Active Directory

Autor: Moser Tobias

Datum: 17.03.2015

Typ: Information

Version: 1.0

Inhaltsverzeichnis

INHALT

1.1 Active Directory (kurz AD)

Mit Windows 2000 wurde das das "Active Directory" eingeführt. Das "Active Directory" ist ein Verzeichnisdienst von MS. Hierdurch wurden die einzelnen Verzeichnisdienste von Windows NT abgelöst und erheblich durch weitere Funktionen erweitert. Die zentrale Funktion von Active Directory ist als zentraler Verzeichnisdienst für alle Objekte (Drucker, Rechner, User usw.) zur dienen. Active Directory ist hierarchisch gegliedert.

1.2 Was ist ein Verzeichnisdienst?

Ein Verzeichnisdienst ist eine Informationsquelle, in der Informationen über Objekte abgelegt werden. Auch ein Telefonbuch, indem Telefonnummern und Adressen zu bestimmten Namen abgelegt werden, kann man als Verzeichnisdienst ansehen.

Im Active-Directory Verzeichnisdienst sind alle Objekte, die es in einem Netzwerk gibt, abgelegt. Solche Objekte sind z.B. Benutzer, Gruppen oder Drucker.

Durch den Verzeichnisdienst ist ein Netzwerk leichter zu administrieren. Wenn z. B. ein User gesucht wird, dessen Name nicht bekannt ist, kann dieser über sein Attribute (Standort, Typ usw...) gesucht werden.

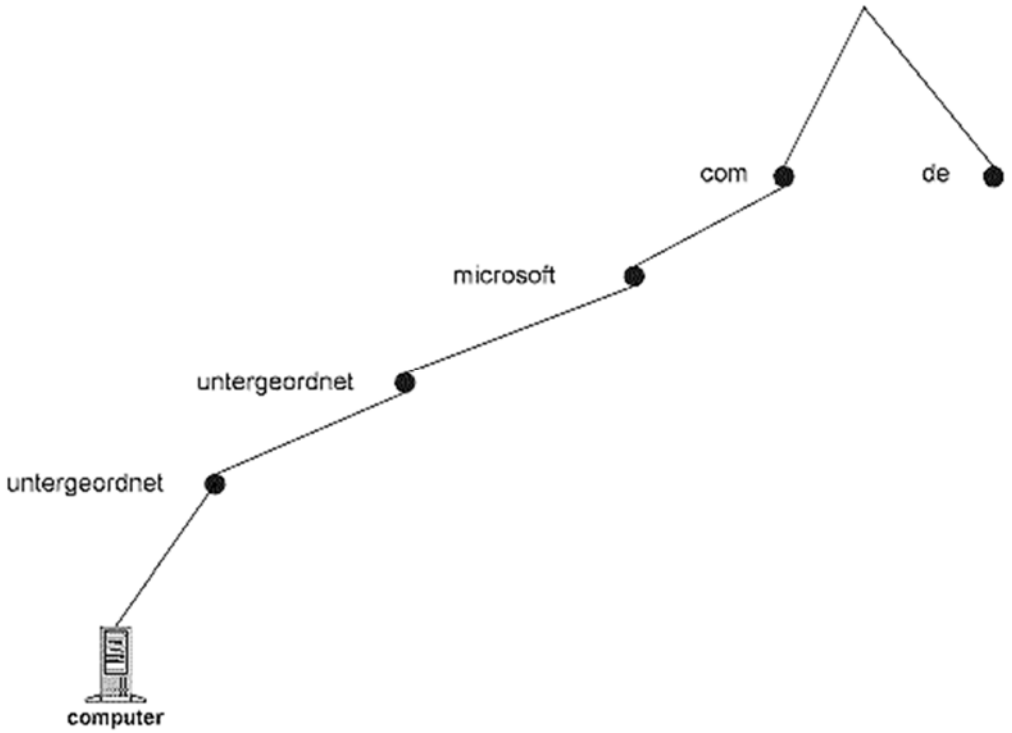
Der Active Directory-Verzeichnisdienst bietet folgende Merkmale:

