

WINDOWS SERVER ADVANCED

Replication

Replication?

Wat is replicatie?

- Synchroniseren van de AD database
 - Bij toevoegingen, aanpassingen en verwijderen van een object
 - Enkel gewijzigde attributen worden doorgestuurd
- Multimaster
 - Elke DC kan schrijven naar de domeinpartitie
- Vanaf 2^{de} DC en verder

Componenten binnen replicatie

- **MULTIMASTER REPLICATION**

- Uitleg: Elke DC kan 'originating updates' ontvangen
- Voordeel: fout tolerantie, niet langer 1 DC verantwoordelijk voor directory taken

- **PULL REPLICATION**

- Uitleg: DC's vragen (pull) wijzigingen (enkel wat ze nodig hebben) i.t.t. tot ze sturen (push). Bij een wijziging informeert een DC z'n partners.
- Voordeel: Dit vermijdt onnodig netwerkverkeer

- **STORE-AND-FORWARD REPLICATION**

- Uitleg: Elke DC communiceert met een set van andere DC's i.p.v. met alle DC's
- Voordeel: De replicatie last wordt verdeeld over meerdere DC's

- **STATE-BASED REPLICATION**

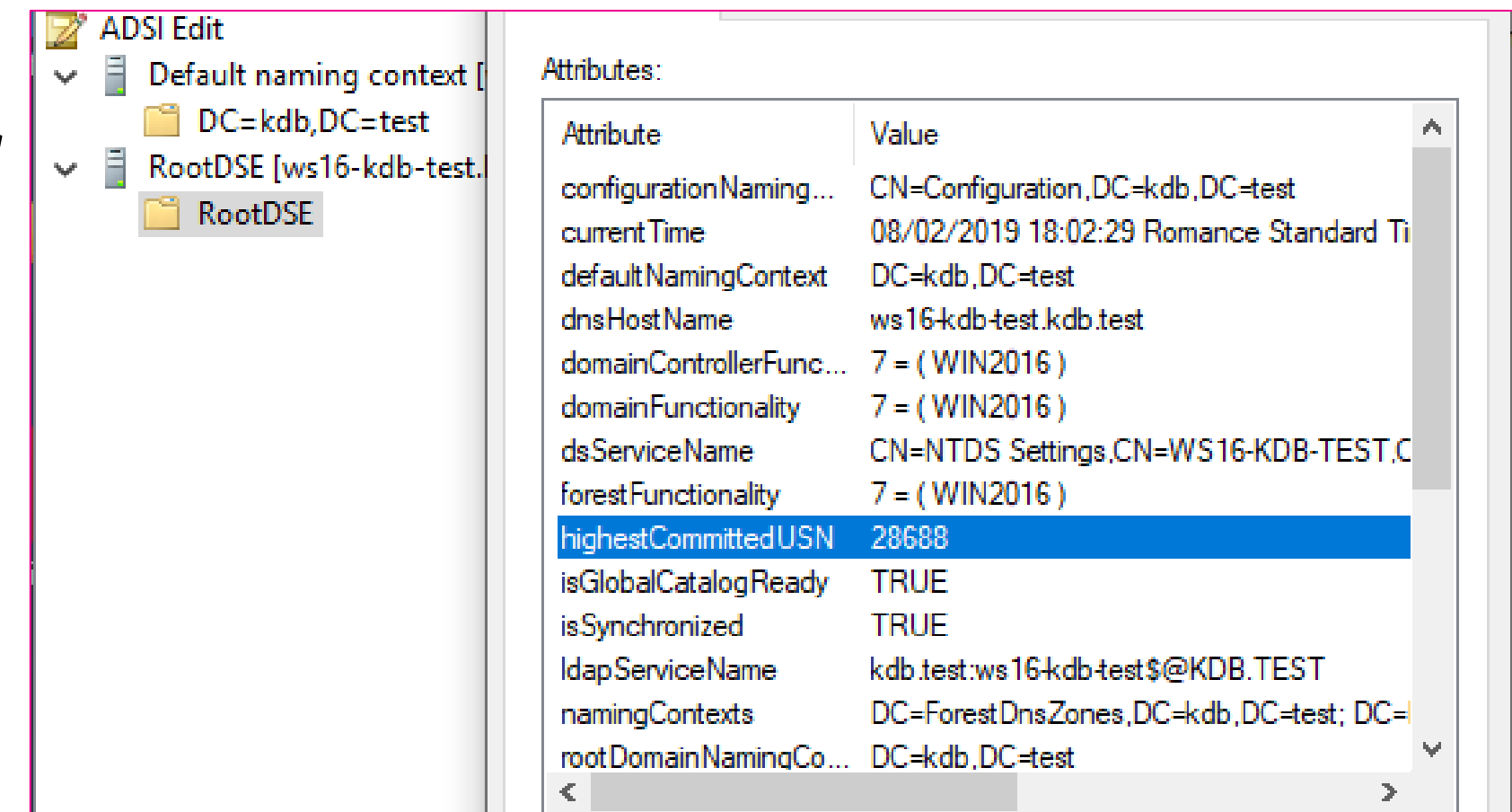
- Uitleg: Elke DC houdt replicatie update bij (zijn state) en vergelijkt met andere DC's
- Voordeel: Conflicten en onnodige replicatie worden verminderd

Convergentie

- Alle objecten hebben gelijke waarden voor alle attributen
- Zal plaatsvinden na een bepaalde tijd (of latency)
- In tussentijd kan er een verschil zitten tussen de databases = *loose consistency*

Update Sequence Number (USN) (1/2)

- USN = 64 –bit nummer en per wijziging (transactie) ingesteld
 - Bijvoorbeeld: DC A heeft USN 1000, 10 minuten later is z'n USN 1056 => in de laatste 10 minuten zijn 56 transacties gebeurd
- Elke DC heeft z'n eigen USN nummering dat onafhankelijk is van een andere DC
- Huidige USN staat in ***highestCommittedUSN*** van het *rootDSE* object van de DC
- USN gaat **enkel** vooruit!



ADSI Edit

Default naming context [...]

DC=kdb,DC=test

RootDSE [ws16-kdb-test. ...]

RootDSE

Attributes:

Attribute	Value
configurationNaming...	CN=Configuration,DC=kdb,DC=test
currentTime	08/02/2019 18:02:29 Romance Standard Ti
defaultNamingContext	DC=kdb,DC=test
dnsHostName	ws16-kdb-test.kdb.test
domainControllerFunc...	7 = (WIN2016)
domainFunctionality	7 = (WIN2016)
dsServiceName	CN=NTDS Settings,CN=WS16-KDB-TEST,C
forestFunctionality	7 = (WIN2016)
highestCommittedUSN	28688
isGlobalCatalogReady	TRUE
isSynchronized	TRUE
ldapServiceName	kdb.test:ws16-kdb-test\$@KDB.TEST
namingContexts	DC=ForestDnsZones,DC=kdb,DC=test; DC=
rootDomainNamingCo...	DC=kdb,DC=test

Update Sequence Number (USN) (2/2)

- Elk object heeft ook volgende attributen
 - USN wanneer object gemaakt werd: **usnCreated**
 - USN wanneer object laatste maal gewijzigd werd: **usnChanged**
- Elk attribuut van een object houdt metadata bij waaronder
 - De USN van de DC op moment dat de wijziging voor dit attribuut heeft plaatsgevonden: **Local USN**
 - De USN van waar de wijziging heeft plaatsgevonden: **Originating USN**
 - Deze zaken behoren tot de “**stamp**”
 - Dient om conflicten op te lossen -> cfr Zegel

pwdProperties	0x1 = (COMPLEX)
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
replUpToDateVector	\02\00\00\00\00\00\00\00\01\00\00\00\
ridManagerReference	CN=RID Manager\$,CN=System,DC=kdb,DC=
serverState	1
subRefs	DC=ForestDnsZones,DC=kdb,DC=test; DC=
systemFlags	0x8C000000 = (DISALLOW_DELETE DOM
uASCompat	1
usnChanged	61454
usnCreated	4099
wellKnownObjects	B:32:6227F0AF1FC2410D8E3BB10615BB5I
whenChanged	11/04/2019 15:42:35 Romance Daylight Tin
whenCreated	01/02/2019 20:10:29 Romance Daylight Tin

Voorbeeld (1/4)

