom* dla każdej partycji utrzymywanej w ramach danej repliki katalogu.

W ramach tablicy przechowywany jest najwyższy zreplikowany numer USN wraz z identyfikatorem **Invocation ID** źródłowej bazy danych.



Docelowy kontroler domeny, po powiadomieniu o istnieniu zmian przez źródłowy kontroler domeny wysyła w odpowiedzi wartość USN z tablicy *high-watermark vector* dla danej partycji katalogu i danej repliki katalogu.

W ramach odpowiedzi na powiadomienie o zmianach, docelowy kontroler domeny wysyła do kontrolera źródłowego również następujące informacje:

- Nazwę partycji katalogu, której dotyczy żądanie replikacji
- Maksymalną liczbę obiektów, które mogą być zreplikowane w ramach sesji
- Maksymalną liczbę wartości atrybutów, które mogą być zreplikowane w ramach sesji
- Zawartość lokalnego *Up-to-Dateness vector*

Źródłowy kontroler domeny używa wartości USN zawartego w tej tablicy do wyfiltrowania zmian wysyłanych w odpowiedzi na żądanie replikacji danych.

Zmiany wysyłane są do docelowego kontrolera domeny w kolejności zmian określonej przez kolejność wartości USN. W odpowiedzi źródłowy kontroler domeny przesyła następujące informacje:

- DSA GUID kontrolera domeny
- Invocation ID instancji bazy danych
- Liczbę obiektów dla których istnieją zmiany wraz z wartością objectGUID dla danego obiektu oraz listę zmian na atrybutach obiektów.
- Najwyższą wartość usnChanged. Wartość ta jest używana przez docelowy DC do uaktualnienia wartości w *high-watermark vector*.
- Znacznik, wskazujący czy liczba zmian przekroczyła maksymalną ilość ustaloną przez docelowy DC i nadal pozostają dane do replikacji.
- W przypadku, gdy wszystkie dane zostały zreplikowane i nie pozostaje więcej danych – zawartość lokalnego *up-to-dateness vector*.

Zawartość lokalnej tablicy *high-watermark vector* dla lokalnej instancji katalogu można wyświetlić używając polecenia:

```
repadmin /SHOWREPL /VERBOSE
```

## Up-to-dateness vector

### Zawartość up-to-dateness vector

Tablica **up-to-dateness vector (UTD)** jest lokalną tablicą utrzymywana w ramach każdego z kontrolerów domeny, dla każdej z partycji katalogu. Partycja ta przechowywana jest w atrybutie `replUpToDateVector` obiektu partycji katalogu. Atrybut ten nie jest replikowany w ramach replikacji danych katalogu.

Tablica ta utrzymywana jest w celu ograniczenia redundantnej replikacji danych pomiędzy kontrolerami domeny. W ramach tablicy UTD lokalny kontroler domeny przechowuje informację o wszystkich kontrolerach domeny w ramach lasu wraz z najwyższym numerem USN dla *originating update* dla danego kontrolera domeny. Tablica UTD zawiera wpisy dotyczące nie tylko bezpośrednich partnerów replikacji, lecz wszystkich kontrolerów domeny, dla których zreplikowana została zmiana pochodząca z danego kontrolera domeny.

Tablica UTD zawiera również informację o usuniętych kontrolerach domeny, które brały udział w replikacji danych.

Począwszy od Windows 2003 tablica UTD zawiera również znacznik czasowy, który zawiera czas zakończenia ostatniego, pełnego cyklu replikacji uwzględniającego dany źródłowy kontroler domeny. W tym wypadku cykl replikacji oznacza bezpośrednią lub pośrednią (przez inne kontrolery domeny) replikację danych, dla których uaktualnienie (*originating update*) pochodzi z danego kontrolera domeny. Znacznik czasowy zawiera lokalny czas dla danego kontrolera domeny (*destination*).

Zawartość lokalnej tablicy *up-to-dateness vector* dla lokalnej instancji katalogu można wyświetlić używając polecenia:

```
repadmin /SHOWUTDVECT
```

Zawartość tablicy UTD prezentowana jest również w ramach konstruowanego atrybutu **msDS-NCRPICursors**. Atrybut ten dostępny jest od wersji Windows Server 2003.

### Rola up-to-dateness vector w procesie replikacji

Rolą tablicy UTD jest wyeliminowanie z procesu replikacji pomiędzy dwoma partnerami replikacji zmian, które zostały już zreplikowane do danego kontrolera domeny z użyciem innej ścieżki replikacji danych.

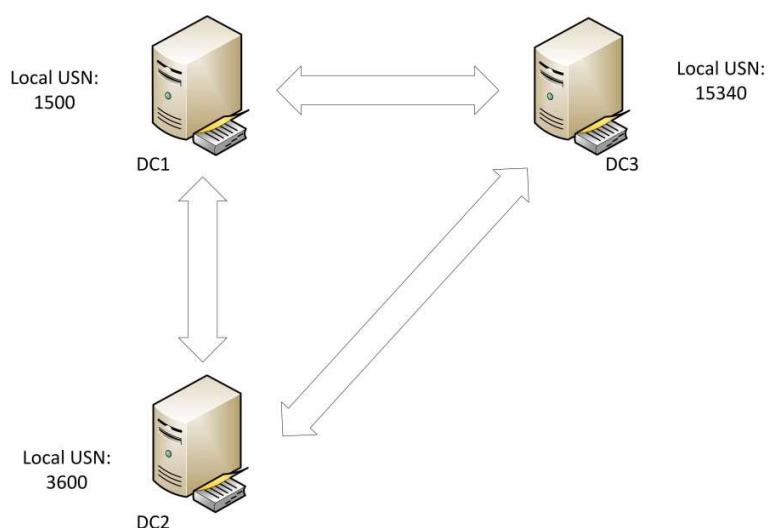
Znaczniki USN w ramach tablicy UTD zawierają najwyższe numery USN dla *originating updates* dla każdego kontrolera domeny. Tablica ta nie jest uaktualniana numerami USN dla uaktualnień replikowanych przez danego kontrolera domeny (*replicating update*). W związku z tym, tabela ta zawiera

informacje o najwyższych numerach nowych zmian zreplikowanych dla każdego z kontrolerów domeny, bez znaczenia czy zmiana ta została zreplikowana bezpośrednio czy też pośrednio, przez replikację z innym kontrolerem domeny.

Wektor UTD zapobiega również niekończącej się replikacji danych w ramach katalogu poprzez kolejne replikowane aktualnienia.

W celu przedstawienia roli wektora UTD w procesie replikacji prześledzony zostanie proces replikacji zmian pomiędzy trzema kontrolerami domeny – DC1, DC2 i DC3 będącymi partnerami replikacji.

Stan początkowy przedstawiony został na poniższym rysunku:



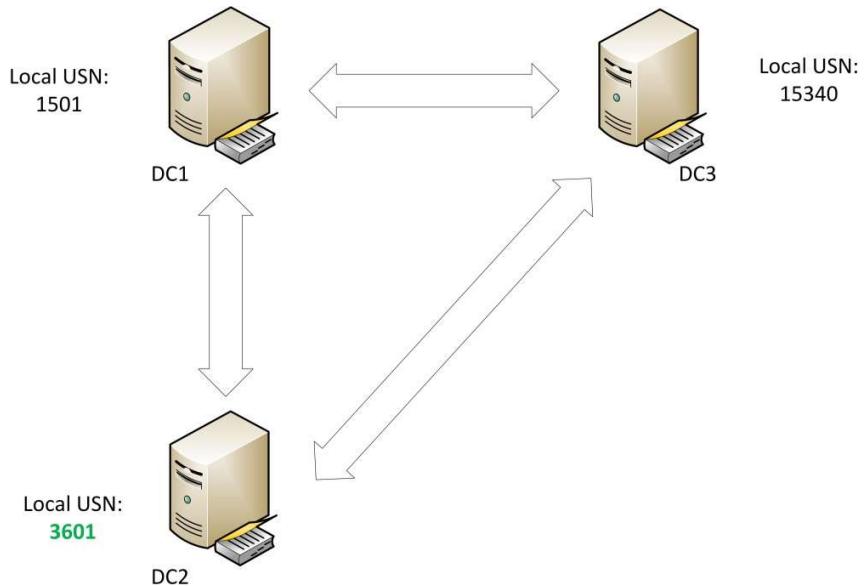
Kontrolery w ramach topologii replikacji znajdują się w stanie ustalonym. W sytuacji początkowej dla DC1 tablice *high-watermark vector* oraz wektor UDT przedstawiają się następująco:

DC	High watermark vector	Wektor UTD
DC2	3600	2590
DC3	15340	15340

W sytuacji takiej oznacza to, że DC1 zareplikował wszystkie zmiany od partnerów replikacji, a ostatnia zmiana wprowadzająca modyfikację (*originating update*) z DC2 miała USN 2950 a z DC3 miała USN 15340.

Na DC2 wprowadzona zostaje zmiana, powodując zwiększenie lokalnego USN do 3601 i jest to zmiana modyfikująca atrybut w lokalnej bazie danych (*originating update*) po powiadomieniu DC1 i replikacji

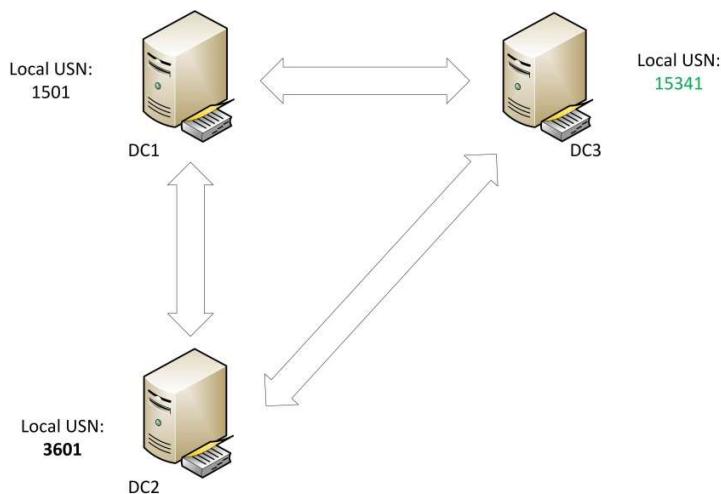
danych z DC1 stan lokalnych USN i tablic *high-watermark vector* oraz UTD dla DC1 przedstawia się następująco:



Kontroler domeny DC1 zapisuje w ramach tablicy *high-watermark vector* ostatni numer USN zreplikowany z kontrolera DC 2 czyli 3601, równocześnie uaktualniając również wartość wektora UTD dla DC2 tą samą wartością, ponieważ replikowana zmiana pochodziła z DC2.

DC	High watermark vector	Wektor UTD
DC2	3601	3601
DC3	15340	15340

W kolejnym kroku replikacji, zmiana atrybutu z DC2 replikowana jest do kontrolera DC3, powodując zwiększenie lokalnego numeru USN na kontrolerze DC3 do wartości 15341. Stan USN na wszystkich kontrolerach domeny oraz wartości tablic *high-watermark vector* oraz UTD dla DC1 przedstawione są poniżej.



Replikacja danych pomiędzy DC2 i DC3 nie powoduje zmiany wartości w tablicach na kontrolerze DC1.

DC	High watermark vector	Wektor UTD
DC2	3601	3601
DC3	15340	15340

W kolejnym kroku replikacji, następuje replikacja danych pomiędzy kontrolerami DC1 i DC3. Ponieważ ostatni znany USN dla DC3 w lokalnej tablicy *high-watermark vector* kontrolera DC1 to 15340 to kontroler ten prosi o przesłanie zmian o USN > 15340. Dodatkowo, jako część żądania replikacji wysyła do DC3 własną tablicę UTD.

Kontroler domeny DC3 stwierdza, że posiada zmiany o USN większym niż 15340, jednakże używając zawartości tablicy UTD kontrolera DC1 stwierdza, że kontroler ten zareplikował już zmianę o *Originating USN* 3601, pochodzącą z DC2. W związku z tym odfiltrowuje tą zmianę i kończy replikację, ponieważ w chwili obecnej nie ma żadnych dodatkowych atrybutów do replikacji.

W ten sposób zawartość tablicy UTD pozwoliła na stwierdzenie, że dany kontroler domeny wie już o tej zmianie i usunęła potrzebę dodatkowej replikacji pomiędzy kontrolerami domeny.

Kontrolery domeny wymieniają się zawartością tablicy UTD w ramach każdego połączenia replikacji, i każdy z nich używa otrzymanych wartości tabeli UTD do uaktualnienia swojej własnej kopii tej tablicy. Dzięki temu, nawet w przypadku gdy kontrolery domeny nie replikują się bezpośrednio w ramach połączeń topologii replikacji, wektor UTD danego kontrolera domeny może zostać uaktualniony tak, aby stwierdzał, które zmiany pochodzące z których kontrolerów domeny zostały już zreplikowane do lokalnej bazy danych.