- Einen **Datenspeicher oder ein Verzeichnis**, in dem Informationen zu Active Directory-Objekten gespeichert werden. Diese Objekte beinhalten in der Regel freigegebene Ressourcen wie Server, Dateien, Drucker sowie Konten für Netzwerkbenutzer und Computer.
- Einen Regelsatz, das so genannte **Schema**. Das Schema definiert die im Verzeichnis enthaltenen Objekt- und Attributklassen, die Einschränkungen und Begrenzungen für Instanzen dieser Objekte sowie ihr Namensformat. Falls Sie sich mit Datenbankstrukturen auskennen, ist es vereinfacht gesagt die Tabellenstruktur der im AD enthaltenen Daten. Der sog. Domänencontroller mit der Funktion des Schemamasters überwacht die Struktur und den Inhalt des Schemas. Wird z.B. ein Microsoft Exchange Mailserver installiert, wird vor der eigentlichen Installation das Schema angepasst, damit Active-Directory die neuen Elemente (z.B. die E-Mail-Adresse...) aufnehmen kann. Ebenso ist eine Schemaerweiterung nötig, wenn z.B. ein Windows Server 2012 Domänencontroller in einem Netzwerk eingerichtet wird, das bisher nur Windows Server 2003 Domänencontroller kannte.
- Einen **globalen Katalog** mit Informationen zu allen im Verzeichnis enthaltenen Objekten. Der Katalog ermöglicht Benutzern und Administratoren die Suche nach Verzeichnisinformationen unabhängig von der Domäne des Verzeichnisses, in dem die Daten enthalten sind.
- Einen **Abfrage- und Indizierungsmechanismus**, mit dessen Hilfe Objekte und ihre Eigenschaften veröffentlicht und von Netzwerkbenutzern oder Anwendungen gesucht werden können.
- Einen **Replikationsdienst**, der Verzeichnisdaten im Netzwerk verteilt. Alle Domänencontroller in einer Domäne sind an der Replikation beteiligt und verfügen über eine vollständige Kopie sämtlicher Verzeichnisinformationen für ihre Domäne. Jede Änderung der Verzeichnisdaten wird auf alle Domänencontroller in der Domäne repliziert.
- Die **Integration mit dem Sicherheitssubsystem** von Windows für sichere Netzwerkanmeldungen sowie eine Zugriffssteuerung für Verzeichnisdatenabfragen und Datenänderungen.

Um die Vorteile von Active Directory in vollem Umfang nutzen zu können, muss auf dem Computer, der über das Netzwerk auf Active Directory zugreift, die erforderliche Clientsoftware ausgeführt werden. Das bedeutet, dass auf den Clients Betriebssystemversionen mit mindestens der PRO-

Versionen eingesetzt werden müssen. Die HOME-Varianten lassen sich nicht korrekt mit einem Active-Directory verbinden.

Jeder Computer innerhalb einer DNS-Domäne wird durch seinen vollqualifizierten DNS-Domänennamen eindeutig identifiziert. Der vollqualifizierte Domänenname eines Computers mit Namen *computer* in der Domäne*untergeordnet.untergeordnet.microsoft.com* würde folgendermassen lauten:*computer.untergeordnet.untergeordnet.microsoft.com.*

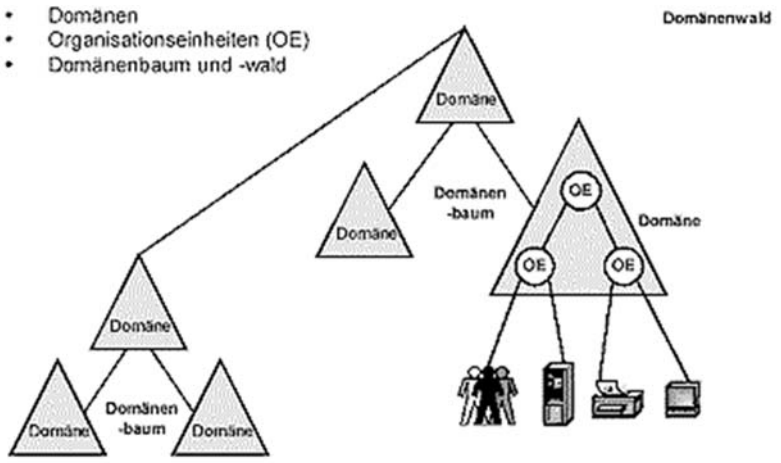


Active Directory arbeitet eng mit DNS zusammen. Active Directory und DNS verfügen über identische hierarchische Strukturen, was aber nicht heisst, dass der Active Directory Name der einen registrierten Internet-Domäne entsprechen muss. Obwohl Active Directory und DNS eigentlich getrennte Einheiten darstellen und für unterschiedliche Anwendungsbereiche implementiert wurden, haben die DNS- und Active Directory-Namespaces einer Organisation dieselbe Struktur. Zum Beispiel kann *lars-web.com* sowohl eine DNS- als auch eine Active Directory-Domäne sein.

DNS-Zonen können in Active Directory gespeichert werden. Bei Verwendung des DNS-Dienstes von Windows können Dateien für primäre Zonen zur Replikation auf andere Active Directory-Domänencontroller in Active Directory gespeichert werden.

Active Directory-Clients verwenden DNS für die Suche nach Domänencontrollern. Um einen Domänencontroller einer bestimmten Domäne zu lokalisieren, fordert ein Active Directory-Client spezifische Ressourceneinträge von seinem konfigurierten DNS-Server an.

Wie oben erwähnt, ist die logische Struktur des Active Directory eine Baumstruktur, die eine wirklichkeitsgetreue Abbildung einer gesamten Organisation ermöglicht.