1. Replication-related Data on DC1 When a User Object is Created



DC USN: 4710 → 4711
Object uSNCreated: 4711
Object uSNChanged: 4711

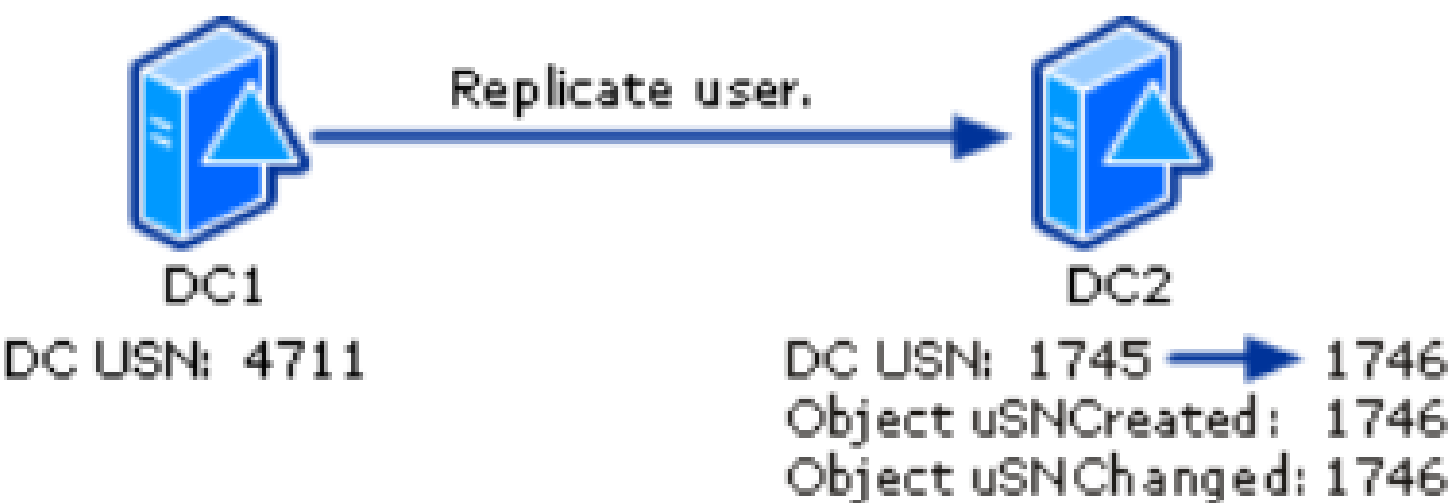
Object meta
-data

Property	Value	Local USN	Version	Originating Time	Originating DC	Originating USN
cn	Jeff Smith	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPassword	6Be8W5q-	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711
sAMAccountName	JSmith	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPrincipalName	JSmith@contoso.com	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711

STAMP

Voorbeeld (2/4)

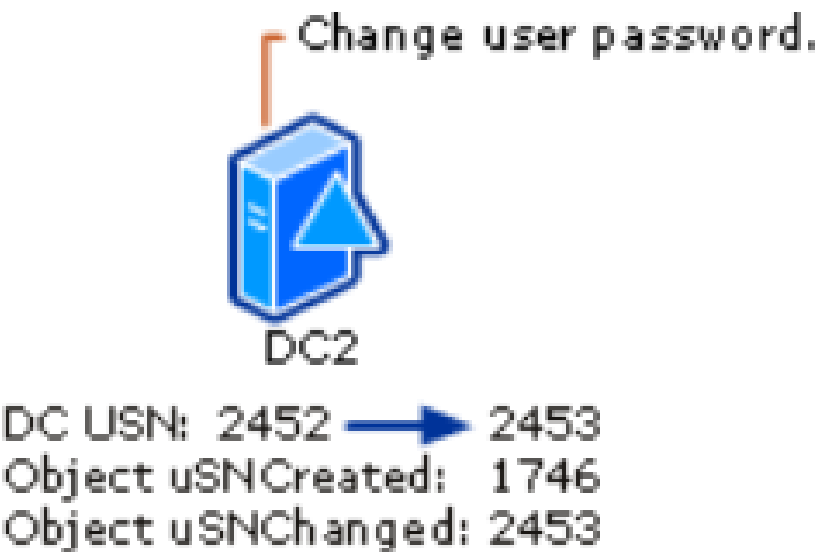
2. Replication-related Data on DC2 When a New User Object is Replicated From DC1



Property	Value	Local USN	Version	Originating Time	Originating DC	Originating USN
cn	Jeff Smith	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPassword	6Be8W5q-	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711
sAMAccountName	JSmith	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPrincipalName	JSmith@contoso.com	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711

Voorbeeld (3/4)

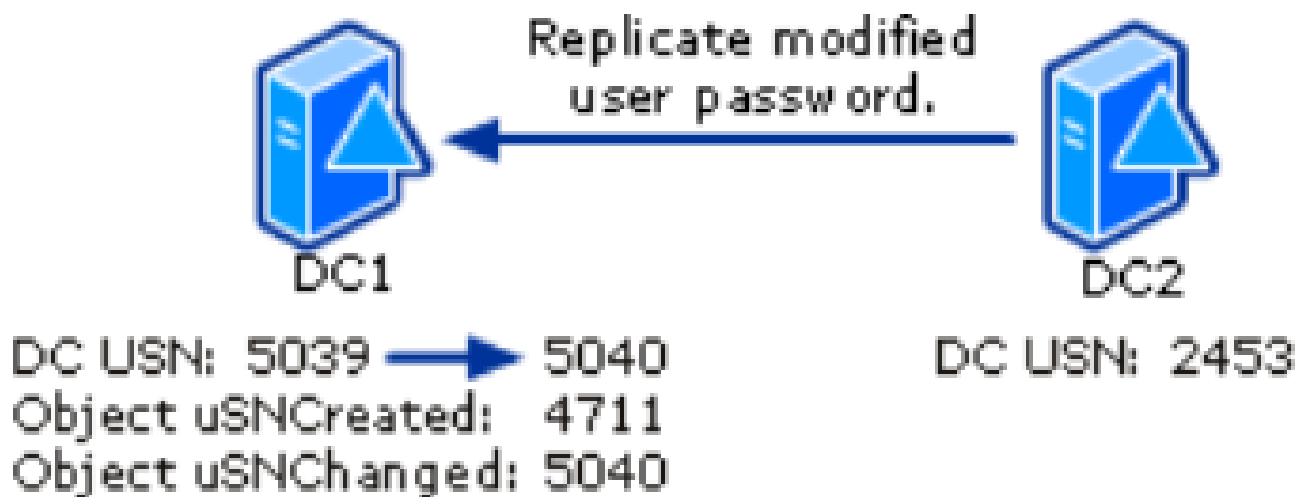
3. Replication-related Data on DC2 After the User Password Value Has Been Changed on DC2



Property	Value	Local USN	Version	Originating Time	Originating DC	Originating USN
cn	Jeff Smith	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPassword	sEP3569?@2	2453	2	2003-09-10 11:53.29	<DC2_GUID>	2453
sAMAccountName	JSmith	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPrincipalName	JSmith@contoso.com	1746	1	2003-09-10 10:49.03	<DC1_GUID>	4711

Voorbeeld (4/4)

