Windows 2012 - Grundbegriffe

Domain (Domäne)

Eine Domäne ist ein Namensraum und besteht aus Management- und Gemanageten-Objekten. Eine Domäne kann auch andere Domänen enthalten. Die enthaltenen Objekte sind anhand von Kriterien (Oftmals organisatorisch oder geografisch) gruppiert.

Subdomain (Subdomäne)

Eine Domäne ist eine Subdomäne wenn sie Teil einer anderen Domäne ist.

Tree (Struktur)

Ein Tree beschreibt die erste Domäne (Root Domain) an welcher weitere Domänen angehängt werden können. Das ganze Gebilde ist dann ein Tree. Sind keine weiteren Standorte vorhanden, dann ist die Domäne ausreichend.

Oft ist es jedoch so, dass Unternehmen weitere Standorte betreiben und es somit erschwert ist eine zentrale Domäne zu verwalten (Probleme mit verschiedenen Zeitzonen, Verbindungsprobleme zwischen den Standorten, Verständigungsprobleme). Treten solche Probleme auf ist es sinnvoll mehrere Domänen einzurichten, so dass diese alle unter einem gemeinsamen Dach arbeiten, als so genannte Struktur (Tree). Unter der Hauptdomäne laufen weitere Unterdomänen, diese gehören zwar zu der Hauptdomäne und tragen ebenfalls den selben Namen, unterhalten jedoch ihre eigene Domäne und tragen ihren eigenen Namen vorran (z.B. subdomain.rootdomain.com).

Die Verbindungen zwischen den Domänen werden durch Vertrauensstellungen hergestellt. Die Vertrauensstellung schafft die Vorrausetzung für einen Benutzer, auf die Ressourcen einer anderen Domäne zuzugreifen.

Forest (Gesamtstruktur)

Mit der Gesamtstruktur ist das ganze Verzeichnis gemeint, das aus mehreren Domänen und Active Directorys (ADs) bestehen kann. (Tree = Bäume und Forest = Wald).

Viele Unternehmen besitzen Tochtergesellschaft, die zwar zur Unternehmengruppe gehören, ihr operatives Geschäft jedoch komplett eigenständig abwickeln und auch einen anderen Namen haben. AD bietet für diese Konstellationen die Gesamtstruktur an, diese bildet die größte Form der Domänenverwaltung.

In einem Forest werden zwei völlig unabhängige Domänen, die unterschiedliche Namensräume haben, durch Vertrauensstellung miteinander verbunden. Ein Forest wird oft als vorüber gehende Lösung eingerichtet. Z.B. Wurde ein anderes Unternehmen

aufgekauft, kann so schnell eine Vertrauensstellung geschafft werden. Bis die endgültige Integration in das Unternehmen erfolgt, arbeitet man in einer Forestumgebung.

Mit einer Gesamtstruktur werden die Vorrausetzungen geschaffen, auf die Ressourcen einer komplett anderen Domäne zuzugreifen, die einen völlig anderen Namensraum haben. Auch hier werden Vertrauensstellung zwischen den Domänen eingerichtet.

Replikation

Die Replikation von AD-Informationen ist nur dann erforderlich, wenn mehrere Domänencontroller in einem Netzwerk vorhanden sind. In einem solchen Fall gibt es oft einen Primären Domänencontroller (PDC) und einen oder mehrere Backup Domänencontroller (BDC) zur sicherung der Daten.
Jeder Domänencontroller repliziert bzw. synchronisiert seine Active Directory-Datenbank mit anderen Domänencontrollern in der Domänengesamtstruktur.
Der Primäre Domänencontroller ist der einzige auf dem neue Daten geschrieben werden, um die Daten konsisten zu halten. Die Replikation umfasst die Einstellung einer Domäne und ist auf die Domäne begrenzt. Je größer ein Netzwerk wird, desto wichtiger wird eine Replikation der Active Directory-Informationen.
Die Replikation geschieht automatisch nach bestimmten Vorgaben. Ein Replikations-Monitor ist zur Überwachung der Replikationen vorhanden.