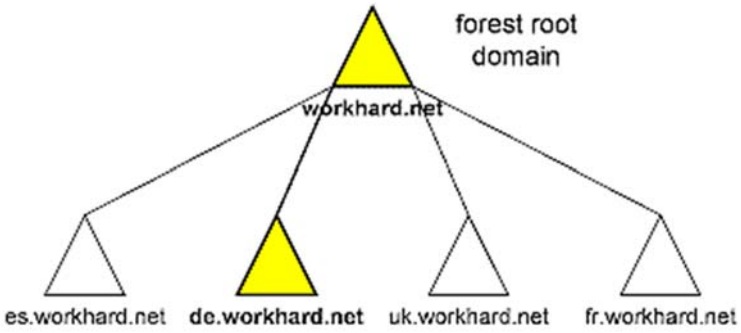


Sie besteht aus:

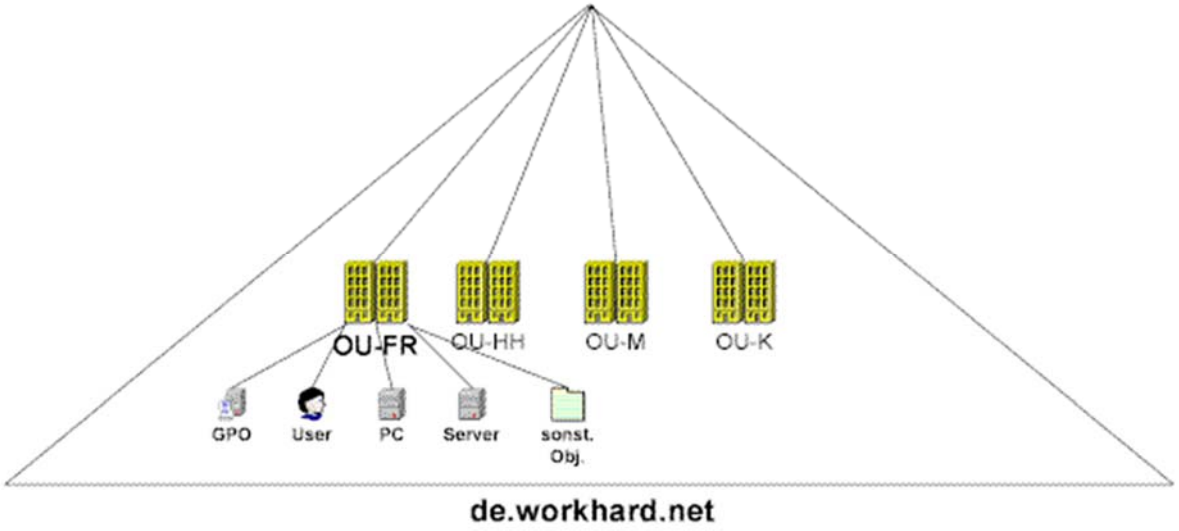
- Domänenwald = Domänengesamtstruktur = Gesamtstruktur = Forest
- Domänenbaum = Domain Tree
- Domäne = Domain
- Organisationseinheiten = OE = Urganisation Units = OU

Die erste Windows Domäne ist die so genannte Root-Domäne. Sie enthält alle Betriebsmasterfunktionen sowie einen Globalen Katalog. Eventuell vorhandene untergeordnete Domänen bilden den Domänenbaum (Domain Tree). Mehrere Domänenbäume bilden den so genannten Domänenwald (Forest).

Ein fiktives Beispiel - die internationale Firma *workhard:* Die Firma ist in mehreren Ländern vertreten und hat in diesen auch mehrere Niederlassungen:



Für eine weitere Unterteilung wird in jeder Niederlassung eine Organisationseinheit (OE = Organizational Unit = OU) eingerichtet. Die Administratoren der Niederlassungen haben in Ihrer OU Vollzugriffsrechte.



Es gilt: Mehrere Domänen im gleichen DNS-Namespace (also Domänen, die über dieselbe Stammdomäne verfügen) bilden einen Domänenbaum.

Ein Domänenwald ist eine Gruppe von Domänenbäumen mit unterschiedlichen DNS-Namensäumen (de.workhard.net, es.workhard.net, ik.workhard.net, fr.workhard.net).

Alle Domänenbäume nutzen jedoch das Schema, die Konfiguration sowie den globalen Katalog der Root-Domäne.

1.3 Was ist ein Domänencontroller?

Bei einem Domänencontroller handelt es sich um einen unter Windows Server ausgeführten Computer mit wichtigen Funktionen für das AD. Netzwerkbenutzern und Computern wird der Active Directory-Verzeichnisdienst zur Verfügung gestellt. Domänencontroller dienen zur Speicherung von Verzeichnisdaten und zur Verwaltung von Interaktionen zwischen Benutzern und Domänen, darunter Benutzeranmeldungen, Authentifizierungen und Verzeichnissuchen.

Eine Domäne enthält einen oder mehrere Domänencontroller. Eine kleine Organisation benötigt möglicherweise nur eine Domäne mit zwei Domänencontrollern, um hohe Verfügbarkeit und Fehlertoleranz zu gewährleisten. Um hohe Verfügbarkeit und Fehlertoleranz in größeren Unternehmen mit zahlreichen Netzwerkstandorten sicherzustellen, sind mehrere Domänencontroller pro Standort erforderlich.

In jeder Active Directory-Gesamtstruktur gibt es mindestens fünf verschiedene Funktionen des Betriebsmasters, die einem oder mehreren Domänencontrollern zugewiesen werden, die sog. FSMO-Rollen oder Betriebsmasterfunktionen.

Es gibt keine Trennung mehr zwischen primären Domänencontrollern und Sicherungsdomänencontrollern. Änderungen in einem Domänencontroller werden automatisch auf allen weiteren Domänencontrollern repliziert.