4. Replication-related Data on DC1 After the Password Change Has Replicated to DC1

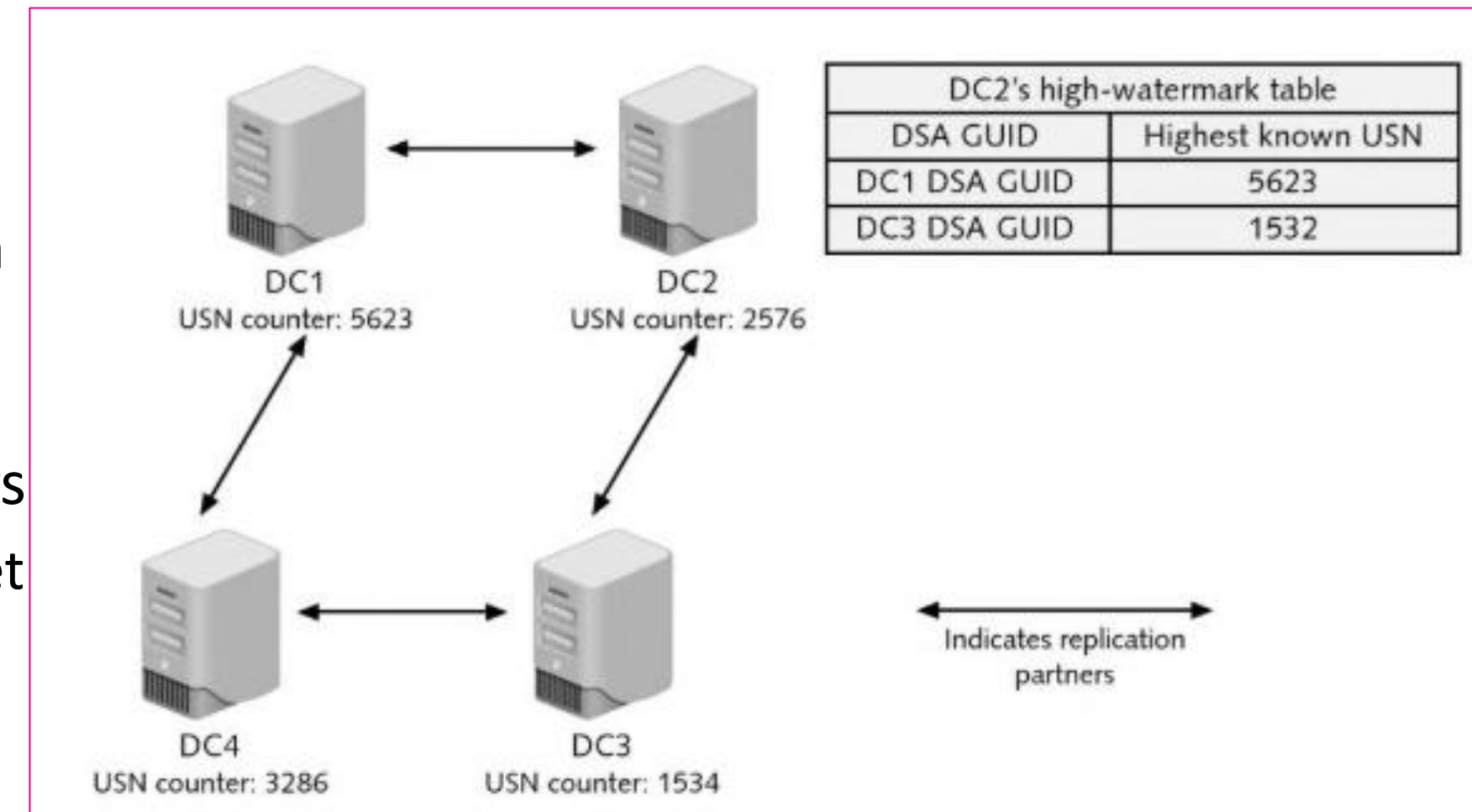


Property	Value	Local USN	Version	Originating Time	Originating DC	Originating USN
cn	Jeff Smith	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPassword	sEP3569?@2	5040	2	2003-09-10 11:53.29	<DC2_GUID>	2453
sAMAccountName	JSmith	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711
userPrincipalName	JSmith@contoso.com	4711	1	2003-09-10 10:49.03	<DC1_GUID>	4711

STAMP

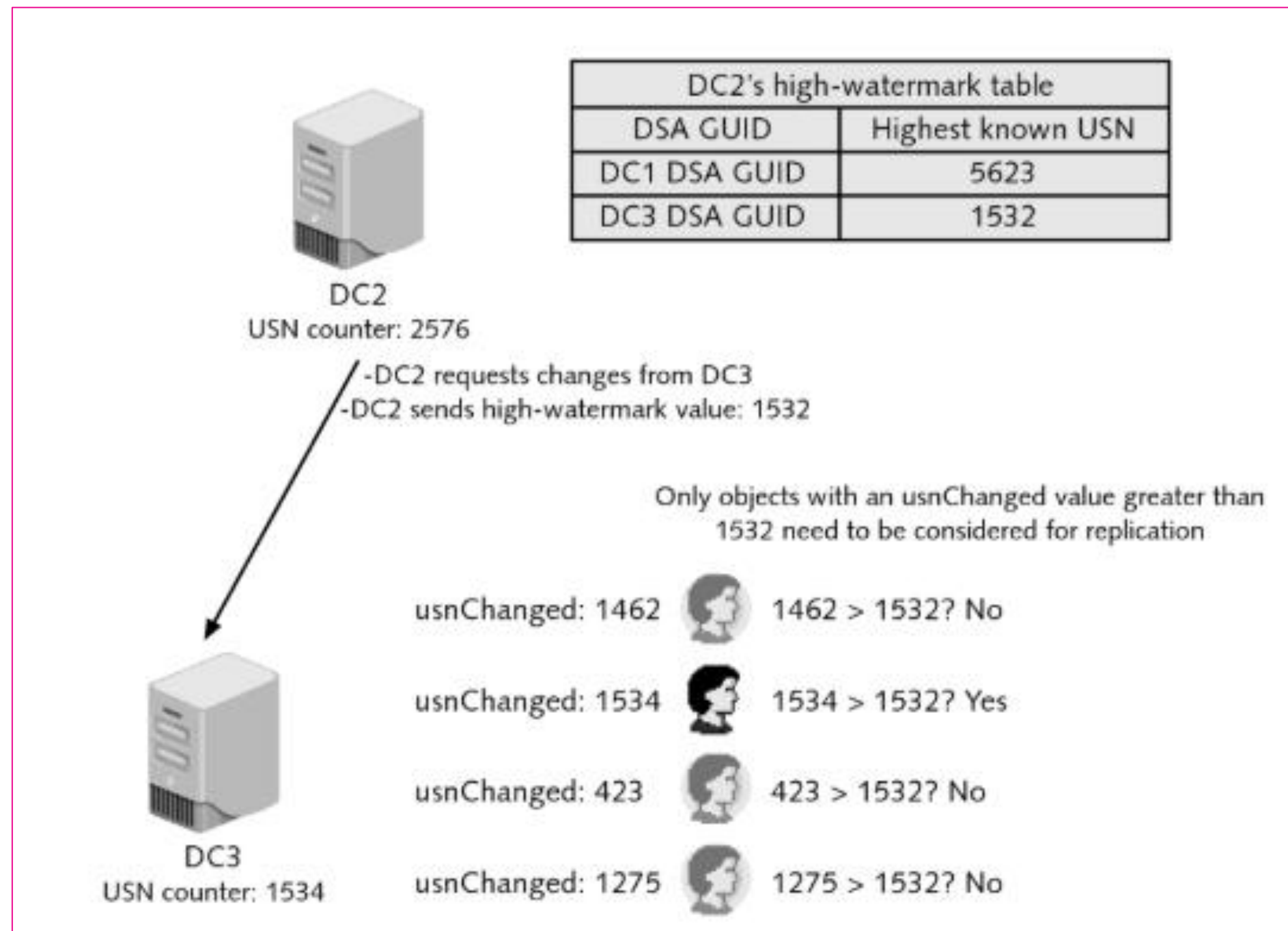
Filteren van replication requests (1/3)

- Bij een replicatie zal een Destination DC de Source DC inlichten van reeds ontvangen updates
 - Voorkomt replicaties die niet nodig zijn
- Hij doet dit via:
 - High Watermark Value (HWMV)
 - Een tabel onderhouden op ELKE DC voor elke directory partitie (minstens 3 (domain , Schema en Configuration partitie)
 - Bevat de hoogste USN van de updates verkregen van elk van z'n replicatiepartners
 - M.a.w. de High Watermark is een tabel met de laatst verkregen wijzigingen (via de hoogste usnChanged waarde) voor elke directory partitie



Filteren van replication requests (2/3)

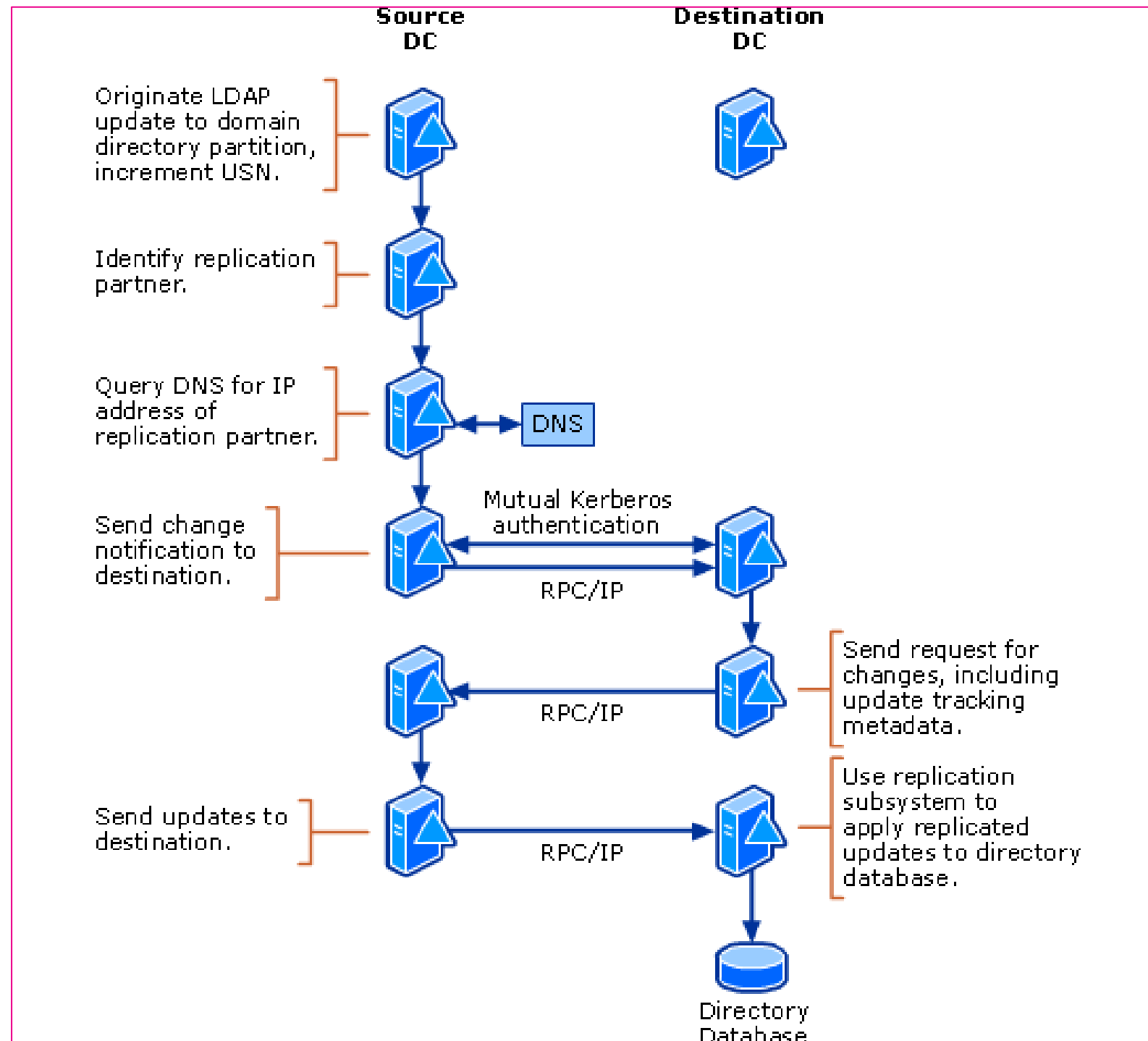
- Via de HWMV bepalen we **welke objecten** te repliceren



