

## Active Directory Replikation Teil 2 - Dienste

Beigesteuert von Yusuf Dikmenoglu

In diesem Artikel widme ich mich den wichtigsten Diensten die bei der Replikation eine große Rolle spielen.

### Teil 2

#### KCC (Knowledge Consistency Checker)

Der KCC (zu Deutsch = Konsistenzprüfungsdienst), ein Prozess des Active Directory ist dafür zuständig, wie der Name schon sagt - das die Verbindung zwischen den Replikationspartnern besteht und das in der Gesamtstruktur eine effiziente Replikationstopologie entsteht. Ebenfalls sorgt der KCC für eine Konsistenz der verteilten Active Directory - Datenbank auf allen Domänencontrollern in der Gesamtstruktur. Wenn z.B. eine Verbindung/Leitung ausfällt, richtet der KCC eine neue Verbindung zum Replikationspartner wieder her. In der Regel nimmt der KCC alle 15 Minuten eine erneute Berechnung der Replikationstopologie für den Domänencontroller vor, damit Änderungen an der Active Directory Struktur automatisch berücksichtigt und somit ein manuelles Eingreifen nicht erforderlich ist. Der Administrator kann weitere Verbindungen erstellen, falls aber die Verbindung an irgendeiner Stelle abbricht, greift der KCC erneut ein und richtet es. Dabei wird das Least-Cost-Spanning-Tree-Algorithmus (Intersite=Standortübergreifend) Verfahren angewendet das auf Bandbreiteneffizienz ausgelegt ist.

Der KCC erstellt anhand eines Ringentwurfs automatisch eine effiziente Replikationstopologie innerhalb eines Standortes (Intrasite) und eine für die Standortübergreifende Replikation (zwischen den Standorten - Intersite). Diese Ringtopologie versucht mindestens zwei Verbindungen zu jedem Domänencontroller zu erstellen (zwecks Fehlertoleranz) mit maximal 3 Hops zwischen den beliebigen DCs (wegen Reduzierung der Replikationswartzeit). Weiter erstellt der KCC für jede Verzeichnispertition eine eigene Replikationstopologie (Schema- Konfigurations- Anwendungs- sowie Domänenverzeichnispartition).

Er überwacht (dynamisch) permanent die Gegebenheiten wie z.B. wenn DCs einem Standort hinzugefügt, entfernt oder verschoben werden, die Kosten sich ändern oder wenn ein Domänencontroller nicht erreichbar ist, dann &bdquo;justiert" der KCC nach, so das die Replikation Reibungslos weiter verläuft.

Falls man nicht möchte das der KCC die Replikationstopologie automatisch erstellt, dann kann man es abstellen, was aber bedeuten würde das man selber für die Replikation des evtl. bestehenden VPNs zuständig ist und was noch viel wichtiger ist, man bekommt nicht &bdquo;gleich" mit das ein Replikationsproblem besteht bis man eingreifen kann. Dieser Artikel beschreibt wie das geht, aber die Empfehlung ist - Finger weg - der KCC macht seine Arbeit schnell und ordentlich: <http://support.microsoft.com/kb/242780/de>

#### ISTG (Intersite Topology Generator)

Der ISTG ist eine Komponente des KCC. Dieser ist für die Verwaltung und Überwachung von standortübergreifenden Replikationsverbindungen verantwortlich. Er ermittelt den jeweiligen Bridgeheadserver eines Standortes und falls dieser nicht mehr zur Verfügung steht, sucht er sich einen neuen. Der erste Domänencontroller eines Standortes bekommt automatisch die Rolle des ISTG zugewiesen, auch wenn weitere DCs dem Standort hinzugefügt werden behält er diese Funktion. Erst wenn dieser (1. DC) nicht mehr zur Verfügung steht, wird diese Rolle an einen anderen Domänencontroller dieses Standortes vergeben.

In einem bestimmten Intervall (Standardmäßig 30 min.), den man unter folgendem Registry - Schlüssel beeinflussen kann &bdquo;HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters"

Attribut "InterSiteTopologyGenerator" informiert der ISTG die anderen DCs des gleichen Standortes, dass er noch vorhanden ist. Falls das Intervall verstreicht und diese Information nicht repliziert wurde, geht der KCC davon aus das dieser nicht mehr zur Verfügung steht und bestimmt einen neuen Domänencontroller der die Rolle des ISTG übernimmt. Wenn mehr als 500 KB (Standortübergreifend) repliziert werden müssen, werden die Daten komprimiert.