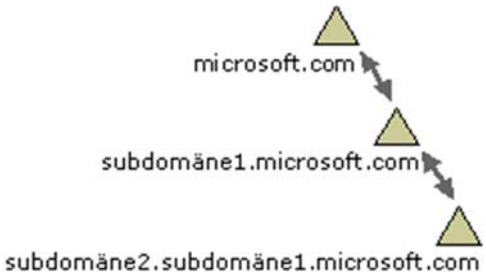
1.4 Übersicht über Domänen

Durch eine Domäne auch wird ein Sicherheitsbereich definiert. Das Verzeichnis beinhaltet eine oder mehrere Domänen, von denen jede über eigene Sicherheitsrichtlinien und Vertrauensstellungen mit anderen Domänen verfügt.

- Sicherheitsrichtlinien und -einstellungen (z. B. Administratorrechte und Zugriffssteuerungslisten) können nicht von einer Domäne auf eine andere übertragen werden (aber bei Bedarf können Vertrauensstellungen / Trusts eingerichtet werden)
- Die Delegierung von Administratorrechten an Domänen oder Organisationseinheiten macht die Ernennung zahlreicher Administratoren mit weitreichenden Administratorrechten überflüssig.
- Domänen unterstützen die Strukturierung des Netzwerkes, damit die jeweilige Organisation besser nachgebildet werden kann.
- In jeder Domäne werden ausschliesslich Informationen zu den in der Domäne enthaltenen Objekten gespeichert.
- Domänen bilden Replikationseinheiten. Alle Domänencontroller in einer bestimmten Domäne sind in der Lage, Änderungen zu empfangen und diese Änderungen auf alle anderen Domänencontroller innerhalb der Domäne zu replizieren.

Eine einzelne Domäne kann sich über mehrere physische Standorte erstrecken. Eine Unterteilung auf verschiedene Subnetze lässt sich ebenfalls abbilden. Dies sollte auch genutzt werden, da so sichergestellt ist, dass Benutzer jedes Standortes auch die richtigen, für sie zuständigen Server kontaktieren.

1.5 Domänenstrukturen



Alle Domänen, die über dieselbe Stammdomäne verfügen, bilden sozusagen einen fortlaufenden Namespace. Dies bedeutet, dass sich der Domänenname einer untergeordneten Domäne aus dem Namen der übergeordneten Domäne plus dem angehängten Namen der untergeordneten Domäne zusammensetzt.

In der Abbildung ist *subdomäne1.microsoft.com* eine untergeordnete Domäne von *microsoft.com* und die übergeordnete Domäne von *subdomäne1.microsoft.com*. Die Domäne *microsoft.com* ist die übergeordnete Domäne von *subdomäne1.microsoft.com* und gleichzeitig die Stammdomäne dieser Struktur.

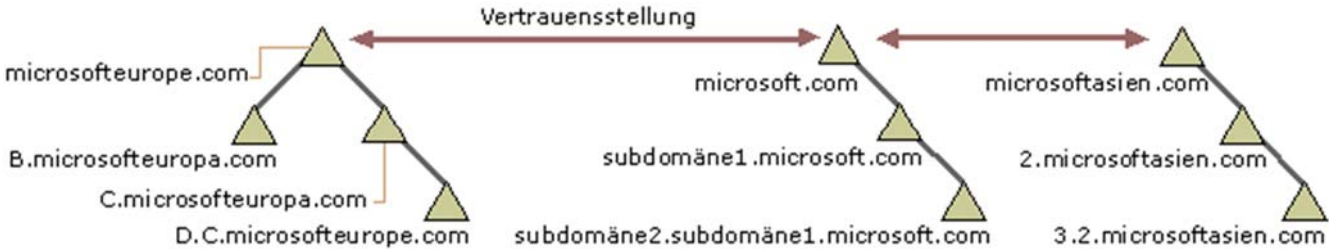
1.5.1 Vertrauensstellungen

Zwischen Windows-Domänen innerhalb einer Struktur bestehen bidirektionale, transitive Vertrauensstellungen. Da diese Vertrauensstellungen bidirektional und transitiv sind, verfügt eine neu eingerichtete Windows-Domäne in einer Domänenstruktur oder Gesamtstruktur direkt über Vertrauensstellungen mit allen anderen Windows 2000-Domänen in der Domänen- oder Gesamtstruktur. Dank dieser Vertrauensstellungen kann ein Benutzer mit einem einzigen

Anmeldevorgang gegenüber allen Domänen in der Domänen- oder Gesamtstruktur authentifiziert werden. Dies bedeutet jedoch nicht gleichzeitig, dass der authentifizierte Benutzer auch in allen Domänen der Gesamtstruktur über Rechte und Berechtigungen verfügt. Da eine Domäne einen eigenen Sicherheitsbereich darstellt, müssen Rechte und Berechtigungen pro Domäne zugewiesen werden.