Filteren van replication requests (3/3)

- Up-To-Dateness vector (UTDV)
 - Een tabel onderhouden op ELKE DC voor elke DP (minstens 3)
 - Gebruikt om de **juiste (gewijzigde) attributen** te repliceren
 - Bevat de hoogste **originating USN** ontvangen van elke DC in de forest die ooit bestaan heeft alsook de datum/tijd van een laatste succesvolle replicatie
- Zowel de HWMV als de UTDV worden gebruikt om
 - Te filteren welke objecten te repliceren
 - Te filteren welke attributen van objecten te repliceren

Replicatieproces



1. Een object in de database wordt gewijzigd en het USN wordt verhoogd
2. De replicatiepartner(s) worden opgezocht in de Replication Topology
3. Het IP van de replicatiepartner(s) wordt via DNS opgevraagd
4. Er wordt via Kerberos een geauthentiseerde verbinding opgezet
5. De bron DC zendt een notificatie naar de doel DC('s) met daarin zijn hoogste USN
6. De doel DC stuurt daarop een vraag naar alle nog niet ontvangen wijzigingen
7. De bron DC stuurt de wijzigingen door
8. De doel DC schrijft alle gerepliceerde updates weg naar de database

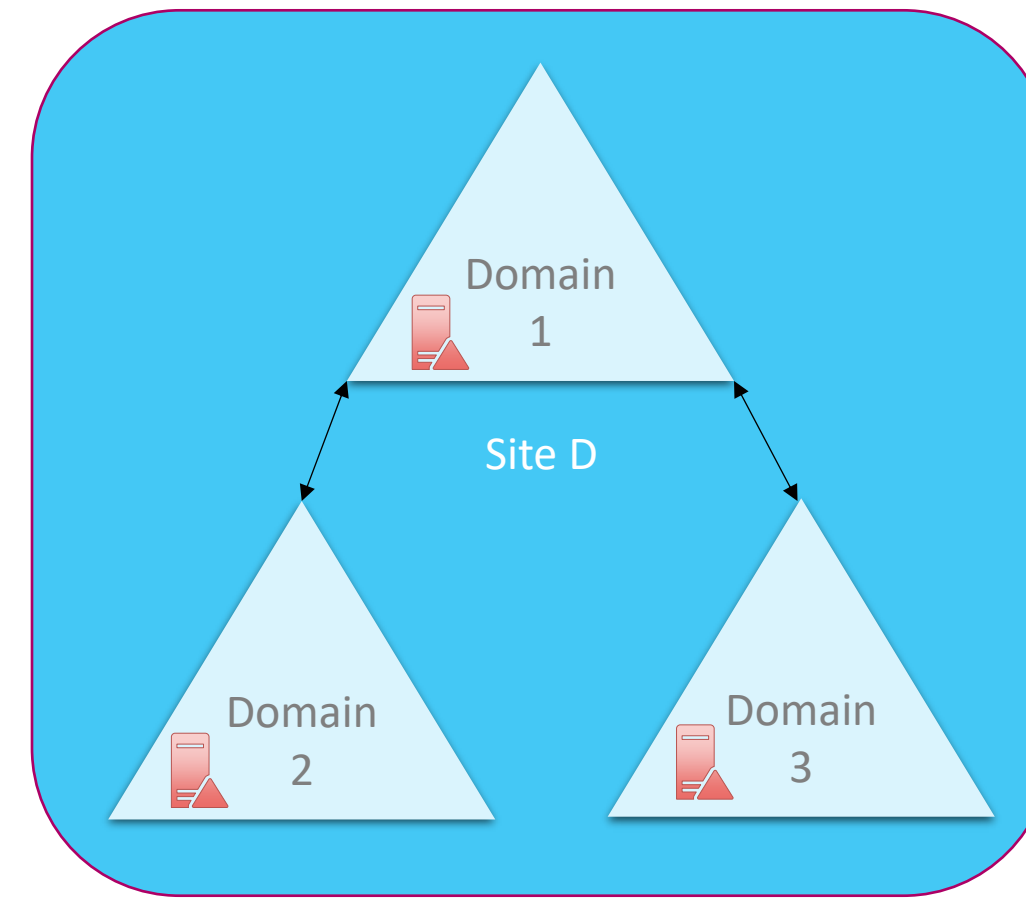
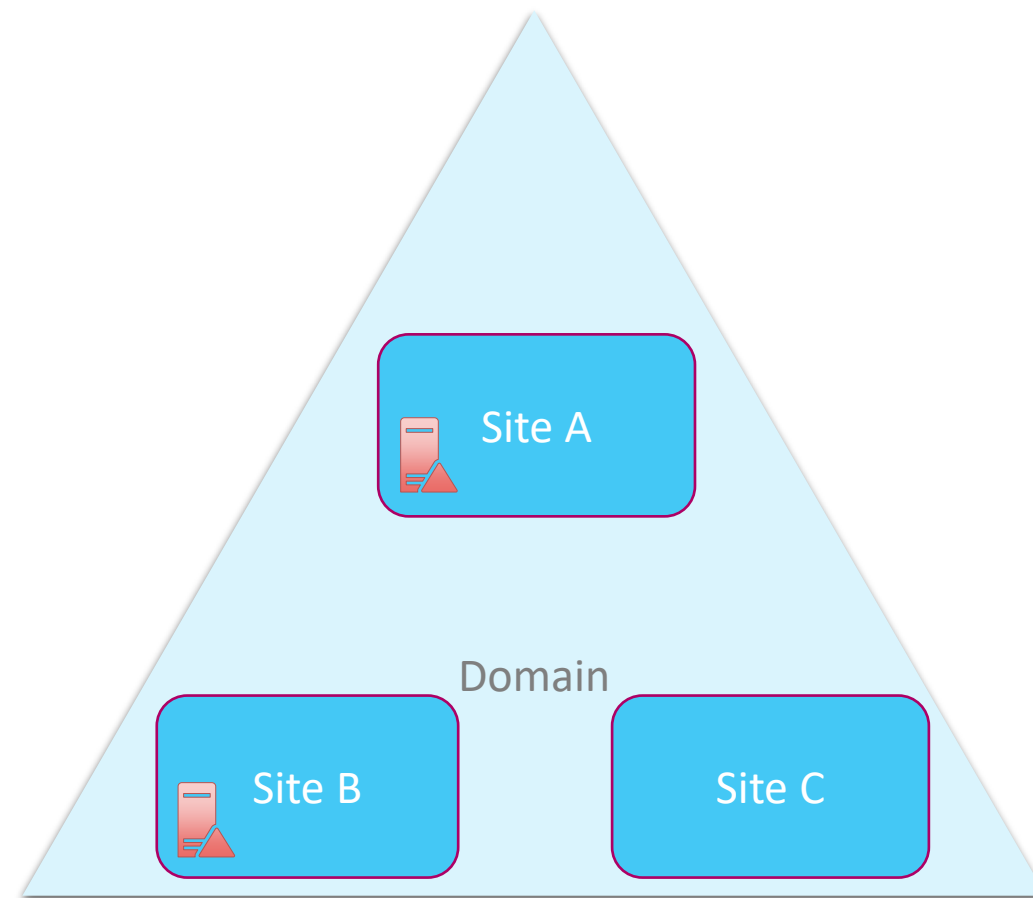
Replication Topology

Sites en Domains (1/2)