## Atrybuty wielowartościowe

### Atrybuty niepołączone

Atrybuty wielowartościowe, niebędące atrybutami połączonymi są to atrybuty, zawierające wiele wartości określonego typu - na przykład łańcuchów znakowych.

Liczba wartości atrybutów możliwych do umieszczenia w ramach pojedynczego obiektu usługi katalogowej limitowana jest przez rozmiar strony bazy danych ESE – 8 KB.

Ograniczenie to dotyczy również atrybutów przechowujących dane w formacie DN, które nie zostały zdefiniowane jako atrybuty połączone.

### Linked attributes

Informacje o obiektach w bazie danych usługi katalogowej przechowywane są w dwóch podstawowych tabelach: tabeli obiektów i tabeli połączeń (*link table*). Każdy obiekt istniejący w bazie danych usługi katalogowej posiada wpis w tabeli obiektów, którego identyfikatorem jest pole DNT (*Distinguished Name Tag*). Tabela połączeń pomiędzy obiektami zawiera informacje o relacjach pomiędzy obiektami wyrażone poprzez DNT. DNT tłumaczone są następnie na poziomie usługi katalogowej na odpowiednie wartości *distinguished name* (DN).

Na poziomie katalogu LDAP relacje pomiędzy obiektami wyrażone są wartościami DN poprzez atrybuty połączone (*linked attributes*).

Schemat usługi katalogowej pozwala na zdefiniowanie atrybutów połączonych (*linked attributes*). Atrybuty połączone są to pary atrybutów, identyfikowane przez wartość atrybutu *LinkID* każdego z nich, dla których system wylicza wartość jednego z nich (*back-link*) na postawie wartości drugiego (*forward link*).

Definicja atrybutów tylko *linked attributes* możliwa jest jedynie dla atrybutów przechowujących dane typu *distinguished name*.

**Forward link** jest to atrybut, do którego fizycznie zapisywane są wartości danych na poziomie obiektu katalogu. Atrybut ten identyfikowany jest przez parzystą wartość *LinkID* w ramach swojej definicji w schemacie usługi katalogowej. W atrybucie tego typu przechowywane są fizyczne wartości, wskazujące poprzez *distinguished Name* na inne obiekty w ramach katalogu.

**Back link** jest to atrybut powiązany w parze z *forward link* poprzez nieparzystą wartość *LinkID* wyliczaną jako „*LinkID forward link +1*”. Wartość tego atrybutu wyliczana jest dynamicznie przez system na podstawie wartości atrybutu będącego *forward link* w danej parze atrybutów.

Najczęściej rozpoznawaną w ramach Active Directory parą atrybutów połączonych jest *member* (*linkID:2*) i *memberof* (*linkID:3*) używane do wyrażenia członkostwa obiektów w ramach grupy usługi katalogowej. Fizyczne członkostwo w grupie wyrażane jest w tym przypadku poprzez wartości atrybutu *member* na obiekcie grupy.

Informacje o powiązaniach pomiędzy obiektami w ramach usługi katalogowej wyrażone poprzez definicje atrybutów powiązanych przechowywane są fizycznie w bazie danych katalogu w osobnej

tabeli danych. Dzięki temu informacje o tych atrybutach nie są wliczane do ogólnego ograniczenia liczby wartości na obiekcie katalogu.

## Replikacja atrybutów wielowartościowych, połączonych i niepołączonych

W przypadku replikacji informacji o atrybutach niepołączonych, lub atrybutach połączonych w Windows 2000 replikowana zawsze jest pełna wartość atrybutu. W przypadku zmiany jednej wartości, pomiędzy kontrolerami domeny biorącymi udział w replikacji danych zawsze replikowana była pełna informacja o wartościach atrybutu.

W Windows 2003 wprowadzony został nowy tryb replikacji – Linked Value Replication (LVR). Wprowadzenie LVR powoduje, że każdy z atrybutów replikowany jest jako osobna wartość i do każdego z nich dołączone są metadane replikacji. Dzięki temu, w przypadku zmiany w ramach atrybutu wielowartościowego, takiego jak *member*, mechanizm replikacji usługi katalogowej replikuje pomiędzy poszczególnymi kontrolerami jedynie informacje o zmienionych wartościach.

W przypadku modyfikacji danych w wielowartościowym atrybucie, niebędącym atrybutem połączonym, wszystkie zmiany w ramach modyfikacji otrzymują taki sam lokalny numer USN ponieważ wykonywane są w ramach pojedynczej transakcji bazy danych.

W przypadku modyfikacji wartości atrybutu wielowartościowego, będącego atrybutem połączonym w środowisku umożliwiającym korzystanie z LVR, każda ze zmian do wartości atrybutu wykonywana jest w ramach osobnej transakcji, dzięki czemu, każda ze zmian do wartości atrybutu posiada przypisany unikalny numer USN.

W przypadku replikacji zmian pomiędzy kontrolerami domeny, zmiany do atrybutów niebędących atrybutami połączonymi replikowane są wcześniej, niż zmiany do atrybutów będących atrybutami połączonymi.

Dodatkowo, pomimo że zmiany do atrybutów zdefiniowanych jako połączone, replikowane są w kolejności zmian określonej przez wartości USN, nie jest gwarantowane, że zmiany te będą zapisane w docelowej bazie danych w takiej samej kolejności transakcji. Ponieważ do zapisu operacji na atrybucie połączonym wymagane jest zapewnianie istnienia w bazie danych obiektu do którego odnosi się wartość atrybutu, możliwe jest że zapis transakcji do bazy danych nastąpi w innej kolejności niż replikacja poszczególnych wartości atrybutu. W wyniku tego, lokalne USN w docelowej bazie danych mogą się różnić kolejnością od źródłowych USN dla atrybutu.

Wcześniejsza replikacji danych o atrybutach niebędących atrybutami połączonymi realizowana jest poprzez podniesienie priorytetu replikacji dla zmian na tych atrybutach, względem zmian dla atrybutów połączonych.

Ze względu na kolejność replikacji atrybutów, zapis transakcji w bazie danych dla atrybutów niebędących atrybutami połączonymi może nastąpić wcześniej, niż dla atrybutów zdefiniowanych jako atrybuty połączone.

## Atrybuty wielowartościowe i limit wielkości transakcji

W przypadku atrybutów wielowartościowych, niebędących atrybutami połączonymi lub w środowisku bez wsparcia dla LVR, zapis zmian wartości atrybutu (*originating update*) musi zostać wykonany w ramach pojedynczej transakcji w bazie danych.

Ze względu na ograniczenia rozmiaru obszaru bazy danych określonego jako *version store*, praktyczny limit wartości możliwych do zapisania w ramach pojedynczej transakcji to około 5 tysięcy wartości. W przypadku przekroczenia tej liczby zapis wszystkich wartości nie jest gwarantowany i możliwa jest utrata danych.

W przypadku środowiska korzystającego z LVR, każda zmiana do wartości atrybutu traktowana jest jako pojedyncza transakcja, co powoduje, że zmiany te nie przekraczają dopuszczalnego rozmiaru dla bufora *version store* bazy ESE.

Dodatkowo, w przypadku atrybutów wielowartościowych niebędących atrybutami połączonymi jednostką transakcji jest cała wartość atrybutu. W przypadku edycji wartości atrybutu na dwóch kontrolerach domeny równocześnie zachowana zostanie tylko ostatnia wartość zgodnie z regułami rozstrzygania konfliktów replikacji.

## Konflikty danych w ramach replikacji

Ze względu na rozproszoną naturę katalogu Active Directory i asynchroniczną replikację danych katalogu pomiędzy partnerami replikacji możliwe jest wystąpienie konfliktów danych pomiędzy zmianami wprowadzanymi na różnych kontrolerach domeny.

Usługa katalogowa stosuje regułę rozwiązywania konfliktów replikacji opartą o metadane replikacji. W rozwiązaniu konfliktu replikacji używane są informacje dotyczące wersji atrybutu, czasu zmiany atrybutu (*originating time*) i informacji o GUID DC wprowadzającego zmianę (*originating DSA GUID*).

W przypadku wystąpienia konfliktu w ramach modyfikacji obiektu stosowane są następujące reguły mające na celu rozwiązanie konfliktu:

- **Porównanie wersji atrybutu:** pierwszym krokiem rozwiązywania konfliktu w ramach replikacji jest porównanie wersji atrybutów. W przypadku różnych wersji wygrywa zmiana z wyższym numerem wersji.
- **Porównanie znacznika czasu wprowadzenia zmiany (*originating time*):** jeżeli atrybuty posiadają taką samą wersję zmiany, wygrywa zmiana wprowadzona później do katalogu.
- **Porównanie GUID DC wprowadzającego zmianę:** w przypadku, gdy zmiany posiadają ten sam znacznik czasowy wygrywa zmiana wprowadzona przez DC z większym (w wyniku sortowania) GUID.

W ramach replikacji katalogu mogą wystąpić następujące konflikty związane z replikacją danych katalogu:

Typ konfliktu	Opis	Metoda rozwiązywania konfliktu
<b>Konflikt wartości atrybutów</b>	Konflikt występuje w przypadku modyfikacji atrybutu obiektu na więcej niż jednym kontrolerze domeny, w chwili gdy zmiany są replikowane pomiędzy kontrolerami domeny.	Rozwiązywanie konfliktu w oparciu o metadane replikacji
<b>Utworzenie lub przeniesienie obiektu do nieistniejącego obiektu nadzawanego</b>	Konflikt występuje w przypadku, gdy obiekt w ramach jednego DC został utworzony lub przeniesiony do kontenera, który został skasowany w ramach innego kontrolera domeny, i zmiana ta nie została jeszcze zreplikowana.	Obiekt objęty konfliktiem na docelowym DC trafia do kontenera „LostAndFound”.
<b>Utworzenie obiektów o takich samych nazwach</b>	W ramach odrębnych replik katalogu tworzone są dwa obiekty o takich samych nazwach (CN) w ramach tego samego kontenera.	Obiekt utworzony później (na podstawie czasu utworzenia) uzyskuje dodany do swojej nazwy sufix CNF[0x00A]:<GUID obiektu>.

Podstawowym zadaniem mechanizmów rozwiązywania konfliktów w ramach replikacji katalogu jest umożliwienie wszystkim kontrolerom domeny uzyskanie spójnego stanu danych po replikacji.

## Usuwanie obiektów

Usunięcie obiektu w ramach katalogu jest specjalnym rodzajem zmiany replikowanym poprzez replikację obiektów nagrobkowych (*tombstone objects*). Replikacja obiektu nagrobkowego ma za zadanie replikację pomiędzy kontrolerami domeny informacji o usunięciu obiektu i umożliwienie usunięcie referencji do tego obiektu utrzymywanych lokalnie w ramach bazy danych każdego z kontrolerów domeny biorących udział w replikacji.

### Obiekty nagrobkowe

Obiekt nagrobkowy jest tworzony w przypadku skasowania obiektu. Obiekt nagrobkowy tworzony jest w następujący sposób:

- Atrybut *isDeleted* obiektu ustawiany jest na wartość *true*
- Wewnętrzny znacznik czasowy w atrybucie *When-Deleted* jest ustawiany na czas modyfikacji atrybutu *isDeleted*.
- CN obiektu jest zmieniane poprzez dodanie do nazwy CN obiektu sufiku w postaci *DEL[0x00A]:<GUID obiektu>*.
- Obiekt przenoszony jest do specjalnego kontenera „Deleted objects”. Kontener ten istnieje w drzewie głównym każdej z domen.
- W systemach Windows 2003 i późniejszych atrybut *lastKnownParent* jest ustawiany na lokację obiektu w chwili skasowania.
- Z obiektu usuwane są wszystkie atrybuty, oprócz tych, które oznaczone są jako zachowywane przy skasowaniu obiektu w schemacie lub bezpośrednio w kodzie systemu operacyjnego.

Obiekt w stanie nagrobka jest replikowany do poszczególnych replik katalogu, umożliwiając im skasowanie referencji do obiektu oraz samego obiektu.

Obiekt nagrobkowy żyje w ramach katalogu poprzez czas określony przez parametr *tombstoneLifeTime*. Domyślne wartości tego atrybutu dla poszczególnych wersji systemu operacyjnego przedstawione są poniżej.