1.6 Gesamtstruktur (Forest)

Eine Gesamtstruktur setzt sich aus mehreren Domänenstrukturen zusammen. Die Domänenstrukturen in einer Gesamtstruktur haben keinen fortlaufenden Namespace. Ein Beispiel: Obwohl die beiden Domänenstrukturen*microsoft.com* und *microsoftasia.com* beide über eine untergeordnete Domäne mit dem Namen "Support" verfügen können, würden die DNS-Namen dieser untergeordneten Domänen *support.microsoft.com* und*support.microsoftasia.com* lauten und aus diesem Grund keinen gemeinsamen Namespace aufweisen.



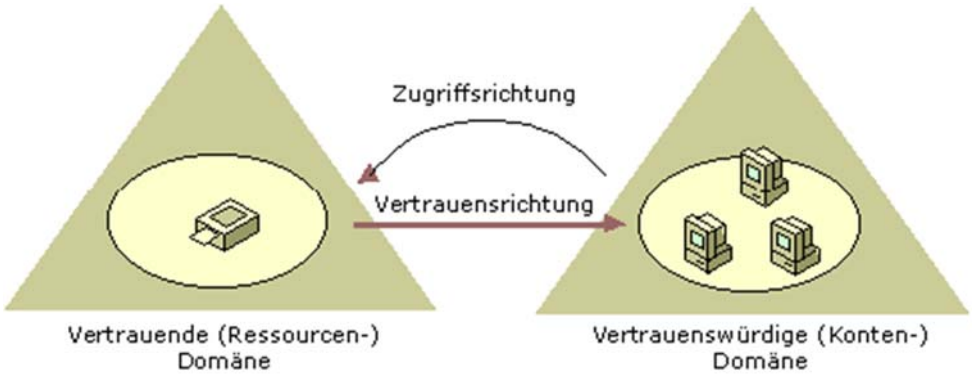
Eine Gesamtstruktur verfügt jedoch über eine Stammdomäne. Bei der Stammdomäne der Gesamtstruktur handelt sich u**m die erste in der Gesamtstruktur erstellte Domäne**. Zwischen den Stammdomänen aller Domänenstrukturen der Gesamtstruktur und der Stammdomäne der Gesamtstruktur werden transitive Vertrauensstellungen eingerichtet. In der Abbildung ist *microsoft.com* die Stammdomäne der Gesamtstruktur. Die Stammdomänen der anderen Domänenstrukturen *microsofteurope.com* und *microsoftasia.com* verfügen über transitive Vertrauensstellungen mit*microsoft.com*. Dies ist erforderlich, damit die Vertrauensstellungen auf alle Domänenstrukturen der Gesamtstruktur ausgedehnt werden können.

Alle Windows-Domänen in allen Domänenstrukturen einer Gesamtstruktur haben gemeinsam:

- Transitive Vertrauensstellungen zwischen den Domänen
- Transitive Vertrauensstellungen zwischen den Domänenstrukturen
- Ein gemeinsames Schema
- Identische Konfigurationsinformationen
- Einen gemeinsamen globalen Katalog
- Die Kombination von Domänenstrukturen und Gesamtstrukturen ermöglicht die flexible Verwendung fortlaufender und nicht fortlaufender Namen. Diese Flexibilität ist z. B. für Unternehmen mit unabhängigen Abteilungen hilfreich, die ihre jeweiligen DNS-Namen beibehalten müssen.

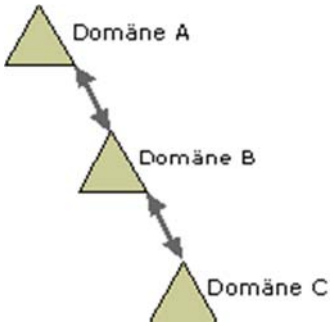
1.7 Vertrauensstellungen zwischen Domänen

Eine Vertrauensstellung ist eine Beziehung zwischen zwei Domänen, durch die Benutzer einer Domäne authentifiziert werden können, der sich in einer anderen Domäne befindet. Eine Vertrauensstellung zwischen Domänen wird immer nur zwischen zwei Domänen aufgebaut: der vertrauenden und der vertrauenswürdigen Domäne.



In der ersten Abbildung sind die Vertrauensstellungen durch einen Pfeil gekennzeichnet (dieser zeigt auf die vertrauenswürdige Domäne).

Unter Windows sind alle Vertrauensstellungen in einem Tree transitiv und bidirektional. Beide Domänen in einer Vertrauensstellung vertrauen sich automatisch gegenseitig.



Aus der Abbildung ist ersichtlich: Wenn Domäne A Domäne B vertraut und Domäne B Domäne C vertraut, können Benutzer aus Domäne C (sofern sie über die entsprechenden Berechtigungen verfügen) auf Ressourcen in Domäne A zugreifen.

Anmerkung

Wenn ein Benutzer von einem Domänencontroller authentifiziert wird, bedeutet dies nicht unbedingt, dass er auf die Ressourcen in dieser Domäne zugreifen kann. Dies wird ausschliesslich durch die Rechte und Berechtigungen bestimmt, die dem Benutzerkonto vom Domänenadministrator für die vertrauende Domäne erteilt wurden.

1.8 Active Directory Datenbank

Die Active Directory Datenbank ist die Datenbank einer Domäne. Sie enthält Informationen über Objekte wie Benutzer, Gruppen, Computer, Drucker, Freigaben...) Änderungen in ihr werden zwischen allen Domänencontrollern innerhalb der Domäne und der Domänengesamtstruktur repliziert und stehen somit den Benutzern im LAN zur Verfügung.