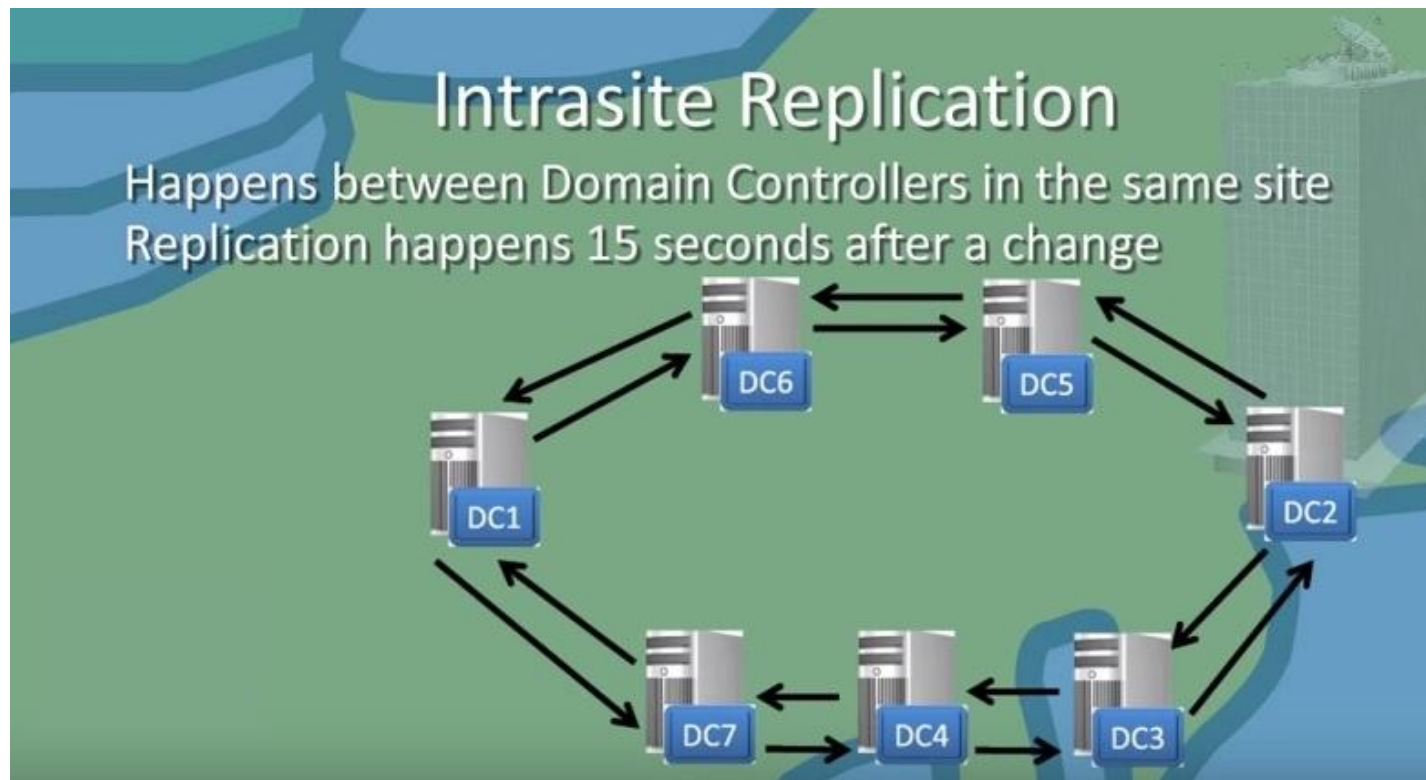
- Site bestaat uit 1 of meerdere subnetten
 - “Verzameling van goed geconnecteerde subnetten”
- Binnen site snelle verbinding tussen DC's
- Site gebruik je om logische collecties te maken waartussen je replicatieafspraken vastlegt
- Helpt clients om de dichtste bron te vinden voor bepaalde services (bv DC, GC, DFS Shares, ...)

Sites en Domains (2/2)

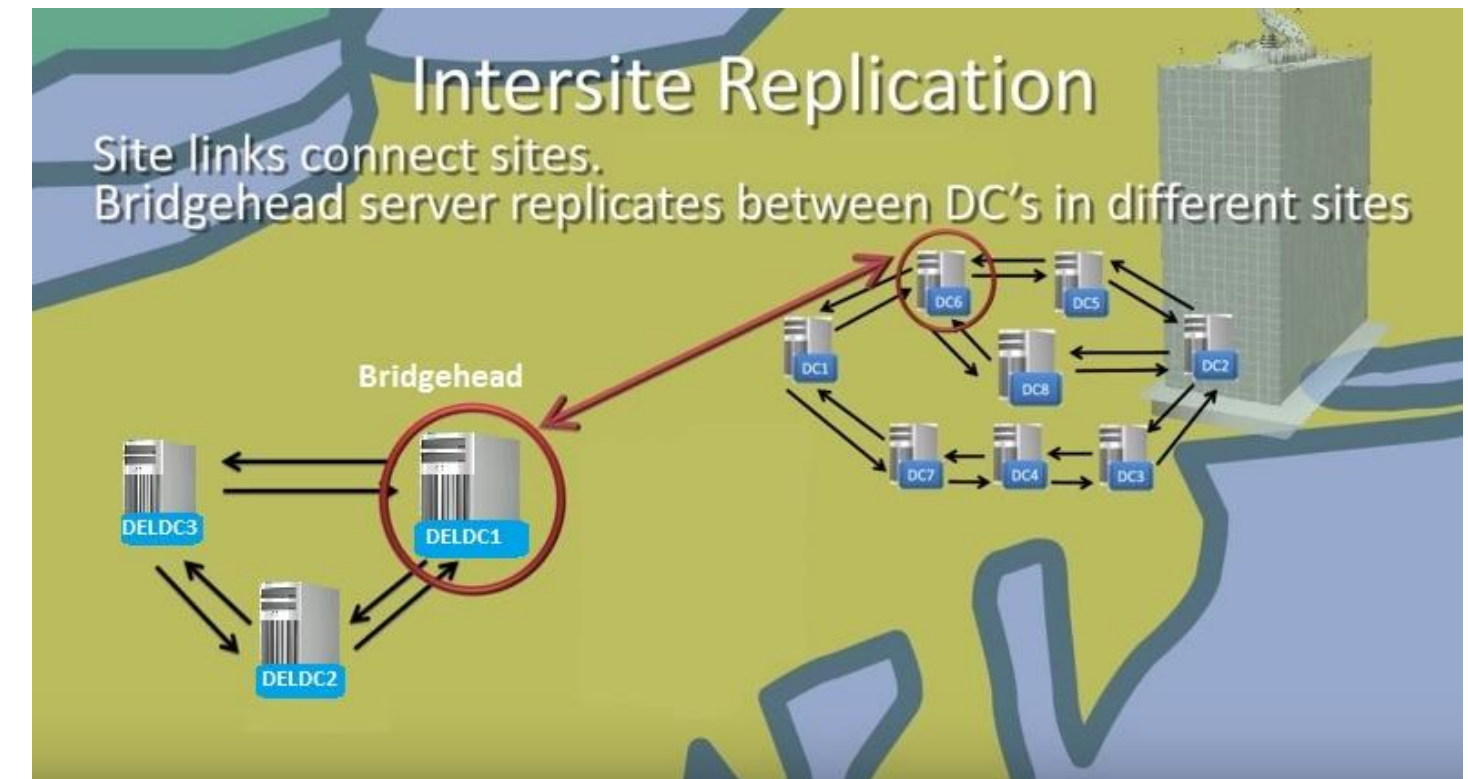
- Multiple Sites | 1 domain
- Multiple Domains | 1 site