Wersja OS	<i>tombstoneLifeTime</i>
Windows 2000 Server	60
Windows Server 2003	60
Windows Server 2003 SP1	180
Windows Server 2003 R2	180
Windows Server 2008	180
Windows Server 2008 R2	180

### **Tombstone Life Time w Windows 2003 R2**

W początkowej dystrybucji systemu Windows Server 2003 R2 istniał błąd w ramach pliku konfiguracyjnego schema.ini używanego do inicjalizacji wartości w ramach konfiguracji usługi katalogowej. W związku z tym, przy instalacji nowego środowiska usługi katalogowej w oparciu o Windows Server 2003 R2, w przypadku, gdy wcześniej na kontrolerze domeny zainstalowane zostały dodatkowe pliki z drugiego nośnika CD, domyślny czas życia obiektów nagrobkowych wynosił 60 dni zamiast 180 dni.

Wynika to z błędu w pliku schema.ini, w którym usunięta została linia definiująca domyślny czas życia obiektów nagrobków.

Obiekt w stanie nagrobka jest replikowany do poszczególnych replik katalogu, umożliwiając im skasowanie referencji do obiektu oraz samego obiektu.

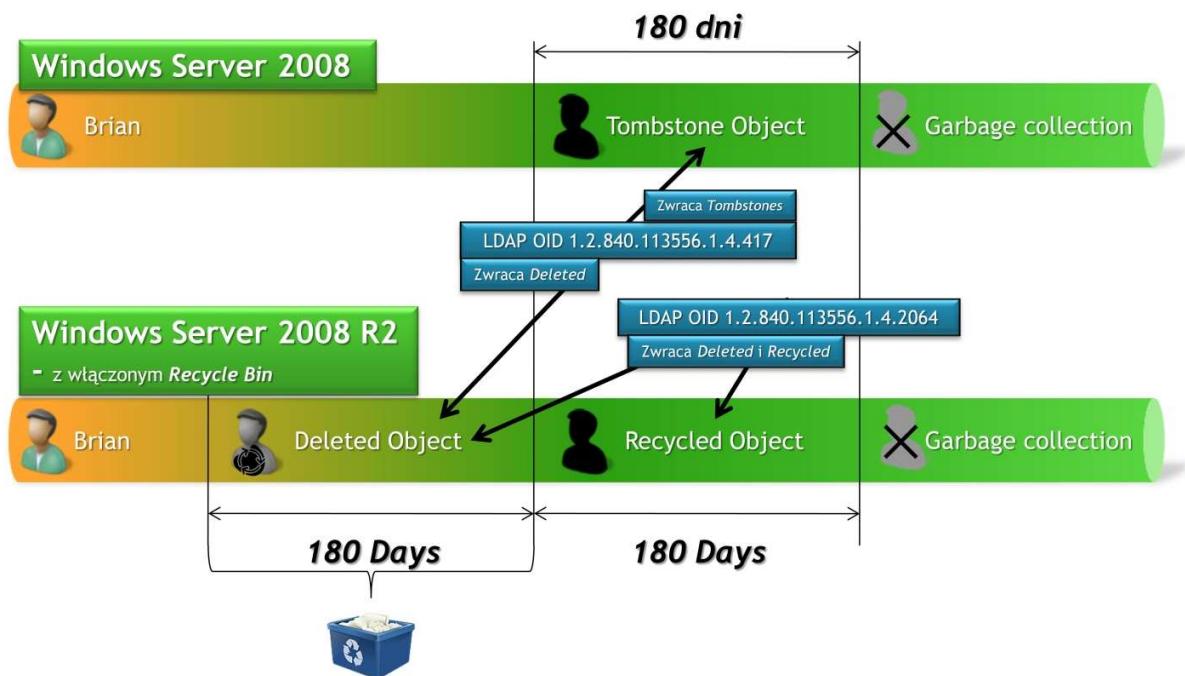
Obiekty nagrobkowe w ramach bazy danych katalogu usuwane są przez proces *Garbage Collector*. Proces ten uruchamiany jest na każdym kontrolerze domeny indywidualnie co 12 godzin.

## Funkcjonalność recycle-bin

W Windows 2008 R2 wprowadzona została nowa funkcjonalność Active Directory Recycle Bin, pozwalająca na skasowanie obiektu z zachowaniem jego wszystkich właściwości i przechowywanie w tym stanie przez określony okres czasu zanim obiekt stanie się obiektem nagrobkowym.

W przypadku włączenia funkcjonalności *Recycle Bin* operacja usunięcia obiektu przebiega w dwóch etapach:

- Obiekt w stanie *Deleted object*: czyli obiekt znajdujący się w Recycle bin z zachowaniem jego wszystkich atrybutów
- Obiekt w stanie *Recycled object (tombstone)*: czyli obiekt nagrobkowy, z usuniętymi atrybutami, istniejący w celu replikacji informacji o skasowaniu obiektu w poszczególnych replikach katalogu.



Obiekt w okresie „*Deleted object*” posiada dodatkowy atrybut *isRecycled* ustawiony na *false*, standardowy atrybut *isDeleted* ustawiony jest na *true*. Obiekt zachowuje wszystkie atrybuty.

Obiekt w okresie „*Recycled object*” posiada atrybut *isRecycled* oraz *isDeleted* ustawiony na wartość *true*. Obiekt ten przetwarzany jest zgodnie z zasadami przetwarzania obiektów nagrobkowych.

## **Informacja o usuniętych obiektach połączonych**

W przypadku usunięcia obiektu i zamiany go na obiekt typu nagrobkowego usuwane są również referencje do tego obiektu z poziomu bazy danych. Operacja ta wykonywana jest lokalnie w ramach bazy danych każdego z kontrolerów domeny, w związku z tym replikacja tej informacji pomiędzy poszczególnymi partnerami replikacji nie jest wymagana.

Usunięcie referencji do obiektu na obiekcie w ramach atrybutu połączonego nie generuje dodatkowej operacji i nie zwiększa lokalnych numerów USN.

W przypadku replikacji wartości atrybutów połączonych z użyciem LVR, po zamianie obiektu na obiekt nagrobkowy odpowiedni link w ramach wartości atrybutu połączonego oznaczany jest jako „*ABSENT*”. Wartość ta oznacza link, do obiektu, który został skasowany. Wartości te usuwane są z bazy danych katalogu po usunięciu obiektu nagrobkowego.

## ***Wpływ Recycle-Bin na proces kasowania wartości połączonych***

W przypadku katalogu opartego o Windows 2008 R2 z włączoną funkcjonalnością *Recycle Bin* obiekt w stanie *Deleted object* nie jest kasowany z bazy danych i zachowuje wszystkie swoje atrybuty, łącznie z atrybutami połączonymi.

Wartości atrybutów połączonych, odnoszących się do obiektów w stanie *Deleted object* oznaczane są na poziomie bazy danych jak „*INACTIVE*”. Wartości te pozostają w tym stanie do czasu przejścia obiektu w tryb *Recycled object* i przetwarzane są analogicznie jak dla obiektów nagrobkowych.

# Replikacja katalogu Active Directory

## **Moduł IV**

### **Analiza procesu replikacji**





## NARZĘDZIA DIAGNOSTYCZNE

Diagnostyka i analiza problemów związanych z replikacją usługi katalogowej obejmuje wiele elementów działania systemu operacyjnego i połączeń sieciowych. W celu zapewnienia poprawnego działania mechanizmów replikacji wymagane jest nawiązanie poprawnych połączeń sieciowych, poprawne rozwiązywanie nazw DNS i ogólny poprawny stan infrastruktury sieciowej. W celu analizy tych elementów należy korzystać ze standardowych narzędzi używanych w diagnostyce połączeń TCP/IP i usług sieciowych.

W systemie Windows Server dostępne jest kilka narzędzi specjalizowanych do analizy i rozwiązywania problemów z replikacją. Dodatkowo, istnieje kilka narzędzi zewnętrznych, ułatwiających dostęp do metadanych replikacji i innych informacji związanych z replikacją danych usługi katalogowej.

### Narzędzia diagnostyki FRS, DFS-R

W ramach opisu narzędzi i opisu metod analizy i rozwiązywania problemów związanych z replikacją danych usługi katalogowej nie są opisane narzędzia oraz metody związane z usługami FRS i DFS-R.

## Repadmin

REPADMIN.EXE jest podstawowym narzędziem służącym do analizy informacji dotyczących stanu i działania mechanizmów replikacji katalogu Active Directory.

W systemach Windows 2000 oraz 2003 narzędzie to było instalowane w ramach dodatku do systemu – Support Tools.

W systemach Windows 2008 i wyższych narzędzie to jest dostępne wprost w systemie operacyjnym.

REPADMIN.EXE jest narzędziem linii poleceń.

Podstawowa składania REPADMIN.EXE:

```
repadmin <subcommand> [<dsa>] [/u: <nazwa użytkownika>] [/pw: {<hasło> | *}] [/rpc] [/ldap]
[/homeserver: <kontroler domeny na którym wykonane zostanie polecenie>]
```

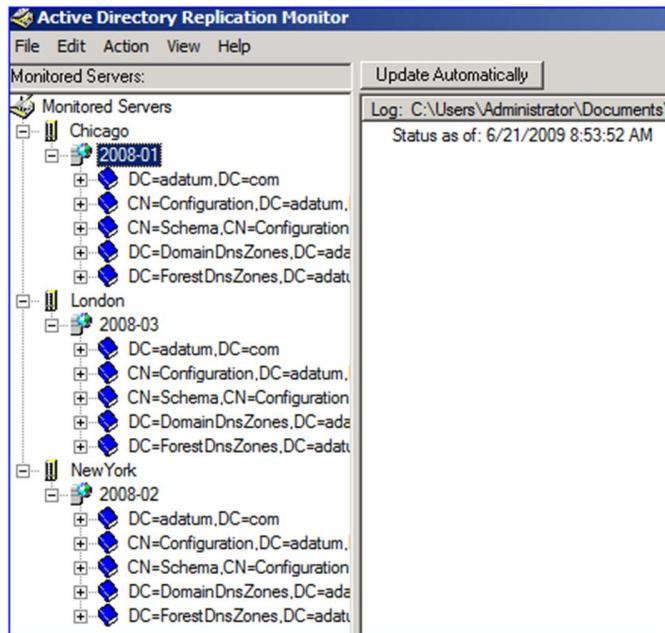
Repadmin posiada szereg komend dodatkowych (*subcommand*), które realizują poszczególne funkcje narzędzia. Każda z tych komend posiada dodatkowe, specyficzne opcje konfiguracyjne.

Pełna składania polecenia REPADMIN opisana jest w ramach dokumentacji systemu na stronach Technet. Link dla wersji Windows 2008: <http://technet.microsoft.com/en-us/library/cc770963%28WS.10%29.aspx>.

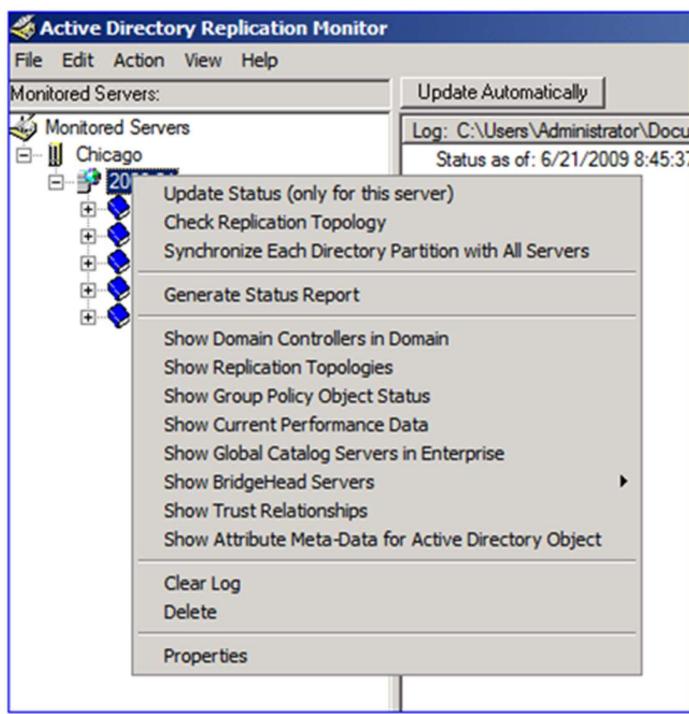
Składnia polecień REPADMIN dostępna jest również poprzez przełączniki /help, /listhelp i /experthelp. W wersji 2008 dostępna jest również opcja /oldhelp prezentująca ekranы pomocy narzędzia z systemu Windows Server 2000 i 2003.

## Replmon

REPLMON jest graficznym narzędziem umożliwiającym analizę konfiguracji i działania replikacji usługi katalogowej.



Narzędzie to umożliwia poprzez konsolę graficzną operacje takie jak wymuszenie replikacji, sprawdzenie statusu replikacji itp.