Per Standard ist der Speicherort Stammverzeichnis:\NTDS. Die Partition, auf der gespeichert wird, muss eine NTFS-Partition sein. Der Speicherort kann angepasst werden, es empfiehlt sich, hierbei auf Partitionen mit Redundanz auszuweichen, da die Objektdatenbank sehr wichtig ist.

Die Datenbank wird in einer Datei mit dem Namen NTS.DIT gespeichert. Sie enthält:

- Schema
- Globalen Katalog
- Objekte des Domänencontrollers

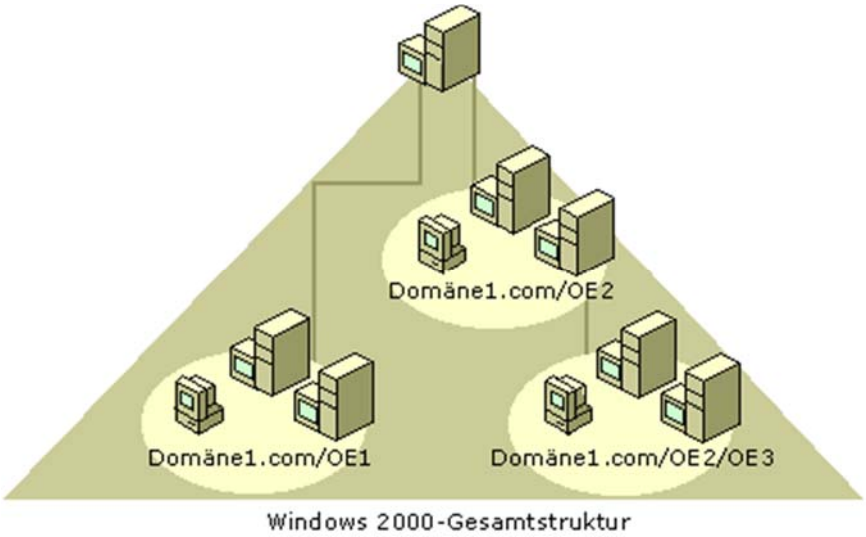
Während des Heraufstufens zum Domänencontoller wird die Datei NTDS.DIT vom Ordner Stammverzeichnis\SYTEM32 in das angegebene Verzeichnis kopiert. Die Active-Directory-Dienste werden gestartet. Falls andere Domänencontroller vorhanden sind, wird die Datei durch Replikation aktualisiert.

Wichtig für das AD ist ausserdem der Ordner Stammverzeichnis\SYSVOL. In ihm werden Skripte, Gruppenrichtlinienobjekte gespeichert. Der Ordner muss sich ebenfalls auf einer NTFS-Partition befinden.

1.9 Organisationseinheiten

Mit Organisationseinheiten (OE, Organisation Units, OU) können Strukturen geschaffen werden, die die Administration vereinfachen. Mit ihnen kann man die Unternehmensstruktur abbilden. Durch die Verwendung von Organisationseinheiten kann die Anzahl der für das Netzwerk benötigten Domänen u. U. minimiert werden. Ziel sollte es bei der AD-Planung immer sein, so wenig wie möglich Domänen zu verwenden und stattdessen auf Organisationseinheiten auszuweichen. Organisationseinheiten sind Active Directory-Container, denen Sie Benutzer, Gruppen, Computer und andere Organisationseinheiten hinzufügen können.

Eine Organisationseinheit stellt den kleinsten Bereich oder die kleinste Einheit dar, der Gruppenrichtlinieneinstellungen zugewiesen oder an die Administratorrechte delegiert werden können.



Organisationseinheiten können weitere Organisationseinheiten enthalten.

Einem Benutzer können Administratorrechte für alle Organisationseinheiten in einer Domäne oder für eine einzelne Organisationseinheit erteilt werden. Es ist nicht erforderlich, dass der Administrator einer Organisationseinheit Administratorrechte für weitere Organisationseinheiten innerhalb der Domäne besitzt.

Im eingangs gezeigten Beispiel wurde für ein internationales Unternehmen für jedes Land eine Child-Domäne gebildet. Pro Niederlassung wurde eine OE gebildet.

Eine OE kann Objekte enthalten:

- Benutzer
- Gruppen
- Computer
- Drucker
- Sicherheitsrichtlinien
- Dateifreigaben
- Applikationen
- untergeordnete OE

Bei der Verwaltung von OE sind Regeln zu beachten:

- Erstellen Sie OEa zum Delegieren von administrativen Verwaltungsaufgaben.
- Entscheiden Sie, wer welche Benutzer, Gruppen und sonstigen Ressourcen administrieren soll.
- Realisieren Sie eine logische und aussagekräftige OE-Struktur, sodass OE-Administratoren ihre Aufgaben effizient durchführen können.
- Vermeiden Sie das Zuweisen zu vieler untergeordneter Objekte innerhalb einer OE.
- Erstellen Sie OE zum Anwenden von Gruppen- bzw. Sicherheitsrichtlinien.