Intersite vs intrasite

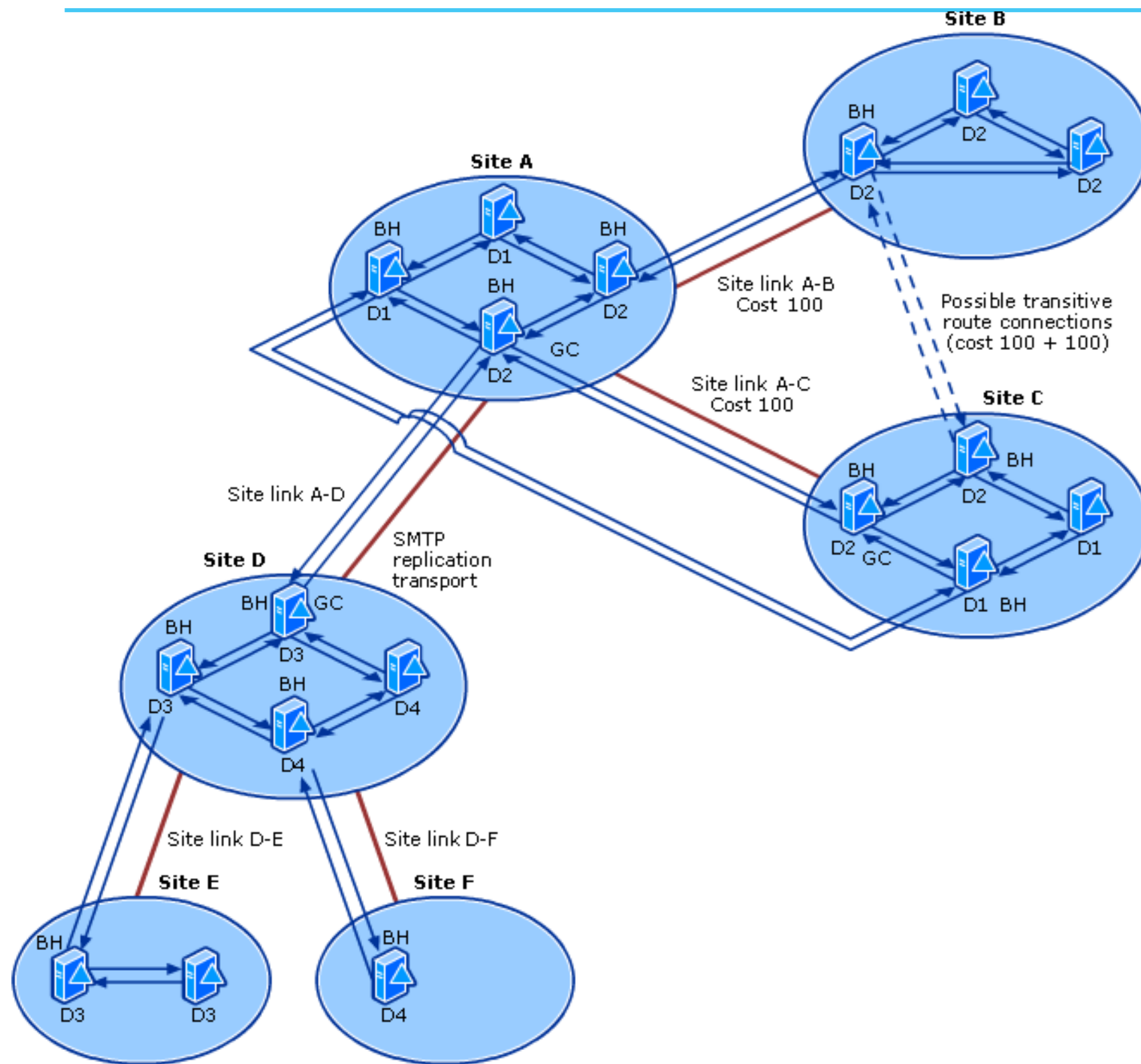


- Tussen DC's in dezelfde site
- Binnen 15 sec na wijziging
- RPC



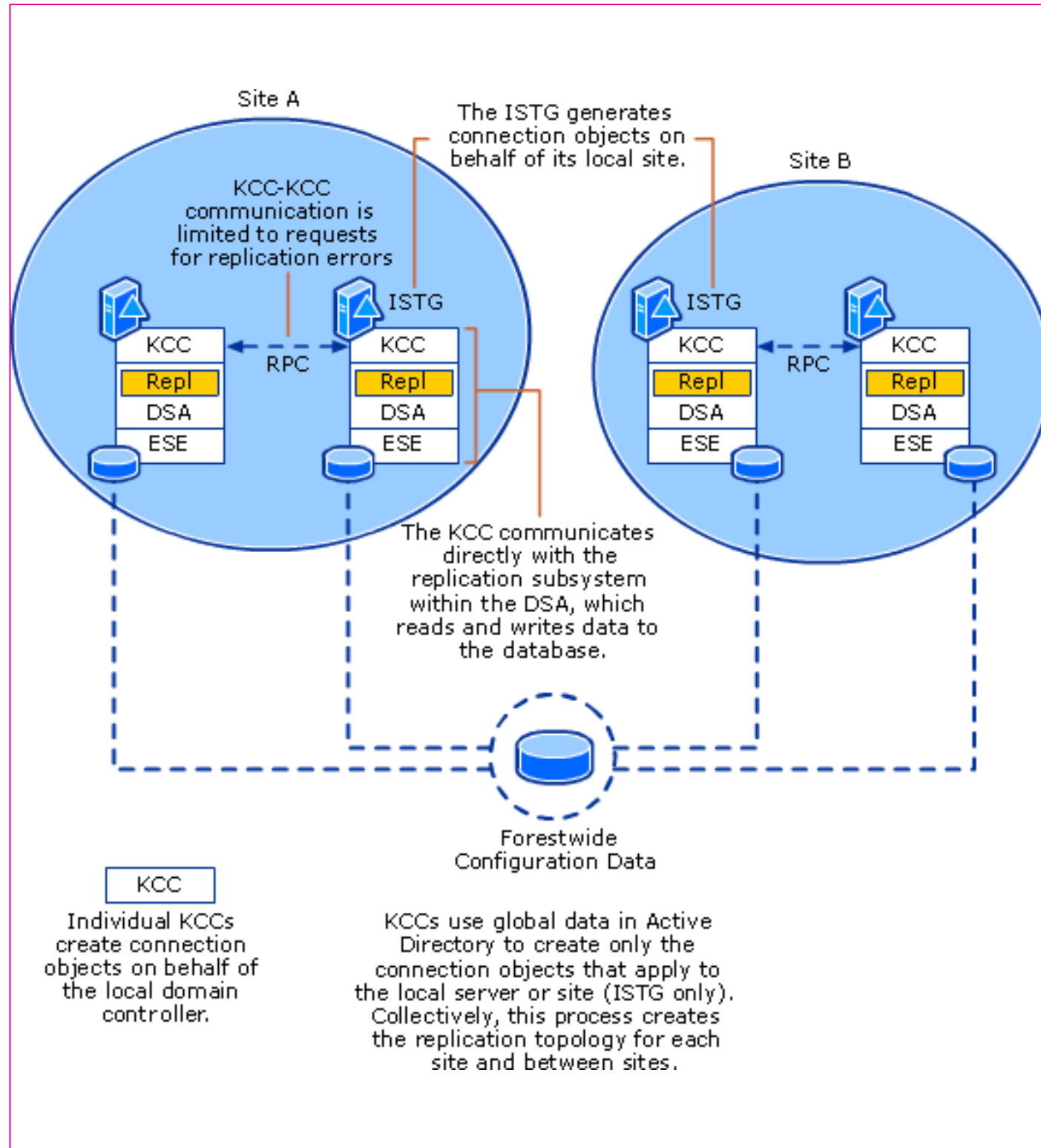
- Tussen 2 sites
- Tussen 'bridgehead' servers
- Standaard 3 uur (min. 15 min)
- RPC (of SMTP → deprecated)

Site Link



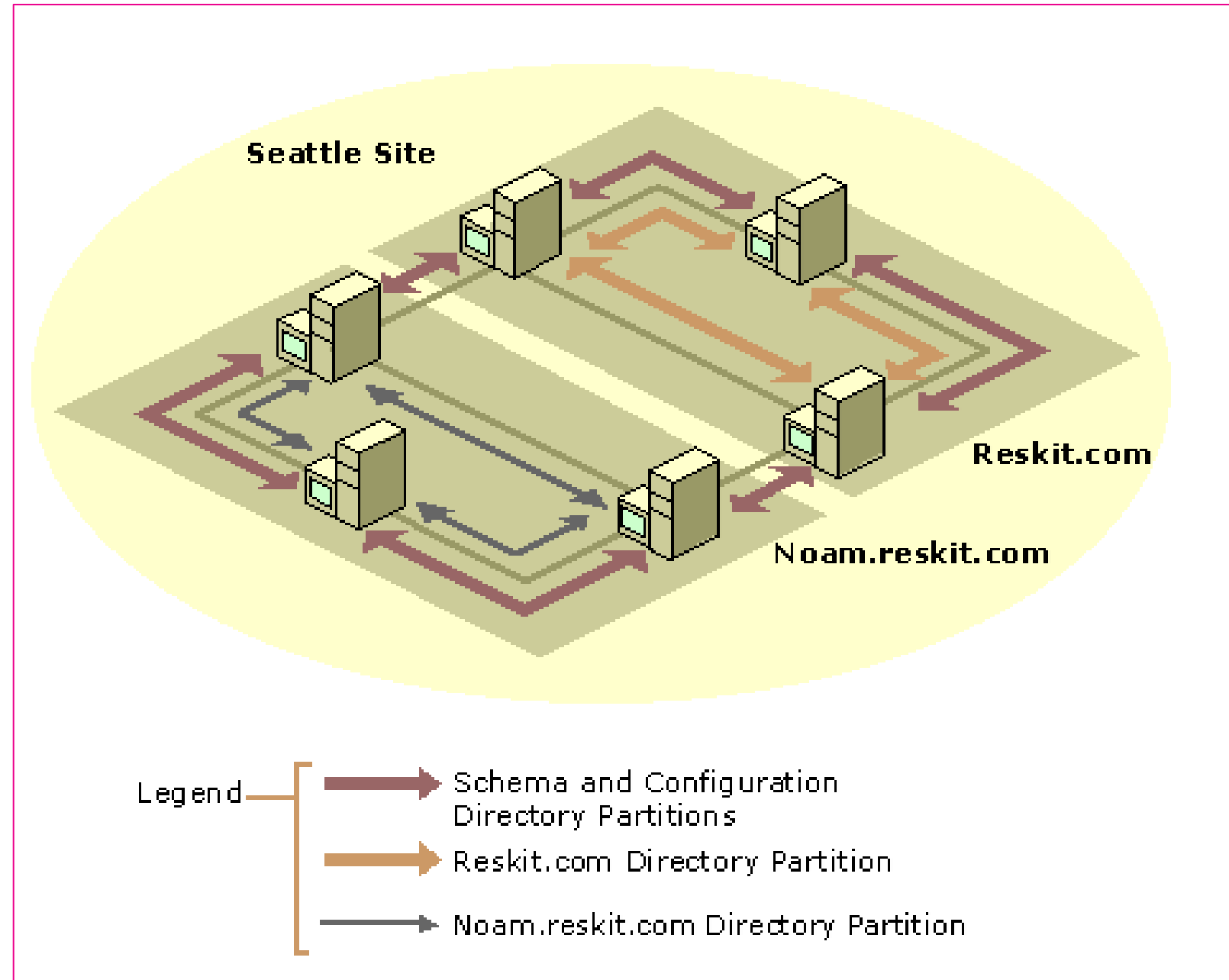
- Laten je toe te bepalen welke sites geconnecteerd zijn en wat de kost is
- **Schedule** = periode (van/tot) wanneer kan gerepliceerd worden
- **Replication period / interval** = frequentie van replicatie tijdens schedule
- **Cost** = Prioriteit
- Transport
 - **RPC** over IP
 - SMTP (deprecated)
- Te vinden onder 'AD Sites and Services -> Sites -> Inter-Site Transports -> IP