Narzędzie to dostępne jest w systemach Windows 2003 i wcześniejszych. REPLMON nie posiada wersji dla systemów operacyjnych Windows 2008 i późniejszych. Narzędzie to zostało w systemach tych zastąpione przez REPADMIN.EXE

#### Użycie REPLMON vs REPADMIN

Zalecanym narzędziem w celu analizy stanu i rozwiązywania problemów z replikacją jest REPADMIN.EXE. REPLMON, ze względu na to że nie jest już rozwijanym narzędziem może nie przedstawiać dokładnych informacji związanych z usługą katalogową.

## DCDIAG

DCDIAG jest narzędziem linii poleceń służącym do zbierania informacji i analizy problemów związanych z działaniem kontrolerów domeny oraz usług powiązanych z poprawnym działaniem kontrolera domeny.

W systemach Windows 2000 oraz 2003 narzędzie to było instalowane w ramach dodatku do systemu – Support Tools.

W systemach Windows 2008 i wyższych narzędzie to jest dostępne wprost w systemie operacyjnym.

Podstawowa składnia DCDIAG.EXE:

```
dcdiag [/s:<Kontroler domeny>] [/n:<Kontekst nazewniczy>] [/u:<Domena>\<Nazwa użytkownika>
/p:{* | <hasło> | ""} [{/a | /e}] [{/q | /v}] [/i] [/f:<LogFile>] [/c [/skip:<Test>]]
[/test:<Test>] [/fix] [{/h | /?}] [/ReplSource:<Źródłowy kontroler domeny>]
```

Pełna składnia DCDIAG dostępna jest w ramach dokumentacji TechNET. Link dla wersji Windows Server 2008: <http://technet.microsoft.com/en-us/library/cc731968%28WS.10%29.aspx>.

## ADFIND

AFIND.EXE jest zewnętrznym narzędziem dostępnym bezpłatnie w ramach witryny [www.joeware.net](http://www.joeware.net).

Narzędzie to służy do zadawania zapytań i analizy danych usługi katalogowej Active Directory z użyciem protokołu LDAP.

Podstawowa składnia narzędzia ADFIND:

```
AdFind [switches] [-b basedn] [-f filter] [attr list]
```

W ramach przełączników i opcji dostępnych w ramach polecenia ADFIND istnieje szereg przełączników przydatnych w analizie konfiguracji replikacji usługi katalogowej:

Klasa obiektu	Opis
Opcje zapytań	
<b>-sites</b>	Ustawienie podstawy zapytania na kontener zawierający definicję lokacji (site)
<b>-subnets</b>	Ustawienie podstawy zapytania na kontener zawierający definicje podsieci(site)
<b>-config</b>	Ustawienie podstawy zapytania na kontener konfiguracji lasu
Opcje formatowania wyników	
<b>-flagdc</b>	Dekodowanie wartości pól w ramach atrybutów zawierających flagi bitowe, między innymi instanceType, options, ms-DS-ReplicatesNCReason
<b>-sitename dc</b>	Dekodowanie GUID lokacji do nazwy lokacji
<b>-rootDSE</b>	Odczytanie i dekodowanie atrybutów obiektu rootDSE
Skróty	
<b>-sc objmeta:xxx</b>	Dostęp do metadanych replikacji dla pojedynczego obiektu
<b>-sc showmeta:xxx</b>	Dodatkowy alias do skrótu objmeta

<b>-sc objsmeta:xxx</b>	Dostęp do metadanych wielu obiektów w ramach wskazanej podstawy zapytania
<b>-sc legacylvr:xxx</b>	Lista wartości typu LEGACY w ramach wartości atrybutu wielowartościowego
<b>-sc legacylvr&amp;:xxx</b>	Jak powyżej, dla wielu obiektów
<b>-sc legacygroupmembers:xxx</b>	Lista członków grupy, dla których członkostwo w grupie nadal składowane jest jako wartość typu LEGACY w środowisku z dostępną replikacją LVR
<b>-sc replqueue</b>	Status kolejki replikacji dla danego kontrolera domeny
<b>-sc ncrepl</b>	Status kolejki replikacji dla danego kontrolera domeny, w rozbiocie na poszczególne partie katalogu
<b>-sc replstat:&lt;DC&gt;</b>	Status i informacje o replikacji dla danego kontrolera domeny

ADFINDEXY automatycznie dekoduje do wartości czytelnej wartości atrybutów:

- msDS-NCReplCursors
- msDS-NCReplInboundNeighbors
- msDS-NCReplOutboundNeighbors
- msDS-ReplAllInboundNeighbors
- msDS-ReplAllOutboundNeighbors
- msDS-ReplAttributeMetaData
- msDS-ReplConnectionFailures
- msDS-ReplLinkFailures
- msDS-ReplPendingOps
- msDS-ReplQueueStatistics
- msDS-ReplValueMetaData
- msDS-RetiredRepINCSignatures

Opis opcji dekodowania metadanych replikacji dostępny jest w ramach przełącznika adfind /meta?.

## Rozwiązywanie kodu błędów

W przypadku, gdy w ramach rezultatu zapytania uzyskamy informację o kodzie błędu w postaci kodu hex lub decymalnego możliwe jest rozwiązywanie go do postaci czytelnej przy pomocy następujących narzędzi:

- NET.EXE

Wbudowane narzędzie systemowe udostępniające informację o kodzie błędu w ramach opcji helppmsg.

- ERR.EXE

Dodatkowe narzędzie udostępniane przez Microsoft, przeszukujące definicję nagłówków w bibliotekach systemowych pod kątem zdefiniowanych kodów błędów i komunikatów.

- REPADMIN

Repadmin umożliwia rozwiązywanie kodu błędu na komunikat poprzez przełącznik /showmsg.

## Logowanie diagnostyczne

Usługa katalogowa Active Directory posiada wbudowane mechanizmy logowania diagnostycznego, obejmujące również mechanizmy związane z działaniem procesu replikacji danych.

Konfiguracja logowania diagnostycznego odbywa się poprzez wpis w rejestrze kontrolera domeny w kluczu HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics.

Logowanie można skonfigurować poprzez utworzenie dla danej kategorii logowania zdarzeń wpisu wartości typu DWORD określającej jeden z 5 poziomów logowania:

- **0 – Brak:** logowane są krytyczne zdarzenia, domyślne ustawienia dla wszystkich kategorii logowania.
- **1 – Minimal:** logowane są zdarzenia o dużym poziomie ogólności. Logowane są zdarzenia dla poszczególnych operacji wykonywanych przez usługę.
- **2 – Basic**
- **3 – Extensive:** Logowane są zdarzenia o dużym poziomie szczegółowości, obejmujące wpisy dla poszczególnych kroków wykonywanych w trakcie realizacji zadania.
- **4 – Verbose:** szczegółowy poziom logowania zdarzeń dla usługi. Logowane są poszczególne kroki w ramach operacji
- **5 – Internal:** Logowane są szczegółowe zdarzenia związane z każdym krokiem operacji, wiadomości zawierają wewnętrzne komunikaty diagnostyczne usługi.

Zalecaną praktyką analizy problemu jest rozpoczęcie logowania na poziomie Minimal lub Basic, następnie po zauważeniu problemu do konkretnej grupy lub usługi przejście na poziomie Extensive lub Internal dla tej usługi.

Z punktu widzenia monitorowania mechanizmów replikacji interesujące są następujące kategorie logowania diagnostycznego:

- 1 Knowledge Consistency Checker (KCC)
- 5 Replication Events
- 6 Garbage Collection
- 19 Inter-site Messaging
- 21 Linked-Value Replication
- 22 DS RPC Client
- 23 DS RPC Server

## Przegląd metadanych obiektów

Przegląd metadanych pojedynczego obiektu możliwe jest z użyciem REPADMIN.EXE lub ADFIND.EXE.

Składnia w przypadku REPADMIN.EXE

```
Repadmin /showobjmeta [DSA_LIST] <Object DN> [/nocache] [/linked]
```

DSA\_LIST określa pojedynczy lub wiele kontrolerów domeny, dla których przeprowadzona zostanie operacja. Dopuszczalne jest używanie znaku maski '\*' przy specyfikacji nazwy DC.

Przełącznik /linked powoduje wyświetlenie metadanych dla pojedynczych wartości atrybutów replikowanych z użyciem LVR.

Składnia w przypadku ADFIND.EXE:

```
ADFINDEXEC -sc showmeta:<object DN>
```

## Propagacja zmian w katalogu, stan replikacji

### **Lista partnerów replikacji wraz ze statusem replikacji**

Listę partnerów replikacji wraz ze stanem połączeń replikacji dla danej repliki katalogu można określić z użyciem REPADMIN.EXE z użyciem przełącznika /showrepl.

Podstawowa składnia polecenia:

```
Repadmin /showrepl <DC_LIST> <SourceDCObjectGUID> [NamingContext] [/verbose] [/nocache] [/repsto] [/conn] [/csv] [/all] [/errorsonly] [/intersite]
```

### **Lista partnerów wychodzących replikacji**

Domyślnie repadmin zwraca w wyniku polecenia showrepl tylko partnerów źródłowych, z których dany kontroler domeny replikuje dane. W celu wyświetlenia partnerów replikacji, dla których dana instancja stanowi źródło informacji należy użyć przełącznika /repsto.

Na początku wyników działania narzędzie prezentowane są DSA GUID oraz Invocation ID kontrolera domeny, dla którego zwarcane są wyniki zapytania.

Sekcja **Inbound neighbours** pokazuje listę partycji katalogu oraz listę wszystkich partnerów replikacji, z których dany kontroler domeny otrzymuje zmiany dla danej partycji katalogu.

Default-First-Site-Name\DC1DNS DC Options: IS_GC Site Options: (none) <b>DC object GUID: 3ecd4489-a34c-4034-a3be-bd81fc3f6360</b> <b>DC invocationID: 3ecd4489-a34c-4034-a3be-bd81fc3f6360</b> ===== INBOUND NEIGHBORS ======	<b>GUID kontrolera domeny</b> <b>GUID instancji bazy danych</b>
(...)	<b>Naming context</b>
DC=contoso,DC=com Default-First-Site-Name\DC3DNS via RPC <b>DC object GUID: 5694a479-19a1-426e-a68e-c58f4e0bc6f6</b>	<b>GUID partnera replikacji</b>
===== OUTBOUND NEIGHBORS FOR CHANGE NOTIFICATIONS =====	

W ramach tych informacji linia zaczynająca się od **Last Attempt @:** oznacza informację o wyniku próby replikacji

W przypadku, gdy zawiera ona datę i komunikat **YYYY-MM-DD was sucessfull:** oznacza to poprawnie zakończoną próbę replikacji.

W przypadku gdy zawiera jeden z komunikatów:

- The last successful inter-site replication was prior to the last scheduled replication.
- The last intra-site replication was longer than one hour ago.
- Replication was never successful.

Lub bezpośrednio stwierdzenie o wystąpieniu błędu wskazuje to na problem z replikacją. W przypadku błędu replikacji w wyniku zapytania zwracany jest kod błędu:

```
Last attempt @ 2010-08-27 09:57.46 failed, result 1722
```

Kod błędu należy zweryfikować przy użyciu Err.EXE.

W celu szybkiego odszukania partnera replikacji wskazanego przez dany GUID przy pomocy LDIFDE:

```
ldifde -d "<GUID=Wartość GUID>" -f con -l 1.1 -p base
```

Przy pomocy REPADMIN:

```
Repadmin /dsaguid . <GUID>
```

Przy pomocy ADFIND.EXE :

```
adfind -b "<GUID=Wartość GUID>"
```

## Połączenia replikacji

W celu zweryfikowania czy pomiędzy danymi kontrolerami domeny istnieją połączenia replikacji należy użyć polecenia repadmin z przełącznikiem /showconn.

Polecenie to może być użyte z różnymi opcjami. Podstawowa składnia polecenia to:

```
repadmin /showconn <DC_LIST> {<ServerRDN> | <ContainerDN> | <DC_GUID>} [/From: <ServerRDN>] [/intersite]
```

W celu wylistowania wszystkich połączeń dla danego kontrolera domeny z innego kontrolera domeny, należy użyć polecenia:

```
repadmin /showconn <nazwa DC> /From: <źródłowy kontroler domeny>
```

## Błędy w procesie replikacji

Dane gromadzone przez KCC pozwalają na wylistowanie wszystkich połączeń replikacji, dla których w danym momencie zidentyfikowana została informacja o problemie z połączeniem. Do wylistowania tej informacji służy polecenie repadmin z przełącznikiem /failcache.

Podstawowa składnia tego polecenia wygląda następująco:

```
repadmin /failcache <DC_LIST>
```

W wyniku polecenia:

- **KCC Connection Failures:** błędy przy próbie stworzenia połączenia replikacji z danym kontrolerem domeny
- **KCC Link Failures:** błędy występujące dla istniejących połączeń.