OEs erstellen Sie unter "Active Directory-Benutzer und-Computer". Klicken sie mit der rechten Maustaste auf das Domänenobjekt oder eine andere Organisationseinheit, in der Sie eine Organisationseinheit erstellen wollen und zeigen sie auf "NEU" und klicken sie anschliessend auf ORGANISATIONSEINHEIT.

1.10 Übersicht über "Active Directory-Standorte und -Dienste"

1.10.1 Dem AD einen Namen vergeben

Zunächst ist der DNS-Namespace des Active Directory festzulegen. Der DNS-Namespace ist ein Domänenenname der obersten Ebene im Active Directory. An den Namensraum sind die Domänenhierarchie, Vertrauensstellungen und die Replikationen geknüpft. Entweder wird der DNS-Namespace nach einem bereits registrierten externen Internet-DNS Namensraum oder als eigenständiger losgelöster DNS-Namensraum vergebenen.

Es gibt bei beiden Modellen Vor- und Nachteile. Im Ergebnis wird aber der Administrationsaufwand bei identischem internen und externen DNS-Namensraum erheblich höher sein. Microsoft empfiehlt daher für den AD-Namensraum eine Subdomäne des externen Namenraums zu vergeben. Z.B. www.lars-web.com -> ad.lars-web.com. Andere Quellen favorisieren Lösungen wie lars-web.local. Kristisch wird die letzte Lösung ist, wenn local jemals ein offizielle Top-Level Domain für das Internet werden sollte. Dann sind Probleme mit der Namensauflösung vorprogrammiert sind. Andere Experten empfehlen daher auch, einen offiziellen Namen zu vergeben und diesen einfach nicht im Internet zu verwenden.

Das Active Directory bedient sich der sog. Multimasterreplikation und ermöglicht es jedem Windows Domänencontroller innerhalb der Gesamtstruktur, Anforderungen, einschliesslich Verzeichnisänderungen durch Benutzer, zu verarbeiten.

Sind alle Computer durch eine breitbandige Netzwerkverbindung miteinander verbunden, dann verursacht die zufällige Auswahl eines Domänencontrollers möglicherweise keine Probleme. Umfangreiche Installationen, in denen ein schmalbandiges WAN (Wide Area Network) zum Einsatz kommt, können jedoch extrem ineffizient arbeiten. Dies wäre z.B. der Fall. wenn sich Benutzer in Frankfurt über eine DFÜ-Verbindung bei einem Domänencontroller in Paris authentifizieren. Mit "Active Directory-Standorte und -Dienste" kann dies durch den Einsatz von Standorten optimieren.

Sie verwenden "Active Directory-Standorte und -Dienste", um Informationen zur physischen Struktur des Netzwerkes im Active Directory zu veröffentlichen. Mit Hilfe dieser Informationen bestimmt Active Directory, auf welche Weise Verzeichnisinformationen repliziert und Dienstanforderungen verarbeitet werden.

Die Zuordnung von Computern zu Standorten erfolgt auf der Grundlage ihrer Position in einem Subnetz oder in einer Gruppe gut verbundener Subnetze. Ähnlich wie Postleitzahlen, unter denen ein bestimmter Bereich von Postanschriften zusammengefasst wird, bieten Subnetze eine einfache Möglichkeit zur Darstellung von Netzwerkgruppierungen. Subnetze sind so ausgelegt, dass physische Informationen zu den Netzwerkverbindungen schnell und einfach an das Verzeichnis übertragen werden können.

1.10.2 Standorte vereinfachen Aufgaben im AD

1.10.2.1 Authentifizierung

Bei der Anmeldung eines Clients über ein Domänenkonto **sucht die Anmelderoutine zuerst nach Domänencontrollern, die sich im selben Standort wie der Client befinden**. Dadurch bleibt der Netzwerkverkehr auf den lokalen Standort beschränkt, und die Effizienz des Authentifizierungsprozesses nimmt zu.

1.10.2.2 Replikation

Verzeichnisinformationen werden sowohl innerhalb als auch zwischen Standorten repliziert. Das Active Directory repliziert Daten innerhalb eines Standortes häufiger als zwischen verschiedenen Standorten. Diese Vorgehensweise schafft einen Ausgleich zwischen der Nachfrage nach möglichst aktuellen Verzeichnisinformationen und den durch die verfügbare Netzwerkbandbreite vorgegebenen Beschränkungen.

Sie können die Datenreplikation im Active Directory anpassen, indem Sie mit Hilfe von Standortverknüpfungen festlegen, auf welche Weise die einzelnen Standorte verbunden sind. Die Informationen zur Verknüpfung der Standorte werden von Active Directory zur Erstellung von Verbindungsobjekten verwendet. Diese Objekte ermöglichen eine effiziente Replikation und gewährleisten Fehlertoleranz.

Dabei können Sie folgendes konfigurieren;

- Kosten einer Standortverknüpfung
- Zeiten, zu denen die Verknüpfung verfügbar ist
- Häufigkeit, mit der eine Verknüpfung genutzt werden soll

Anhand dieser Informationen bestimmt Active Directory, welche Standortverknüpfung für die Datenreplikation verwendet wird.