Im Active Directory des Windows Server 2000 hat der ISTG-Algorithmus seine Grenzen und arbeitet ab ca. 300 Standorten nicht mehr effizient, so dass man diesen ISTG-Algorithmus ausschalten und die Definition und Verwaltung von Verbindungen manuell erledigen musste. Bei Windows Server 2003 wurde die Skalierbarkeit erheblich erweitert und nun ist es auch möglich, bei 3.000 Standorten immer noch eine effiziente Replikationstopologie zu ermitteln.

#### FRS (File Replication Service)

Der Dateireplikationsdienst ist zuständig für die Replikation der Daten im SYSVOL - Verzeichnis eines Domänencontrollers, auch wird FRS für die Replikation des verteilten Dateisystem`s (DFS = Distributed File System) verwendet.

An dieser Stelle sei erwähnt, dass sich dieses Verhalten in Windows Server 2003 R2 ändert, dort repliziert DFS sich über sein eigenes Replikationsverfahren.

Einige Informationen von Gruppenrichtlinien werden nicht im Active Directory gespeichert, sondern im Dateisystem eines Domänencontroller's wie z.B. Scripts oder Ordnerumleitungen. In einer Umgebung wo mehrere Domänencontroller existieren, sorgt das FRS dafür - das die Daten im Active Directory und auch im SYSVOL - Verzeichnis erfolgreich auf alle DCs repliziert werden, damit auch jeder Benutzer sowie Client egal von welchem Domänencontroller sie angemeldet werden, überall die gleichen Einstellungen erhalten. Das FRS arbeitet so wie das Active Directory nach der Multi-Master Replikation, so dass Änderungen an jedem Domänencontroller zulässig sind. Anders als bei der Active Directory - Replikation werden die Daten bei FRS standortübergreifend nicht komprimiert, daher kann es eine Weile dauern (bei umfangreichen Daten) bis alle Daten repliziert worden sind oder bei der Erst-Replizierung eines Domänencontroller. FRS speichert Logs im Verzeichnis %Systemroot%\Debug die ggf. bei Problemen behilflich sein können mit den Namen Ntfrs\_0001.log bis Ntfrs\_0005.log.

Ebenfalls wird ein Log - File erstellt (Ntfrsapi.log) wenn ein Server zum Domänencontroller heraufgestuft und herabgestuft wird.

Des Weiteren basiert FRS auf Layer 7 - Anwendungsschicht im Open Systems Interconnection - Layer Model (OSI-Model) und verwendet Remoteprozeduraufrufe über TCP/IP (RPC over TCP/IP).

FRS hat folgende Inhalts- und Datengrenzen:

- Eine maximale Dateigröße von 20 GB
- Maximal 64 GB an Daten
- Maximal 500.000 Dateien unter dem Replikations - Stamm
- Maximal 1.000.000 gleichzeitiger Änderungsanforderungen

Und folgende Topologie Grenzen:

- Maximal 1.000 Replikationspartner
- Maximal 150 Replikas pro Computer

#### Replikations Transport - Protokolle

Das Active Directory repliziert standardmäßig über Remoteprozeduraufrufe (Remote Procedure Call = RPC) over Internetprotokoll (IP). Diese Protokolle werden sowohl für die standortinterne als auch standortübergreifende Replikation verwendet. Für die Sicherheit bei der Übertragung der Daten durch diese Protokolle, sorgt einmal die Authentifizierung mit dem Kerberos V5-Authentifizierungsprotokoll und des Weiteren die Datenverschlüsselung. Eine Komprimierung der Daten findet dabei nicht statt. Die standortübergreifende IP - Replikation benutzt standardmäßig Zeitpläne, die sich aber auch ignorieren lassen.

Als weiteres Protokoll kann auch SMTP (Simple Mail Transfer Protocol) verwendet werden. SMTP kann aber NUR Standortübergreifend eingesetzt werden und nicht standortintern. Da SMTP kein sicheres Protokoll ist, braucht man ebenfalls eine Organisationszertifizierungsstelle (CA) um die Replikationsinformationen digital signieren und verschlüsseln zu können, damit sichergestellt ist das die gesendeten Daten unverändert und die Echtzeit der Daten auf der Empfängerseite sichergestellt ist. Eine weitere Einschränkung ist auch, dass man damit die Schema-, Konfigurations- sowie Anwendungsverzeichnispartition replizieren kann, jedoch nicht die Domänenverzeichnispartition.

Replizierungsinformationen werden vor ihrer Übertragung komprimiert um die Bandbreite effizient auszunutzen.

© 2006 by Yusuf Dikmenoglu