W przypadku braku błędów wynik polecenia wygląda w sposób następujący:

```
C:\>repadmin /failcache  
repadmin running command /failcache against server localhost  
==== KCC CONNECTION FAILURES =====  
<none>  
==== KCC LINK FAILURES =====  
<none>  
C:\>
```

## Weryfikacja statusu replikacji

### Weryfikacja statusu replikacji przy użyciu Repadmin

Weryfikacja całkowitego stanu replikacji w ramach organizacji umożliwia przełącznik /replsummary narzędzia repadmin. Podstawowa składnia repadmin w tym wypadku:

```
Repadmin /replsummary <DC_LIST> [/bysrc] [/bydest] [/errorsonly] [/sort:{delta | partners | failures | error | percent}]
```

Polecenie to zbiera informacje o połączeniach replikacji i ich statusie z wszystkich kontrolerów domeny w ramach organizacji. W przypadku braku możliwości skontaktowania się z danym kontrolerem domeny polecenie to zaraportuje błąd wraz z komunikatem określającym powód wystąpienia błędu połączenia.

W celu zebrania danych o stanie replikacji w całej organizacji należy posłużyć się poleceniem:

```
Repadmin /replsummary /bysrc /bydest /sort:delta
```

W wyniku polecenia:

- **Largest delta:** Najdłuższa przerwa replikacji w ramach połączeń replikacji dla danego kontrolera domeny
- **Total:** liczba połączeń replikacji dla danego kontrolera domeny
- **Fails:** liczba błędnych połączeń replikacji dla danego kontrolera domeny (0 oznacza brak błędów, nigdy większe niż *Total* ).

#### **REPLSUMMARY i połączenia przejściowe**

Repadmin z przełącznikiem REPLSUMMARY analizuje dane w oparciu o połączenia replikacji uwzględniając opóźnienia w replikacji pomiędzy bezpośrednio sąsiadującymi ze sobą (połączonymi przez obiekty połączeń) kontrolerami domeny.

Narzędzie to nie określa czasu przejścia i opóźnienia w replikacji pomiędzy kontrolerami domeny, które nie replikują się bezpośrednio.

W ramach wyniku działania polecenia należy w pierwszej kolejności weryfikować wyniki w odniesieniu do kontrolerów docelowych (replikacja w trybie pull).

## Opóźnienia w replikacji

W celu określenia opóźnień w replikacji danych w ramach katalogu należy posłużyć się poleceniem repadmin z przełącznikiem /showutdvec.

### Wersja dla Windows 2000

Działanie przełącznika /showutdvec jest oparte o rozszerzoną informację o znaczniku czasowym przechowywaną w ramach tablicy UTD. Informacja ta wprowadzona została w Windows Server 2003, dlatego przełącznik ten nie może być użyty w ramach środowiska Windows 2000.

W wersji Windows 2000 istnieje przełącznik /latency wykonujący to samo zadanie w oparciu o inną informację (uaktualnienia atrybutu dla ISTG).

Podstawowa wersja polecenia repadmin z /showutdvec wygląda następująco:

```
repadmin /showutdvec <DC_LIST> <NamingContext> [/nocache] [/latency]
```

Wynik przedstawia opóźnienie w replikacji danych z punktu widzenia danego kontrolera domeny w odniesieniu do informacji o ostatniej zakończonej bezpośredniej lub przechodniej replikacji danego kontekstu nazewniczego z danym kontrolerem domeny.

### GUID w wynikach polecenia repadmin /showutdvec

W przypadku, gdy w wyniku polecenia repadmin z przełącznikiem widoczne są GUID zamiast nazw kontrolerów domeny reprezentują one informacje o zmienionych *Invocation ID* lub usuniętych kontrolerach domeny.

## Narzędzia alternatywne – convergeCheck

convergeCheck jest alternatywnym narzędziem (skrypt CMD) stworzonym przez Deana Wellsa, które określa czas replikacji w ramach katalogu zmian poprzez śledzenie replikacji do wszystkich kontrolerów domeny zmiany na wskazanym obiekcie katalogu.

Skrypt ten posługuje się w celu określenia informacji o propagacji obiektu w katalogu śledzeniem propagacji numeru USN zmian wykonanej na śledzonym obiekcie do poszczególnych kontrolerów domeny biorących udział w replikacji. Składnia skryptu:

```
convergeCheck <DN obiektu testowego>
```

Obiekt testowy to dowolny obiekt katalogu replikowany pomiędzy replikami katalogu, na którym wykonano zmiany której propagacja ma być śledzona w organizacji.

Skrypt do działania wymaga obecności w systemie następujących narzędzi:

- Find.exe
- Ldifde.exe
- Repadmin.exe

Skrypt obrazuje czas propagacji zmiany w środowisku z uwzględnieniem czasu przejścia replikowanej zmiany pomiędzy kontrolerami domeny, które nie są bezpośrednio połączone w ramach topologii replikacji.

## **Weryfikacja stanu replikacji pojedynczej zmiany dla kontrolera domeny**

W celu uzyskania informacji o tym, czy dwa kontrolery domeny wykonały replikację zmian pomiędzy sobą należy posłużyć się poleceniem repadmin z przełącznikiem /checkprop.

Polecenie to weryfikuje czy dany numer USN określający numer zmiany wprowadzonej na kontrolerze domeny (originating update) została już zreplikowana do wskazanego kontrolera domeny:

Podstawowa składnia polecenia repadmin z przełącznikiem /checkprop:

```
repadmin /checkprop <DC_LIST> <NamingContext> <OriginatingDCInvocationID> <OriginatingUSN>
```

## **Kolejka połączenia i oczekujące zmiany**

Repadmin z przełącznikiem /queue pozwala na wyświetlenie kolejki zmian oczekujących na replikację w ramach danego kontrolera domeny.

Podstawowa składnia tego polecenia to:

```
repadmin /queue <DC_LIST>
```

W celu określenia zmian, które oczekują na replikację pomiędzy dwoma partnerami replikacji należy posłużyć się poleceniem repadmin z przełącznikiem /showchanges, w następującej składni:

```
repadmin /showchanges <DestDC> <SourceDCObjectGUID> <NamingContext> [/verbose] [/statistics] [/noincremental] [/objectsecurity] [/ancestors] [/atts: <attribute1>,<attribute2>,...] [/filter: <ldap filter>]
```

Gdzie **DestDC** oznacza docelowy kontroler domeny otrzymujący zmiany a **SourceDCObjectGUID** oznacza źródłowy kontroler domeny, na którym zmiany oczekują na replikację.



# Replikacja katalogu Active Directory

## **Moduł V**

### **Problemy z procesem replikacji**





# TYPOWE PROBLEMY ZWIĄZANE Z REPLIKACJĄ DANYCH KATALOGU

## Problemy infrastruktury

### Usługa DNS

W celu poprawnego działania mechanizmów replikacji, partnerzy replikacji muszą mieć możliwość rozwiązania nazwy zdefiniowanej w ramach rekordu CNAME opartego o GUID kontrolera domeny.

W przypadku braku możliwości rozwiązania tej nazwy lub błędnych danych zwracanych przez ten rekord replikacja pomiędzy partnerami replikacji nie będzie mogła być przeprowadzona.

Przy wywołaniu polecenia repadmin z przełącznikiem /rep1summary, dodatkowy przełącznik /verbose pozwala uzyskać szczegółowe informacje o partnerze replikacji.

```
(...) wynik repadmin /verbose (...)
```

Wynik działania zawiera następujące informacje:

- **Address:** record DNS używany do rozwiązania nazwy kontrolera domeny będącego partnerem replikacji
- **DC invocation ID:** GUID instancji bazy danych
- Flagi dla połączenia replikacji
- **USNs:** wartość
  - /OU: wartość USN z *high-watermark vector*, wartość USN w trakcie replikacji
  - /PU: wartość USN z *high-watermark vector*, najwyższa wartość USN zreplikowana od danego partnera replikacji.

#### Interpretacja wartości USN

Różne wartości USN w opcjach OU i PU oznaczają cykl replikacji w trakcie trwania. Wartość PU równa 0 oznacza połączenie, które nigdy nie zostało poprawnie zreplikowane.

Wartość zwracana jako **Address** wskazuje adres DNS jaki używany jest do połączenia z danym kontrolerem domeny. W celu weryfikacji poprawności rozwiązywania nazw DNS dla partnera replikacji należy posłużyć się narzędziem pozwalającym na rozwiązywanie nazw DNS:

```
NSLOOKUP -Q=ANY <CNAMES dla kontrolera domeny>
```

Błędy połączenia wynikające z błędnych danych DNS logowane będą w ramach logowania diagnostycznego w kategorii „DS RPC Client”.

W celu weryfikacji poprawności rejestracji rekordów DNS kontrolera domeny należy użyć narzędzia DCDIAG z przełącznikiem /test:dns.

Typowe komunikaty błędów związane z błędym rozwiązywaniem nazw DNS w ramach statusów replikacji:

- **Kod błędu 8524:** ERROR\_DS\_DNS\_LOOKUP\_FAILURE
- **Kod błędu 1722:** The RPC server is unavailable

Procedura weryfikacji i rozwiązania problemów związanych z usługą DNS dla kontrolera domeny opisana jest w artykule Technet „Fixing Replication DNS Lookup Problems (Event IDs 1925, 2087, 2088)” <http://technet.microsoft.com/en-us/library/cc737678%28WS.10%29.aspx>.

## Konfiguracja połączeń sieciowych

Komunikacja związana z ruchem replikacji usługi katalogowej, zarówno wewnętrz lokacji jak i pomiędzy lokacjami w większości przypadków odbywa się z użyciem protokołu RPC. Komunikacja z użyciem protokołu RPC wymaga otwarcia komunikacji z użyciem dynamicznie otwieranego zakresu portów sieciowych.

Lista usług i portów wymaganych dla poprawnego działania usługi katalogowej opisana jest w artykule „Active Directory and Active Directory Domain Services Port Requirements” <http://technet.microsoft.com/en-us/library/dd772723%28WS.10%29.aspx>.

### Komunikacja pomiędzy kontrolerami domeny

Zalecane jest aby ruch pomiędzy kontrolerami domeny nie był blokowany lub ograniczany przez mechanizmy takie jak firewall.

W przypadku konieczności ograniczenia konfiguracji portów sieciowych do statycznego zakresu portów możliwe jest wskazanie mechanizmom usługi katalogowej statycznej listy portów, które mają być używane w ramach mechanizmów replikacji danych katalogu. Konfiguracja statycznych portów RPC dla replikacji usługi katalogowej opisana jest w KB „Restricting Active Directory replication traffic and client RPC traffic to a specific port” <http://support.microsoft.com/kb/224196>.

Najczęstszym objawem problemów w ramach replikacji związanych z problemami z połączeniem sieciowym są następujące błędy:

- **Kod błędu 1722:** The RPC server is unavailable
- **Kod błędu 5:** ERROR\_ACCESS\_DENIED

Procedura weryfikacji i rozwiązyania problemów wynikających z połączeń sieciowych opisana jest w ramach artykułu Technet „Event ID 1925: Attempt to establish a replication link failed due to connectivity problem” <http://technet.microsoft.com/en-us/library/cc787129%28WS.10%29.aspx>.

## Problemy występujące w procesie replikacji danych

### No more endpoints

Komunikat “No more endpoints” w ramach status replikacji wskazuje na problem wynikający z połączenia sieciowego. Komunikat ten wskazuje na to, że KCC było w stanie utworzyć połączenie replikacji pomiędzy dwoma partnerami replikacji, jednak brak połączenia sieciowego, nieprawidłowe dane DNS lub stan źródłowego systemu nie pozwala na wykonanie połączenia replikacji.

W celu diagnostyki problemu należy:

- Zweryfikować poprawność rozwiązywania nazw DNS i rejestracji adresu IP
- Zweryfikować stan systemu partnera replikacji,
- Zweryfikować ruch sieciowy pomiędzy partnerami replikacji.

### Active Directory replication has been preempted

Komunikat ten oznacza, że dane żądanie replikacji zostało wywalczone przez żądanie z wyższym priorytetem. Żądanie takie może zostać wywołane przez manualne wymuszenie synchronizacji (repadmin /sync) lub przez ruch replikacji o wyższym priorytecie.

W celu diagnostyki problemu należy posłużyć się poleceniami:

- Repadmin /showrepl: weryfikacja istniejących połączeń i stanu replikacji
- Repadmin /queue: stan kolejki replikacji dla danego kontrolera domeny.