Normalerweise werden Informationen zwischen Standorten von allen Domänencontrollern ausgetauscht. Sie können jedoch stärkeren Einfluss auf das Replikationsverhalten nehmen, indem Sie

einen Bridgeheadserver für die standortübergreifende Replikation von Informationen benennen. Richten Sie einen Bridgeheadserver ein, wenn anstelle eines beliebigen verfügbaren Servers ein dedizierter Server für die standortübergreifende Replikation bereitgestellt werden soll. Ein Bridgeheadserver kann auch eingerichtet werden, wenn die Netzwerkinstallation Proxyserver, z. B. für das Senden und Empfangen von Informationen durch einen Firewall, umfasst.

1.11 Gruppen

Gruppen sind Objekte in Active Directory oder auf dem lokalen Computer, die Benutzer, Kontakte, Computer und andere Gruppen enthalten können. Gruppen werden für folgende Zwecke verwendet:

- Verwalten von Benutzer- und Computerzugriffen auf freigegebene Ressourcen wie Active Directory-Objekte und dazugehörige Eigenschaften, Netzwerkfreigaben, Dateien, Verzeichnisse, Druckerwarteschlangen usw.
- Filtern von Gruppenrichtlinieneinstellungen
- Erstellen von E-Mail-Verteilerlisten

Es gibt zwei Arten von Gruppen:

- Sicherheitsgruppen
- Verteilergruppen

Mit Hilfe von Sicherheitsgruppen werden Benutzer, Computer und andere Gruppen in Gruppen zusammengefasst, die bequem verwaltet werden können. Administratoren sollten Ressourcenberechtigungen (z. B. für Dateifreigaben, Drucker usw.) vorzugsweise den jeweiligen Sicherheitsgruppen und nicht einzelnen Benutzern zuweisen. So werden die Berechtigungen nur einmalig der Gruppe und nicht mehrere Male einzelnen Benutzern zugewiesen (=>Vereinfachung). Jedes der Gruppe hinzugefügte Konto erhält automatisch die für die Gruppe definierten Rechte und Berechtigungen nach vorheriger Ab- und wieder Anmeldung.

Verteilergruppen können lediglich als E-Mail-Verteilerlisten eingesetzt werden. Sie können nicht zum Filtern von Gruppenrichtlinieneinstellungen verwendet werden. Sie haben keine Sicherheitsfunktionen.

1.11.1 Unterschied AD-Gruppen und Organisationseinheiten

Organisationseinheiten werden im Gegensatz zu Gruppen für die Zusammenfassung von Objekten innerhalb einer Einzeldomäne verwendet. Sie dienen jedoch nicht zur Übertragung von Mitgliedschaften. Die Verwaltung einer Organisationseinheit und der darin enthaltenen Objekte kann an einen einzelnen Administrator oder an eine Gruppe delegiert werden.

Gruppenrichtlinienobjekte können auf Standorte, Domänen oder Organisationseinheiten, jedoch niemals auf Gruppen angewendet werden. Ein Gruppenrichtlinienobjekt ist eine Gruppe von Einstellungen, die sich auf Benutzer oder Computer auswirkt. Mit Hilfe von Gruppenmitgliedschaften werden die Gruppenrichtlinienobjekte herausgefiltert, die Einfluss auf die Benutzer und Computer an einem Standort bzw. in einer Domäne oder Organisationseinheit haben.

1.12 Serverfunktionen / Serverrollen

Windows Server können mit verschiedenen Serverfunktionen ausgeführt werden.

1.12.1 Domänencontroller / Mitgliedsserver / Eigenständige Server

1.12.1.1 Domänencontroller

1.12.1.2 Mitgliedsserver

Ein Mitgliedsserver ist zwar Mitglied einer Domäne, aber kein Domänencontroller. Er verarbeitet keine Kontoanmeldungen, ist nicht an Active Directory-Replikationen beteiligt und speichert keine Richtlinieninformationen zur Domänensicherheit.

Mitgliedsserver werden in der Regel eingesetzt als:

- Dateiserver
- Anwendungsserver
- Datenbankserver
- Webserver
- Zertifikatsserver
- ...

Bis einschliesslich Server 2003 wurde die jeweilige Funktion einfach per Installation der entsprechenden Software zugewiesen. Mit Server 2008 hat Microsoft den Begriff "Rolle" eingeführt. Man fügt daher dem Server z.B. die Rolle Datei- und Speicherdienste hinzu.

- Mitgliedsserver unterliegen den für den Standort, die Domäne oder die Organisationseinheit aufgestellten Gruppenrichtlinieneinstellungen.
- Auf einem Mitgliedsserver verfügbare Ressourcen werden über die Zugriffssteuerung konfiguriert.
- Benutzer von Mitgliedsservern verfügen über zugewiesene Benutzerrechte.

1.12.1.3 Eigenständige Server

Ein eigenständiger Server ist ein unter Windows Server ausgeführter Computer, der keiner Active-DirectoryDomäne angehört. Ist Windows Server als Mitglied einer Arbeitsgruppe installiert, handelt es sich bei dem betreffenden Server um einen eigenständigen Server.

Eigenständige Server können Ressourcen mit anderen Computern im Netzwerk gemeinsam nutzen, profitieren jedoch nicht von den Vorteilen von Active Directory.