Knowledge Consistency Checker (KCC)



- Component verantwoordelijk voor genereren van de replicatie topologie tussen DC's
 - = Connection Objects
 - Intrasite en intersite
- Communiceert met de AD database [configuration partition]
 - Sites
 - Site Links
 - DC's
- Communiceren onderling enkel via RPC

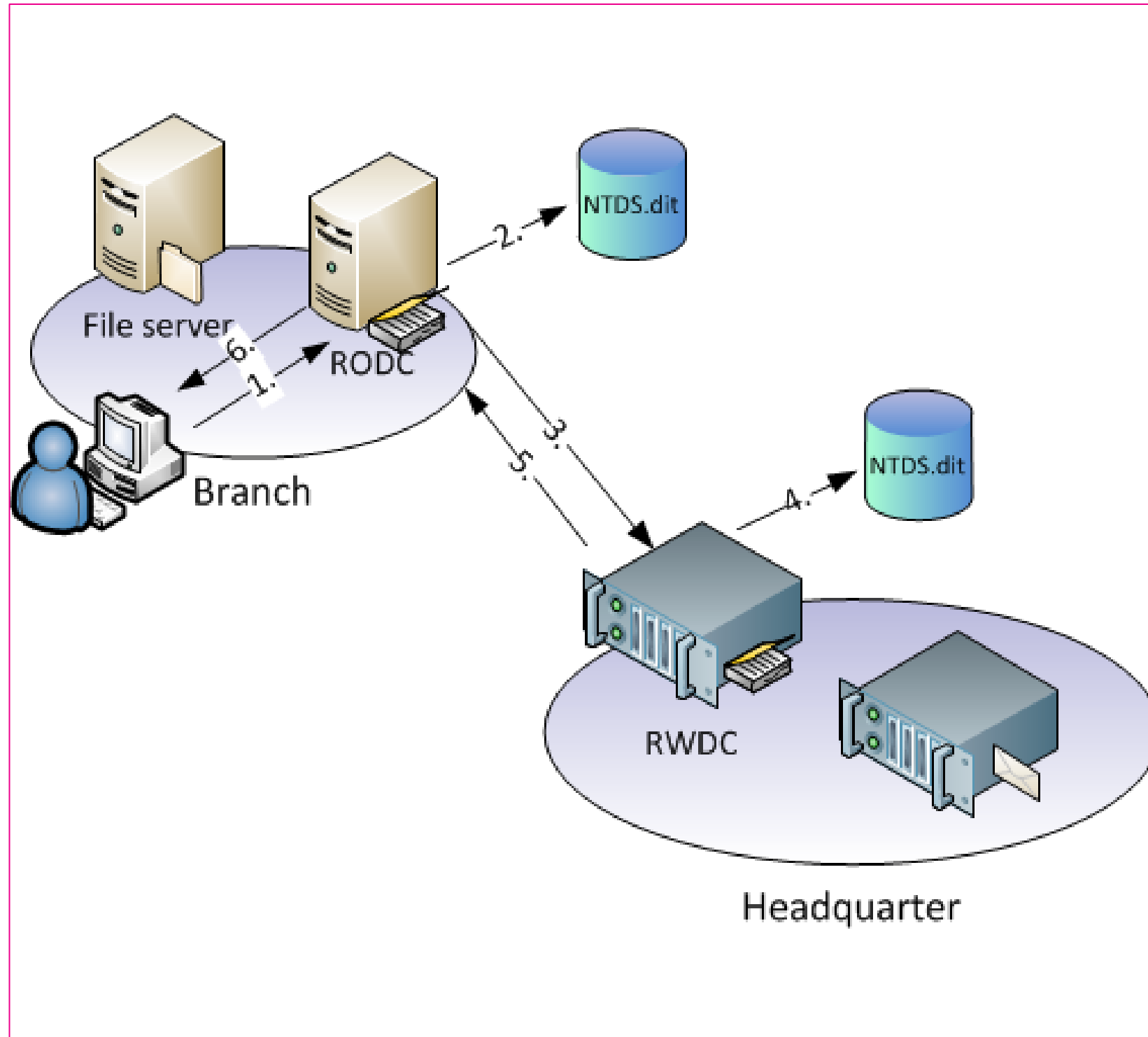
Intersite Topology Generator (ISTG)



- Onderdeel van de KCC
- Maakt de topologie aan tussen sites (meestal in ringvorm)
- Kiest de servers die intersite replicatie zullen doen (bridgehead servers)
- Op basis van de gegevens in de database
 - Sites
 - Site Links
 - DC's
- Aparte topologie voor schema/configuratie en domeinpartities zijn mogelijk

RODC

Read-Only Domain Controller (RODC) (1/2)