### Access denied

Komunikat o kodzie błędu 5 – *access denied* może wynikać z wielu przyczyn, w szczególności z:

- Błędów w rozwiązywaniu nazw DNS pomiędzy partnerami replikacji
- Problemów w komunikacji występujących na poziomie ruchu sieciowego, błędów połączenia lub wyfiltrowania portów niezbędnych do działania mechanizmów replikacji na poziomie ruchu sieciowego.
- Błędów nawiązania połączenia replikacji z wyłączeniem lub nieistniejącym kontrolerem domeny.
- Próby nawiązania połączenia replikacji z kontrolerem domeny, dla którego w lokalnej bazie danych istnieje nieprawidłowe hasło.

W przypadku problemów związanych z usługami DNS i połączaniami sieciowymi należy dokonać diagnostyki z użyciem wymaganych do tego narzędzi.

W przypadku błędów wynikających z braku dostępu do kontrolera domeny należy zweryfikować czy dany kontroler domeny jest włączony. W przypadku nieistniejących kontrolerów domeny należy wykonać operację usunięcia metadanych kontrolera z katalogu zgodnie z procedurą opisaną w KB „How to remove data in Active Directory after an unsuccessful domain controller demotion” (<http://support.microsoft.com/kb/216498>).

Problem wynikający z błędного hasła kontrolera domeny może powstać na przykład w wyniku odtworzenia kopii zapasowej kontrolera domeny, sprzed okresu po którym kontroler domeny (jak każdy komputer w ramach domeny) zmienił swoje hasło komputera.

Ponieważ do poprawnego działania mechanizmów replikacji wymagana jest poprawna komunikacja z użyciem protokołu Kerberos, błędne hasło kontrolera domeny nie pozwala na nawiązanie połączenia replikacji pomiędzy dwoma kontrolerami domeny (hash hasła używany jest jako klucz szyfrowania w ramach uwierzytelnienia Kerberos).

W takim przypadku należy przeprowadzić operacje resetu hasła komputera dla kontrolera domeny zgodnie z KB „How to use Netdom.exe to reset machine account passwords of a Windows Server domain controller” <http://support.microsoft.com/kb/325850>.

## No inbound neighbors

Występowanie tego błędu wskazuje na problem z utworzeniem przychodzących połączeń replikacji pomiędzy danym kontrolerem domeny a innymi kontrolerami domeny. Ponieważ replikacja danych katalogu działa w trybie pull, połączenie przychodzące jest wymagane do poprawnego działania mechanizmów replikacji.

Brak przychodzących połączeń replikacji może wynikać z faktu:

- Braku utworzonych połączeń, w przypadku gdy proces KCC został zatrzymany przez administratora
- Braku możliwości nawiązania połączenia z kontrolerami domeny w ramach istniejących połączeń
- Skasowanie istniejących połączeń replikacji, w sytuacji gdy KCC nie utworzyło ponownie połączeń replikacji danych.

W celu diagnostyki problemu należy skorzystać z następujących poleceń:

- Repadmin /showrepl: weryfikacja istniejących połączeń i stanu replikacji
- Repadmin /showconn: lista istniejących połączeń
- Repadmin /failcache: lista znanych dla KCC błędów związanych z replikacją
- Repadmin /kcc: wymuszenie uruchomienia KCC w celu utworzenia połączeń

W przypadku stwierdzenia braku połączeń replikacji należy utworzyć połączenia replikacji i

## ZAAWANSOWANE PROBLEMY Z PROCESEM REPLIKACJI

### Linger objects

Linger objects (*ang. Zestarzały, przewlekły, opuszczony*) jest to obiekt, który występuje w jednej lub więcej replik katalogu a nie występuje w pozostałych replikach katalogu. Obiekty tego typu powstają w przypadku, gdy dany obiekt został usunięty przez proces Garbage Collector z poprawnie działających replik katalogu a w wyniku błędu konfiguracji lub działań administratora nie został on usunięty lub został przywrócony z kopii zapasowej na danej replice katalogu.

### Mechanika powstawania linger objects

Powstanie obiektów typu *linger objects* wymaga aby zaszły warunki, w których pojedyncza replika katalogu nie była w stanie zakończyć procesu usunięcia. Obiekty typu *linger objects* mogą powstać w następujących przypadkach:

- Długotrwałe odłączenie kontrolera domeny od sieci, uniemożliwiające mu otrzymanie informacji o usunięciu obiektu w ramach procesu replikacji. Okres odłączenia kontrolera domeny od sieci i brak replikacji musi przekraczać wartość *tombstoneLifeTime*.
- Błąd konfiguracji powodujące wyłączenie kontrolera domeny z procesu replikacji przez okres przekraczający *tombstoneLifeTime*.
- Przywrócenie kontrolera domeny z kopii zapasowej, starszej niż dopuszczalny czas życia kopii zapasowych (wyznaczany przez *tombstoneLifeTime*).
- Zmiana czasu w ramach domeny wybiegająca w przyszłość, w chwili gdy poszczególne repliki katalogu nie są w pełni zsynchronizowane
- Zmiany *tombstoneLifeTime* (skrócenie) mające na celu przyspieszenie procesu Garbage Collector.

W wyniku tych operacji może wystąpić sytuacja, w której w ramach pojedynczego (lub wielu) replik katalogu pozostaną obiekty, które zostaną usunięte z innych replik katalogu.

### Replikacja z partnerami zawierającymi linger objects

W przypadku wystąpienia *linger object* w ramach repliki katalogu, jej partnerzy replikacji nie powinni replikować się z daną repliką katalogu.

W Windows 2000 (i późniejszych) replikacja katalogu z partnerami, którzy zawierają niepoprawne dane kontrolowane jest przez wpis w rejestrze kontrolera domeny. W kluczu HKLM\System\CurrentControlSet\Services\NTDS\Parameters, utworzona musi zostać wartość Allow Replication With Divergent and Corrupt Partner (DWORD). Wartość 1 w ramach tego klucza powoduje, że partner replikacji nie wykonuje replikacji z kontrolerem domeny zawierającym *linger objects*.

## Strict \ loose replication consistency

W Windows Server 2003 wprowadzono nowy mechanizm wykrywania i ochrony kontrolerów domeny przed replikacją danych o niepoprawnych obiektach o nazwie *Strict replication consistency*.

Mechanizm ten w domyślnych ustawieniach powoduje, że partner replikacji odmawia replikacji z kontrolerem domeny zawierającym obiekty typu *lingering objects* i loguje odpowiedni wpis w dzienniku zdarzeń(Event ID: 1988).

Administrator ma możliwość wyłączenia mechanizmu ochrony i przejście w tryb *Loose replication consistency* umożliwiającej replikację danych z partnerami, zawierającymi błędne dane. W takim wypadku w ramach dziennika zdarzeń logowane jest zdarzenie Event ID:1388 zawierające następujące informacje:

- Adres sieciowy źródłowego kontrolera domeny (w postaci rekordu CNAME zawierającego GUID).
- DN obiektu
- GUID obiektu
- DN partycji katalogu zawierającego nieoprawny obiekt
- Najwyższy USN na docelowym kontrolerze domeny.

Tryb replikacji kontrolowany jest przez wpis w rejestrze kontrolera domeny, w kluczu HKLM\System\CurrentControlSet\Services\NTDS\Parameters, wartość *Strict Replication Consistency (DWORD)*:

- 0 – Loose replication consistency
- 1 – Strict replication consistency

Domyślnie, kontrolery domeny oparte o systemy operacyjne Windows Server 2003 i wyższe działają w trybie *Strict replication consistency*.

## Diagnostyka problem

W przypadku kontrolerów domeny pracujących w oparciu o system operacyjny Windows Server 2003 lub wyższy, kontroler domeny, który działa w trybie *Strict replication consistency* w chwili wykrycia problemu zapisuje w dzienniku zdarzeń systemowych Event o ID 1988.

W celu wykrycia obiektów powodujących wystąpienie problemu należy posłużyć się poleceniem repadmin z przełącznikiem /removelingerobject w trybie ADVISORY

```
REPADMIN /REMovelingerobjects <FQDN kontrolera domeny zawierającego błędne dane> <DSA GUID DC z poprawnymi danymi> <DN partycji katalogu> /ADVISORY_MODE
```

W wyniku działania narzędzia, na kontrolerze domeny zawierającym niepoprawne dane wywołane zapisane zostaną następujące zdarzenia w dzienniku zdarzeń:

- EventID:1337 – rozpoczęcie procesu weryfikacji danych

- Ewenki: 1945 – wpis dla każdego wykrytego obiektu objętego problemem
- EventID:1339 – podsumowanie procesu weryfikacji obiektów.

W celu przeprowadzenie procesu wymagane jest działanie kontrolerów domeny w trybie *Strict replication consistency*.

## Rozwiążanie problemu

W celu usunięcia obiektów powodujących wystąpienie problemy należy posłużyć się polecением repadmin z przełącznikiem /removelingerobject:

```
REPADMIN /REMOVELINGERINGOBJECTS <FQDN kontrolera domeny zawierającego błędne dane> <DSA GUID DC z poprawnymi danymi> <DN partycji katalogu>
```

## USN roll-back

USN roll-back jest to sytuacja, w której lokalny licznik USN zostaje przywrócony do wartości mniejszej, niż USN przypisany do poprzednio wprowadzonych na tym kontrolerze domeny zmian.

Ponieważ USN jest lokalny dla danego DC i jest zwiększany o 1 z każdą transakcją przeprowadzoną na danym kontrolerze domeny, wartość tego licznika nigdy nie powinna się zmniejszyć w ramach danej instancji bazy danych katalogu. Jest to podstawowe założenie, które używane jest w mechanizmach replikacji danych katalogu.

### Schemat powstawania problemu

Najczęstszą przyczyną powstawania problemu określano jako USN roll-back jest odtworzenie kontrolera domeny z użyciem metody, która nie wykonuje wszystkich wymaganych operacji związanych z odtworzeniem kopii kontrolera domeny w wyniku czego w trakcie operacji odtworzenia kontrolera domeny nie są zmieniane wartości *Invocation ID* dla danej instancji bazy danych.

Ponieważ wartość USN wraz z informacją o *Invocation ID* składa się na informację przechowywaną w tabeli *high-watermark vector*, cofnięcie numeru USN powoduje, że dany kontroler domeny nie jest w stanie zreplikować danych wprowadzanych do katalogu po operacji powodującej USN roll-back, do czasu, gdy lokalny numer USN nie osiągnie wartości większej niż maksymalny USN zapamiętany przez partnerów replikacji.

#### Obrazy dysków

Główną przyczyną powstawania sytuacji określanych jako USN roll-back jest odtworzenie kontrolera domeny z obrazu dysku lub snapshotu maszyny wirtualnej.

### Diagnostyka

W przypadku, gdy w ramach danego kontrolera domeny zajdzie sytuacja powodująca powstawanie USN roll-back, przy najbliższej próbie replikacji kontroler ten wykryje tą sytuację i zaloguje w dzienniku zdarzeń Event ID:2095.

Wykrycie USN roll-back następuje na podstawie przesłanej do źródłowego (objętego problemem) DC tablicy high-watermark vector partnera replikacji. Na jej podstawie kontroler domeny stwierdza, że obecny USN jest mniejszy niż najwyższy USN przekazany już partnerowi replikacji.

### Rozwiążanie problemu

W praktyce, jedyne dostępne rozwiązanie problemu to usunięcie kontrolera domeny objętego problemem z katalogu.

# Replikacja katalogu Active Directory

## **Moduł VI**

### **Integracja usługi katalogowej z DNS**



# **INTEGRACJA DNS Z USŁUGĄ ACTIVE DIRECTORY**

## **Strefy DNS usługi katalogowej Active Directory**

Usługa DNS w ramach Windows Server może utrzymywać dwa typy stref usługi DNS:

- Strefy standardowe, przechowywane w ramach systemu plików serwera DNS
- Strefy zintegrowane z usługą katalogową Active Directory, przechowywane w ramach danych usługi katalogowej.

W ramach systemów opartych o Windows 2000 informacje o strefach DNS utrzymywane były w ramach partycji domenowej katalogu, w związku z czym replikowane były do wszystkich kontrolerów domeny w ramach danej domeny.

Strefa \_msdcs w domenie głównej lasu replikowana była w ramach partycji domenowej tej domeny. Informacje o obiektach związanych z usługą DNS replikowane były również do partycji GC.

W systemach Windows Server 2003 i wyższym dane usługi DNS przechowywane są w ramach partycji aplikacyjnych.

- CN=DomainDNSZones,< DN partycji domenowej katalogu>, domyślnie replikowana tylko do kontrolerów domeny, pełniących rolę serwera DNS w ramach danej domeny.
- CN=ForestDNSZones,< DN partycji domenowej głównej domeny lasu >, domyślnie replikowana do wszystkich kontrolerów domeny, pełniących rolę serwera DNS w ramach całego lasu.