Global Catalog (GC)

Der globale Katalog hat keine eigene, sondern eine vom Active Directory abgeleitete Datenbank, um suchen im Active Directory zu beschleunigen.
Der globale Katalog ist ein Verzeichnis aller Active Directory-Objekte inklusive aller Attribute innerhalb der Domäne in der sich der globale Katalog befindet. Auch Objekte anderer Domänen können sich in dem globale Katalog befinden, aber nur die Attribute, die für eine Suchoperation relevant sein könnten (z.B. der Domain Name eines Objekts) werden gespeichert.
Des Weiteren hat der globale Katalog einen Index, in dem hinterlegt ist, welches Objekt auf welchem Domänencontroller im Active Directory liegt.
Der erste Domänencontroller der in einer Gesamtstruktur installiert wird, ist automatisch auch ein globaler Katalog.
Alle weiteren Domänencontroller sind standardmäßig keine globalen Kataloge und weitere globale Kataloge können manuell angelegt werden.

Vertrauensstellung

Grundlegendes Vertrauenstellung

Bevor ein Benutzer auf eine Ressource einer anderen Domäne zugreifen kann, muss durch das Sicherheitssystem auf Domänencontrollern bestimmt werden, ob zwischen der vertrauenden Domäne (in der die Ressource enthalten ist, auf die der Benutzer zugreifen möchte) und der vertrauenswürdigen Domäne (Anmeldedomäne des

Benutzers) eine Vertrauensstellung besteht. Zu diesem Zweck wird vom Sicherheitssystem der Vertrauenspfad zwischen einem Domänencontroller in der vertrauenden Domäne und einem Domänencontroller in der vertrauenswürdigen Domäne berechnet. Eine Domänenvertrauensstellung wird immer nur zwischen zwei Domänen erstellt: der vertrauenden Domäne und der vertrauenswürdigen Domäne.

Vertrauensstellungstypen

Extern – um eine Vertrauensstellung außerhalb der Gesamtstruktur zu erstellen. Dies ist sinnvoll, wenn ein Benutzer Zugriff auf eine Domäne innerhalb einer seperaten Gesamtstruktur (Forest) benötigt.
Bereich – für Cross Platformen
Gesamtstruktur – wenn einem anderen Forest transitiv vertraut wird
Abkürzung – um die Zugriffsgeschwindigkeit auf einen Tree zu erhöhen

Unidirektionale Vertrauensstellung

Diese Vertrauensstellung geht nur in eine Richtung. So kann beispielsweise ein Benutzer von Domäne A auf Daten in der Domäne B zugreifen, aber der Benutzer von der Domäne B nicht auf Daten der Domäne A.

Bidirektionale Vertrauensstellung

Beim Anlegen einer Subdomain besteht eine bidirektionale Vertauensstellung zwischen dieser und der Hauptdomäne. Dies bedeutet, dass beide Domänen der jeweils anderen vertrauen und auf die Daten zugreifen können.

Transitive Vertrauenstellung

Wird eine weitere Dömane in eine bereits vorhandene Vertrauenstellung zwischen mindestens zwei Domänen hinzugefügt, so vertrauen sich alle Domänen gleichermaßen.

Cross-Forest-Trust

Cross-Forest-Trust beinhaltet die Vertrauenstellung zwischen mehreren Forests.

QUELLEN:

http://blog.dikmenoglu.de/Globaler+Katalog+Global+Catalog+GC.aspx
http://de.wikipedia.org/wiki/Primary_Domain_Controller
http://www.edv-lehrgang.de/domaenenstrukturen/
http://technet.microsoft.com/de-de/library/cc754612.aspx
http://www.tecchannel.de/server/windows/461654/kerberos_tools/

http://technet.microsoft.com/de-de/library/cc730798.aspx