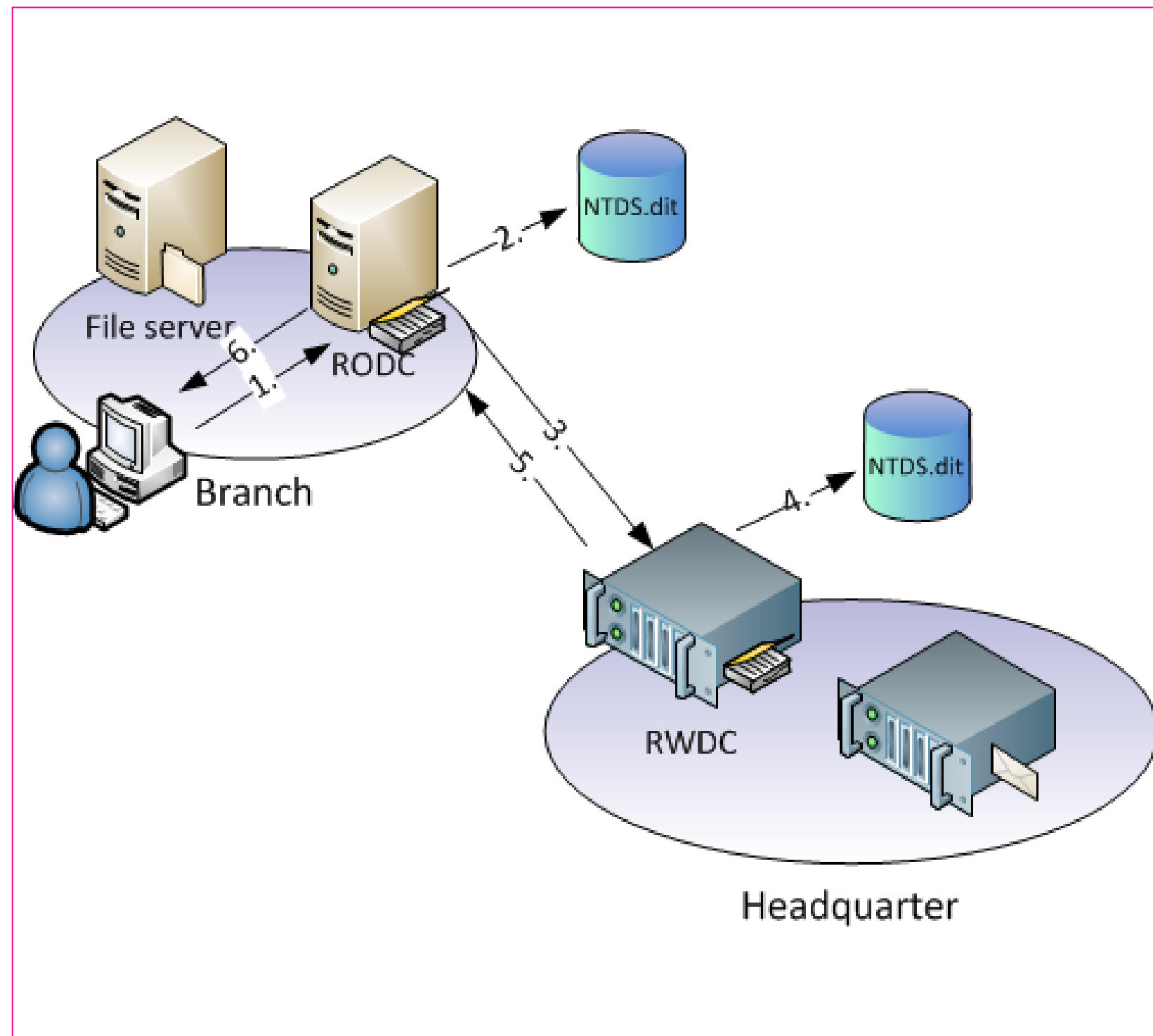


- Waar / wanneer?
 - Minder te beveiligen servers
 - Hoger risico (DMZ – externe site)
- Wat?
 - Read-only kopie van de database, zonder paswoorden voor accounts
 - Bijna geen paswoorden in cache
 - 1 richtingsreplicatie
 - Administrator Role Separation: aparte account om RODC te beheren
 - Filtered Attribute Set: Attributen kunnen gefiltered worden om niet te repliceren naar een RODC

RODC Principe

“The principle is the core assumption that the RODC is compromised by default”

Read-Only Domain Controller (RODC) (1/2)

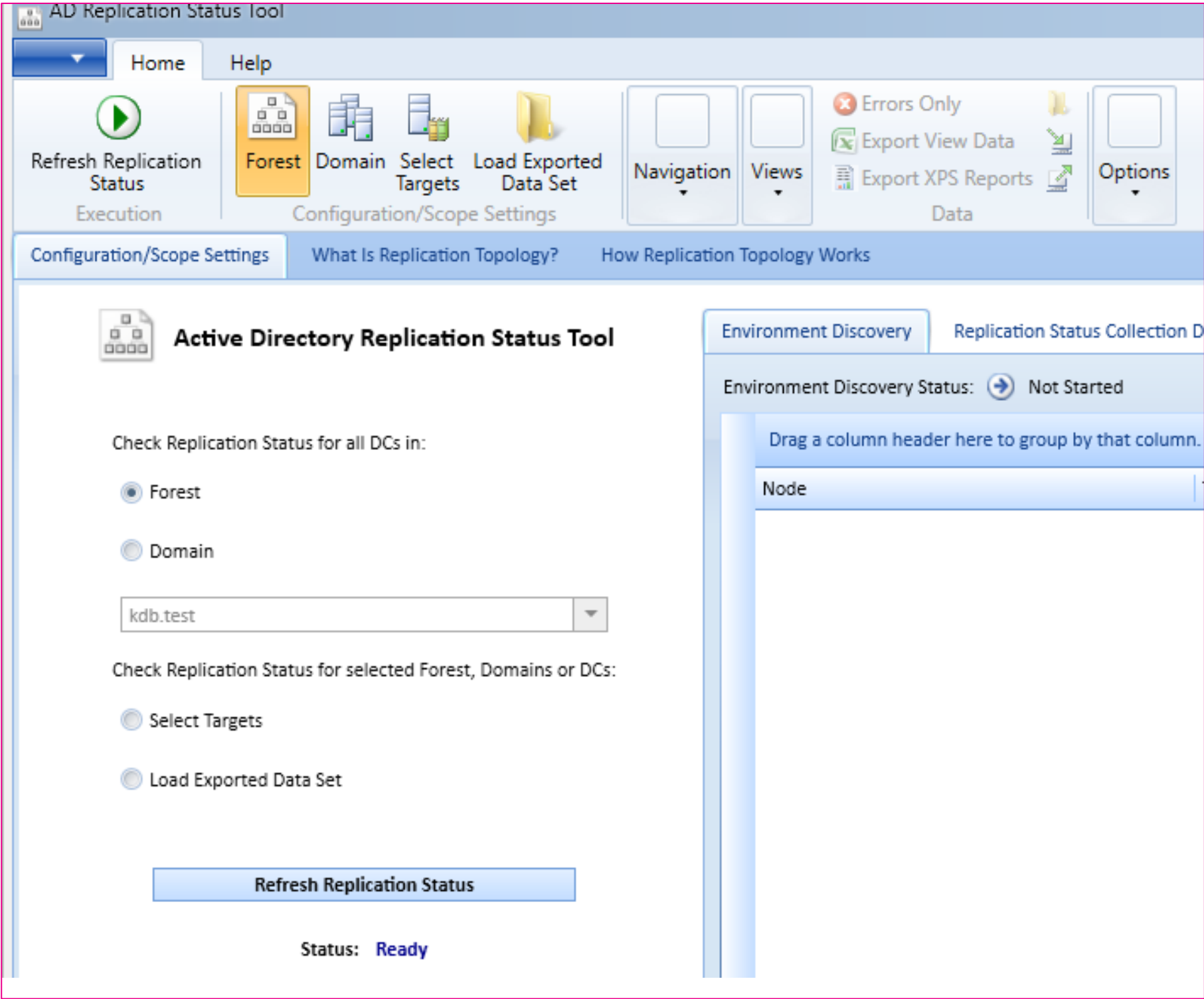


Stappen

1. Gebruiker wil aanmelden op PC remote site.
2. RODC heeft de account niet gecached en contacteert HQ DC.
3. HQ DC authenticceert gebruiker en kijkt of credentials mogen bewaard worden op RODC
 1. Default niet maar common practise om credentials van branch gebruikers te cachen.
4. RODC ontvangt credentials en stopt in cache.
5. Gebruiker geauthenticeerd
6. Volgende aanmelding via stored credentials RODC

Tools

Active Directory Replication Status Tool



Repadmin

Commandline: repadmin

Repadmin /?

Help opvragen

Repadmin /replsum

Summary

Repadmin /showrepl [DC]

Replication status

Repadmin /showconn [DC]

Connections

Repadmin /showobjmeta [DC] "ldap://dn=xxx"

Attributes + USN voor een object

Repadmin /kcc [DC]

Topology check

Repadmin /syncall

```
C:\Users\Administrator>repadmin /replsum
Replication Summary Start Time: 2019-04-11 16:01:05

Beginning data collection for replication summary, this may take awhile:
....

Source DSA          largest delta    fails/total %%    error

Destination DSA     largest delta    fails/total %%    error

C:\Users\Administrator>repadmin /showrepl

Repadmin: running command /showrepl against full DC ws16-kdb-test.kdb.test
Default-First-Site-Name\WS16-KDB-TEST
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 71a4b47f-3209-4451-90f3-1d8dd7e3c08b
DSA invocationID: 71a4b47f-3209-4451-90f3-1d8dd7e3c08b

C:\Users\Administrator>repadmin /showconn

Repadmin: running command /showconn against full DC ws16-kdb-test.kdb.test
Base DN: CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=kdb,DC=test
==== KCC CONNECTION OBJECTS =====
```

Powershell

PowerShell: Get-ADReplication...

Get-ADReplicationAttributeMetadata

Get-ADReplicationConnection

Connections

Get-ADReplicationFailure

Failure log

Get-ADReplicationPartnerMetadata

Get-ADReplicationQueueOperation

Get-ADReplicationUpToDatenessVectorTable

Get-command get-adrepl*

```
PS C:\Users\Administrator> Get-ADReplicationUpToDatenessVectorTable

cmdlet Get-ADReplicationUpToDatenessVectorTable at command pipeline
Supply values for the following parameters:
(Type !? for Help.)
Target[0]: ws16-kdb-test
Target[1]:

LastReplicationSuccess : 4/11/2019 3:58:53 PM
Partition               : DC=kdb,DC=test
PartitionGuid           : 75d73932-56f3-417f-a7c9-de11c952ae09
Partner                 : CN=NTDS Settings,CN=WS16-KDB-TEST,CN=Server
                        : ion,DC=kdb,DC=test
PartnerInvocationId     : 71a4b47f-3209-4451-90f3-1d8dd7e3c08b
Server                  : ws16-kdb-test.kdb.test
UsnFilter                : 61472

LastReplicationSuccess : 2/17/2019 4:30:07 PM
Partition               : DC=kdb,DC=test
PartitionGuid           : 75d73932-56f3-417f-a7c9-de11c952ae09
Partner                 :
PartnerInvocationId     : 42a83dd1-9bde-4c7e-ad2c-607fe2eb2674
Server                  : ws16-kdb-test.kdb.test
UsnFilter                : 20487
```

Metadata cleanup

- Wanneer een DC niet meer te herstellen valt
 - Zonder 'demotion'
 - Orphaned DC
- Manual actions:
 - Transfer/Seize FSMO Roles!
 - Delete DC computer object
 - Delete DC object in AD Sites & Services
 - Delete DNS A & SRV records in DNS