Przeniesienie danych DNS do partycji aplikacyjnych pozwala na replikowanie ich tylko do kontrolerów domeny, pełniących rolę serwerów DNS. Dodatkowo, dane partycji aplikacyjnych nie wchodzą w skład danych replikowanych do partycji Global Catalog, ograniczając tym samym zakres danych i rozmiar tych partycji.

W ramach każdej domeny usługi katalogowej tworzona jest strefa DNS dla danej domeny, przechowywana w ramach partycji aplikacyjnej CN=DomainDNSZones.

W ramach lasu usługi katalogowej tworzona jest wspólna strefa DNS o nazwie \_MSDCS.<FQDN domeny głównej lasu>. Strefa \_MSDCS zawiera rekordy SRV dla wszystkich kontrolerów domeny w ramach lasu. Strefa ta jest wymagana do poprawnego działania mechanizmów lokalizacji kontrolerów domeny oraz replikacji usługi katalogowej.

# REKORDY DNS USŁUGI KATALOGOWEJ

## Rekordy DNS rejestrowane przez kontroler domeny

Usługa netlogon na każdym z kontrolerów domeny odpowiedzialna jest za rejestrację rekordów DNS dla danego kontrolera domeny.

### Częstotliwość rejestracji rekordów DNS

Po uruchomieniu kontroler domeny okresowo dokonuje rejestracji rekordów w usłudze DNS. Rejestracja ta odbywa się w następujących okresach czasu:

- Dla Windows 2000: raz na godzinę
- Windows 2003: raz na 24 godziny
- Windows 2008 i późniejsze (do 2008 R2): raz na godzinę.

*Rejestracja rekordów DNS wykonywana jest również przy każdym starcie usługi Netlogon na kontrolerze domeny.*

Poniższa tabela przedstawia listę rekordów SRV rejestrowanych przez usługę netlogon na kontrolerze domeny. W ramach poniższej tabeli:

- DnsDomainName:FQDN strefy DNS domeny usługi katalogowej
- DnsForestName: FQDN głównej domeny lasu usługi katalogowej

Rekord SRV	Opis
_ldap._tcp.DnsDomainName.	Rekord lokalizacji usługi LDAP w ramach danej domeny. Rekord usługi LDAP niekoniecznie wskazuje kontroler domeny. Każdy kontroler domeny domyślnie rejestruje tego typu rekord. Wszystkie kontrolery domeny Windows 2003 i wyższe domyślni rejestrują tego typu rekord.
_ldap._tcp.SiteName._sites.DnsDomainName.	Rekord lokalizacji usługi LDAP w ramach lokacji usługi katalogowej. Rekord usługi LDAP niekoniecznie wskazuje kontroler domeny. Każdy kontroler domeny domyślnie rejestruje tego typu rekord. Wszystkie kontrolery domeny Windows 2003 i wyższe domyślni rejestrują tego typu rekord.
_ldap._tcp.dc._msdcs.DnsDomainName.	Rekord lokalizacji usługi kontrolera domeny w ramach domeny. Wszystkie kontrolery domeny Windows 2003 i wyższe domyślne rejestrują tego typu rekord.
_ldap._tcp.SiteName._sites.dc._msdcs.DnsDomainName.	Rekord lokalizacji usługi kontrolera domeny w ramach lokacji w danej domenie. Wszystkie kontrolery domeny Windows 2003 i wyższe domyślne rejestrują tego typu rekord.
_ldap._tcp.pdc._msdcs.DnsDomainName.	Rekord lokalizacji kontrolera domeny pełniącego rolę PDC Emulator w ramach domeny. Wszystkie kontrolery domeny Windows 2003 i wyższe domyślne rejestrują tego typu rekord.
_ldap._tcp.gc._msdcs.DnsForestName.	Rekord lokalizacji kontrolera domeny pełniącego rolę GC w ramach lasu usługi katalogowej.
_ldap._tcp.SiteName._sites.gc._msdcs.DnsForestName.	Rekord lokalizacji kontrolera domeny pełniącego rolę GC w ramach danej lokacji usługi katalogowej.
_gc._tcp.DnsForestName.	Rekord lokalizacji serwera Global Catalog dla lasu usługi katalogowej. Rejestrowany domyślnie przez każdy DC pełniący rolę GC.

_gc._tcp.SiteName._sites.DnsForestName.	Rekord lokalizacji serwera Global Catalog dla lasu usługi katalogowej w ramach danej lokacji usługi katalogowej. Rejestrowany domyślnie przez każdy DC pełniący rolę GC.
_ldap._tcp.DomainGuid.domains._msdcs.DnsForestName.	Rekord lokalizacji kontrolera domeny z użyciem GUID dla obiektu domeny.
_kerberos._tcp.DnsDomainName.	Rekord lokalizacji serwerów pełniących rolę KDC w ramach domeny, dla komunikacji z użyciem TCP.
_kerberos._udp.DnsDomainName.	Rekord lokalizacji serwerów pełniących rolę KDC w ramach domeny, dla komunikacji z użyciem UDP.
_kerberos._tcp.SiteName._sites.DnsDomainName.	Rekord lokalizacji serwerów pełniących rolę KDC w ramach domeny w danej lokacji usługi katalogowej, dla komunikacji z użyciem TCP.
_kerberos._tcp.dc._msdcs.DnsDomainName.	Rekord lokalizacji serwerów pełniących rolę KDC w ramach domeny, dla komunikacji z użyciem TCP.
_kerberos.tcp.SiteName._sites.dc._msdcs.DnsDomainName.	Rekord lokalizacji serwerów pełniących rolę KDC w ramach domeny w danej lokacji usługi katalogowej, dla komunikacji z użyciem TCP.
_kpasswd._tcp.DnsDomainName.	Rekord lokalizacji usługi zmiany hasła z użyciem protokołu Kerberos w ramach domeny, dla komunikacji przy pomocy TCP.
_kpasswd._udp.DnsDomainName.	Rekord lokalizacji usługi zmiany hasła z użyciem protokołu Kerberos w ramach domeny, dla komunikacji przy pomocy UDP.

Rekordy typu A (host) rejestrowane przez kontroler domeny:

Rekord SRV	Opis
DnsDomainName.	Rekord A wskazujący na nazwę domeny i adres IP kontrolera domeny. Pozwala na lokalizację dowolnego kontrolera domeny przez odwołanie do rekordu A
Gc._msdcs.DnsForestName	Rekord A wskazujący na adres IP kontrolera domeny. Pozwala na lokalizację dowolnego kontrolera domeny pełniącego rolę GC w ramach lasu.

Dodatkowo, każdy kontroler domeny pełniący role serwera DNS dla danej domeny rejestruje rekord NS dla danej domeny.

Usługa netlogon rejestruje również rekord CNAME oparty o identyfikator GUID kontrolera domeny, używany w celu lokalizacji partnerów replikacji. Rekord ten ma postać `DsaGuid._msdcs.DnsForestName`.

#### **Weryfikacja rejestracji rekordów DNS dla kontrolera domeny**

Weryfikację rekordów rejestrowanych przez kontroler domeny przeprowadzić na podstawie wartości pliki NETLOGON.DNS zlokalizowanego na kontrolerze domeny w folderze %systemroot%System32\config\NETLOGON.DNS. W ramach tego pliku rejestrowane są rekordy DNS tworzone i uaktualniane przez kontroler domeny w usłudze DNS. Linie rozpoczętające się od znaku średnika ';' oznaczają rekordy DNS, których nie udało się zarejestrować w usłudze DNS.

Weryfikację rejestracji rekordów DNS można przeprowadzić również przy pomocy narzędzi takich jak nslookup, netdiag, dcdiag.

## Wpisu *domain wide* i *site specific*

W ramach konfiguracji rekordów DNS w domenie, usługa netlogon rejestruje dwa typy rekordów dla usług kontrolera domeny:

- Domenowe (*domain wide*): rekordy te wskazują na usługi zarejestrowane jako usługi dla całej domeny usługi katalogowej.
- Dla lokalizacji (*site specific*): rekordy te wskazują na usługi zarejestrowane, dla danej lokacji usługi katalogowej.

Rekordy te używane są w procesie lokalizacji kontrolera domeny przez klienta i usługi korzystające z usługi DC Locator. Klient, lokalizujący kontroler domeny, w chwili gdy znana jest lokacja do której przypisany jest klient wykonuje zapytanie dotyczące kontrolera domeny dla danej domeny, w danej lokacji:

```
_ldap._tcp.<SITE>._sites.dc._msdcs.<FQDN Domeny>
```

Rekordy tego typu rejestrowane są domyślnie przez wszystkie kontrolery domeny dla lokacji, w której znajduje się dany kontroler domeny.

W przypadku, gdy klient nie posiada informacji o lokacji do której jest przypisany w ramach usługi katalogowej klient posługuje się zapytaniem o rekord usługi kontrolera domeny rejestrowany na poziomie domeny:

```
_ldap._tcp.dc._msdcs.<FQDN Domeny>
```

Używając rekordów specyficznych dla danej lokacji, klient może zlokalizować kontroler domeny w ramach danej lokacji. W przypadku, gdy klient nie zna lokacji, nie może być przypisany do żadnej lub lokalne kontrolery domeny w lokacji nie są dostępne, klient w oparciu o rekordy rejestrowane dla domeny jest w stanie zlokalizować kontroler domeny obsługujące klientów z całej domeny.

W domyślnej konfiguracji każdy kontroler domeny rejestruje oba typy rekordów.

## Konfiguracja rekordów DNS w scenariuszach branch office

W przypadku scenariuszy konfiguracji usługi katalogowej, w której występują lokacje centralne jak i lokacje oddziałowe, domyślna konfiguracja rejestracji rekordów DNS przez usługę netlogon powoduje, że dowolny kontroler domeny, z dowolnej lokacji może zostać zlokalizowany przez klienta w odpowiedzi na zapytanie o kontrolery domeny na poziomie domeny.

Konfiguracja taka może doprowadzić do sytuacji, gdzie w przypadku braku lokalnego kontrolera domeny w danej lokacji, klient nie jest obsługiwany przez kontrolery domeny z lokacji centralnej lecz przez inny kontroler domeny z lokacji oddziałowej (*branch office*).

Jeżeli wymagane jest zapewnienie odpowiedniej rejestracji rekordów DNS dla usługi katalogowej, tak aby uzyskać optymalne wyniki rezultatów poszukiwania kontrolerów domeny w scenariuszu Branch Office należy skonfigurować następujące ustawienia rejestracji rekordów DNS:

- Dla lokalizacji centralnych (hub, data center) pozostawić domyślne ustawienia rekordów DNS przez usługę netlogon.
- Dla lokalizacji oddziałowych\ satelickich (branch office) należy ograniczyć konfigurację rekordów w usłudze DNS tylko do rekordów specyficznych dla danej lokacji.
- Dla lokalizacji oddziałowych \ satelickich (branch office) należy wyłączyć rejestrację rekordów NS przez kontrolery domeny.

Przy konfiguracji rekordów DNS rejestrowanych przez poszczególne kontrolery domeny poprzez GPO lub wpis w rejestrze kontrolera domeny należy posługiwać się mnemonikami zdefiniowanymi dla poszczególnych rekordów DNS. Poniższa tabela przedstawia listę mnemoników zdefiniowanych dla usługi DNS.

Mnemonic	Typ	Rekord DNS
Dc	SRV	_ldap._tcp.dc._msdcs.<DnsDomainName>
DcAtSite	SRV	_ldap._tcp.<SiteName>._sites.dc._msdcs.<DnsDomainName>
DcByGuid	SRV	_ldap._tcp.<DomainGuid>.domains._msdcs.<DnsForestName>
Pdc	SRV	_ldap._tcp.pdc._msdcs.<DnsDomainName>
Gc	SRV	_ldap._tcp.gc._msdcs.<DnsForestName>
GcAtSite	SRV	_ldap._tcp.<SiteName>._sites.gc._msdcs.<DnsForestName>
GenericGc	SRV	_gc._tcp.<DnsForestName>
GenericGcAtSite	SRV	_gc._tcp.<SiteName>._sites.<DnsForestName>
GclpAddress	A	_gc._msdcs.<DnsForestName>
DsaCname	CNAME	<DsaGuid>._msdcs.<DnsForestName>
Kdc	SRV	_kerberos._tcp.dc._msdcs.<DnsDomainName>
KdcAtSite	SRV	_kerberos._tcp.dc._msdcs.<SiteName>._sites.<DnsDomainName>

Ldap	SRV	_ldap._tcp.<DnsDomainName>
LdapAtSite	SRV	_ldap._tcp.<SiteName>._sites.<DnsDomainName>
LdapIpAddress	A	<DnsDomainName>
Rfc1510Kdc	SRV	_kerberos._tcp.<DnsDomainName>
Rfc1510KdcAtSite	SRV	_kerberos._tcp.<SiteName>._sites.<DnsDomainName>
Rfc1510UdpKdc	SRV	_kerberos._udp.<DnsDomainName>
Rfc1510Kpwd	SRV	_kpasswd._tcp.<DnsDomainName>
Rfc1510UdpKpwd	SRV	_kpasswd._udp.<DnsDomainName>

Konfiguracja wykluczeń rekordów rejestrowanych przez dany kontroler domeny realizowana jest przez ustawienia GPO obejmującego kontroler domeny w sekcji Computer Configuration\Administrative Templates\System\Net Logon\DC Locator DNS Records,

ustawienie DC Locator DNS records not registered by the DCs.

W ramach tego ustawienia należy po włączeniu tej opcji GPO (*Enabled*) jako wartość podać rozdzielone przecinkami listę mnemoników, które nie powinny być rejestrowane przez kontrolery domeny w lokacjach oddziałowych. Lista mnemoników, które należy wykluczyć dla kontrolerów domeny w lokacjach oddziałowych obejmuje:

- Dc
- DcByGuid
- Gc
- GclpAddress
- GenericGc
- Kdc
- Ldap
- LdapIpAddress
- Rfc1510Kdc
- Rfc1510Kpwd
- Rfc1510UdpKdc
- Rfc1510UdpKpwd

## DOSTĘP DO DANYCH DNS Z POZIOMU LDAP

Dane usługi DNS zintegrowanej z usługą katalogową przechowywane są w ramach odpowiedniej partycji aplikacyjnej usługi katalogowej.

Każda ze stref usługi katalogowej zintegrowana z usługą katalogową reprezentowana jest przez obiekt klasy **DNS-Zone**. Obiekt ten przechowuje atrybuty danej strefy usługi katalogowej oraz stanowi kontener, w ramach którego możliwe jest tworzenie obiektów, reprezentujących poszczególne wpisy w ramach strefy DNS.

Wpisy w ramach strefy DNS reprezentowane są przez obiekty klasy **dnsNode**. Każdy rekord DNS tworzony w ramach strefy DNS zintegrowanej z usługą katalogową przechowuje dane dotyczące tego rekordu w ramach binarnej struktury danych w atrybucie dnsRecord.

W ramach struktury danych przechowywanej w tym atrybucie występują następujące znaczące pola

Pole	Długość (abajty)	Opis
Rdata length	2	Długość danych w polu Rdata
Type	2	Typ rekordu
Nieopisane	4	Nieopisane
UpdatedAtSerial	4	Wartość odpowiadająca polu serial w ramach rekordu SOA
TTL	4	Czas życia rekordu (Time To Live)
Nieopisane	4	Zawsze wartość 0
TimeStamp	4	Znacznik czasowy obiektu
Rdata	Zmienne	Dane rekordu DNS

Pole Rdata zawiera informacje o rekordzie DNS, które zależą od typu rekordu. Poniżej przedstawiony został opis danych rekordu dla poszczególnych typów rekordów DNS.

### A

Dane rekordu A zawierają tylko informację o adresie IP w postaci 32-bitowego pola danych, gdzie każdy bajt oznacza jeden oktet adresu IP.

```

1          1   1   1   1   1   1
2     0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
3 +-----+-----+-----+-----+-----+-----+-----+-----+
4 |           DATA           |
5 |           |
6 +-----+-----+-----+-----+-----+-----+-----+-----+

```

### **CNAME and NS**

```

01          1   1   1   1   1   1
02     0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
03 +-----+-----+-----+-----+-----+-----+-----+-----+
04 |       LENGTH      |   NUMBER OF LABELS   |
05 +-----+-----+-----+-----+-----+-----+-----+-----+
06 |       LABEL LENGTH    |           |
07 |-----+-----+-----+-----+-----+-----+-----+-----+
08 /           DATA           /
09 /           /
10 +-----+-----+-----+-----+-----+-----+-----+-----+

```

### **MX**

```

01          1   1   1   1   1   1
02     0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
03 +-----+-----+-----+-----+-----+-----+-----+-----+
04 |           PRIORITY        |
05 +-----+-----+-----+-----+-----+-----+-----+-----+
06 |       LENGTH      |   NUMBER OF LABELS   |
07 +-----+-----+-----+-----+-----+-----+-----+-----+
08 |       LABEL LENGTH    |           |
09 |-----+-----+-----+-----+-----+-----+-----+-----+
10 /           DATA           /
11 /           /
12 +-----+-----+-----+-----+-----+-----+-----+-----+

```

## SOA

```
01          1 1 1 1 1  
02 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5  
03 +-----+-----+-----+-----+-----+  
04 |           SERIAL           |  
05 |                           |  
06 +-----+-----+-----+-----+-----+  
07 |           REFRESH          |  
08 |                           |  
09 +-----+-----+-----+-----+-----+  
10 |           RETRY            |  
11 |                           |  
12 +-----+-----+-----+-----+-----+  
13 |           EXPIRE           |  
14 |                           |  
15 +-----+-----+-----+-----+-----+  
16 |           MINIMUM TTL     |  
17 |                           |  
18 +-----+-----+-----+-----+-----+  
19 |           LENGTH           | NUMBER OF LABELS |  
20 +-----+-----+-----+-----+-----+  
21 |           LABEL LENGTH     |  
22 +-----+-----+-----+  
23 /           DATA             /  
24 /                           /  
25 +-----+-----+-----+-----+-----+  
26 |           LENGTH           | NUMBER OF LABELS |  
27 +-----+-----+-----+-----+-----+  
28 |           LABEL LENGTH     |  
29 +-----+-----+-----+  
30 /           RESPONSIBLE PERSON /  
31 /                           /  
32 +-----+-----+-----+-----+-----+
```

## SRV

```
01          1 1 1 1 1  
02 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5  
03 +-----+-----+-----+-----+-----+  
04 |           PRIORITY          |  
05 +-----+-----+-----+-----+-----+  
06 |           WEIGHT            |  
07 +-----+-----+-----+-----+-----+  
08 |           PORT              |  
09 +-----+-----+-----+-----+-----+  
10 |           LENGTH           | NUMBER OF LABELS |  
11 +-----+-----+-----+-----+-----+  
12 |           LABEL LENGTH     |  
13 +-----+-----+-----+  
14 /           DATA             /  
15 /                           /  
16 +-----+-----+-----+-----+-----+
```

## **TXT**

```
1          1   1   1   1   1  
2      0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5  
3  +---+---+---+---+---+---+---+---+---+---+---+---+---+---+  
4  |       LENGTH           |           |  
5  |---+---+---+---+---+---+  
6  /           DATA           /  
7  /           /           /  
8  +---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

## KOPIE ZAPASOWE I ODZYSKWIANIE DANYCH DNS

Usługa DNS w systemie Windows Server ma możliwość przechowywania danych stref DNS w ramach usługi katalogowej, jako strefy zintegrowane z Active Directory (*AD integrated zone*).

Dane strefy DNS zintegrowanej z usługą katalogową przechowywane są w ramach danych usługi Active Directory, dzięki czemu zapewniona jest ich wysoka dostępność i odporność usługi na awarię (dane na wielu kontrolerach domeny udostępniających usługę DNS) oraz możliwe jest skorzystanie z dodatkowych mechanizmów systemu – na przykład bezpiecznych aktualnień DNS wymagających uwierzytelnienia w usłudze katalogowej.

Z punktu widzenia zabezpieczenia kopii zapasowych danych stref DNS zintegrowanych z usługą katalogową i procesu ich odtworzenia wymagane jest zapewnienie kopii danych usługi katalogowej analogicznie jak w przypadku zabezpieczenia kopii innych danych przechowywanych w Active Directory.

W celu zapewnienia kopii zapasowej danych wszystkich wymaganych stref usługi DNS w środowisku usługi katalogowej, w szczególności w środowiskach lasu Active Directory z wieloma domenami, należy zapewnić kopię zapasową danych usługi katalogowej przynajmniej jednego kontrolera domeny, utrzymującego każdą ze stref DNS. Należy w tym wypadku pamiętać o tym, że strefy usługi DNS w ramach usługi katalogowej mogą być replikowane:

- do wszystkich kontrolerów domeny dla danej domeny usługi katalogowej.
- do wszystkich kontrolerów domeny w ramach danego lasu usługi katalogowej.

W zależności od zakresu replikacji danych stref DNS pomiędzy kontrolerami domeny należy zaplanować odpowiednio wykonanie kopii zapasowej danych usługi katalogowej dla wszystkich kontrolerów domeny, tak aby dostępny był pełny zestaw danych stref DNS.

Odtworzenie danych strefy DNS w przypadku skorzystania z kopii danych usługi katalogowej przeprowadzane jest w sposób analogiczny, jak w przypadku odtworzenia obiektów usługi katalogowej.

## **Awaryjna kopia w ramach strefy zapasowej**

Alternatywnym podejściem w zakresie zapewnienia kopii zapasowej danych stref DNS jest wykorzystanie replikacji stref DNS pomiędzy serwerami usługi w sposób standardowy zgodnie z mechanizmami DNS.

Utworzenie standardowej strefy (niezintegrowanej z Active Directory) zapasowej na dodatkowym serwerze pełniącym rolę serwera DNS zapewnia kopię danych danej strefy DNS niezależną od mechanizmów usługi katalogowej. Dane pochodzące ze stref standardowych, mogą być użyte w przypadku konieczności odtworzenia całej strefy DNS zintegrowanej z usługą katalogową.

Informacje stref standardowych, w odróżnieniu od stref zintegrowanych z usługą katalogową nie są przechowywane w ramach danych katalogu Active Directory, lecz w postaci plików na lokalnym systemie plików każdego serwera DNS utrzymującego daną strefę.

Dane każdej ze stref przechowywane są w pliku odpowiadającym nazwie tej strefy.

Alternatywną metodą wykonania kopii zapasowej strefy DNS w postaci pliku danych strefy DNS jest wyeksportowanie danych strefy do pliku tekstowego:

```
DNSCMD /ZoneExport <nazwa strefy DNS> <nazwa pliku kopii zapasowej>
```

### **Lokalizacja plików usługi DNS**

Pliki standardowych stref DNS jak i pliki eksporty przechowywane są domyślnie w następującej lokacji:  
%systemroot%\system32\dns

## **Rekordy statyczne vs dynamiczne**

W ramach stref DNS tworzone są dwa typy rekordów:

- **Dynamiczne (Dynamic)**

Rekordy dynamiczne rejestrowane są przez usługi, stacje robocze i serwery dynamicznie przy starcie lub uruchomieniu usługi lub systemu. W przypadku utraty rekordy tego typu można odtworzyć poprzez ponowne wymuszenie ich rejestracji w ramach usługi DNS, na przykład uruchamiając ponownie usługę \ system.

- **Statyczne(Static)**

Rekordy statyczne rejestrowane są poprzez administratora usługi DNS w sposób ręczny.

Rekordy tego typu nie zostaną odtworzone samoczynnie po uruchomieniu usługi lub systemu i w celu ich odtworzenia konieczne jest ich ponowne zarejestrowanie w ramach usługi.

Z punktu widzenia zagadnienia odtworzenia danych usługi DNS każdy z typów rekordów stanowi oddzielne zagadnienie związane z zapewnieniem możliwości jego odzyskania.

W przypadku usunięcia pojedynczego rekordu dynamicznego lub grupy rekordów najprostszym sposobem ich odzyskania jest wymuszenie ich ponownej rejestracji poprzez odpowiednie narzędzie lub ponowne uruchomienie usługi \ systemu.

W przypadku usunięcia rekordów stacji roboczych lub serwerów, rekordy te zostaną ponownie zarejestrowane w trakcie następnego restartu systemu.

W przypadku usług działających w systemie rejestrujących dynamicznie rekordy DNS możliwe jest ich ponowne zarejestrowanie poprzez restart usługi lub odpowiednie narzędzie. Przykładem usługi dynamicznie rejestrującej rekordy DNS jest usługa NETLOGON działająca na kontrolerze domeny.

W przypadku utraty rekordu statycznego w ramach usługi DNS odzyskanie go możliwe jest poprzez:

- Odtworzenie danych rekordu z kopii zapasowej
- Ponowne zarejestrowanie rekordu w ramach usługi.

Najprostszą metodą odtworzenia rekordu statycznego jest jego ponowne zarejestrowanie w ramach usługi DNS. W tym celu należy posiadać informację o wszystkich rekordach statycznych, które są rejestrowane statycznie w ramach poszczególnych stref DNS w postaci źródłowej. Źródłem takiej informacji może być skrypt zawierający polecenia rejestracji poszczególnych rekordów w postaci:

```
DNSCMD /RecordAdd <nazwa strefy> <nazwa węzła> <typ rekordu> <adres>
```