Grundlegendes zur physischen Struktur von Active Directory

Zusammenfassung: Dieser Artikel erläutert die Active Directory-Komponenten Standort, Domänencontroller und Globaler Katalog. Standorte sind die strukturelle Komponente von Active Directory, die für die Kommunikation von Daten und Replikation wichtig ist. Domänencontroller bilden die physische Struktur, sie enthalten eine Kopie des Active Directory. Mithilfe des globalen Katalogs lassen sich Abfrageprozesse optimieren und die Anmeldung beim Netzwerk vereinfachen.

Von Robert Williams

Artikel der Ausgabe vom Mai 2000 des Magazins *Windows 2000 Advantage*

In der Märzausgabe (englischsprachig) von *Windows 2000 Advantage* wurden die Grundlagen von Active Directory erläutert und seine logische Struktur analysiert. (Zusätzliche Informationen finden Sie auch unter: http://windows2000advantage.de/.) Active Directory verfügt auch über eine physische Struktur. Diese Struktur umfasst die Mechanismen für die Kommunikation von Active Directory-Daten und der Replikation. In diesem Artikel wird zunächst die strukturelle, auch als Standort bezeichnete Komponente erläutert, die eine zuverlässige Kommunikation verwaltet. Danach wird die physische Struktur, in der Active Directory-Daten gespeichert und repliziert werden und die als Domänencontroller bezeichnet wird, untersucht und ihre Beziehung zu Standorten. Abschließend wird der spezielle globale Katalog (Global Catalog, GC) erläutert.

Windows 2000-Standorte

Active Directory muss eine solide Netzwerkinfrastruktur verfügen können, damit es wichtige Aufgaben wie die Anmeldung von Benutzern und Anforderungen von Netzwerkobjekten durchführen kann. Unter idealen Bedingungen wäre die Netzwerkkommunikation immer konsistent schnell und zuverlässig. Leider müssen aufgrund geografischer und anderer Einschränkungen kleinere als Subnetze bezeichnete Netzwerke erstellt werden, um eine zuverlässige Kommunikation innerhalb eines physischen Standortes und standortübergreifend sicherstellen zu können. Windows 2000 verwendet das Konzept von Subnetzen.

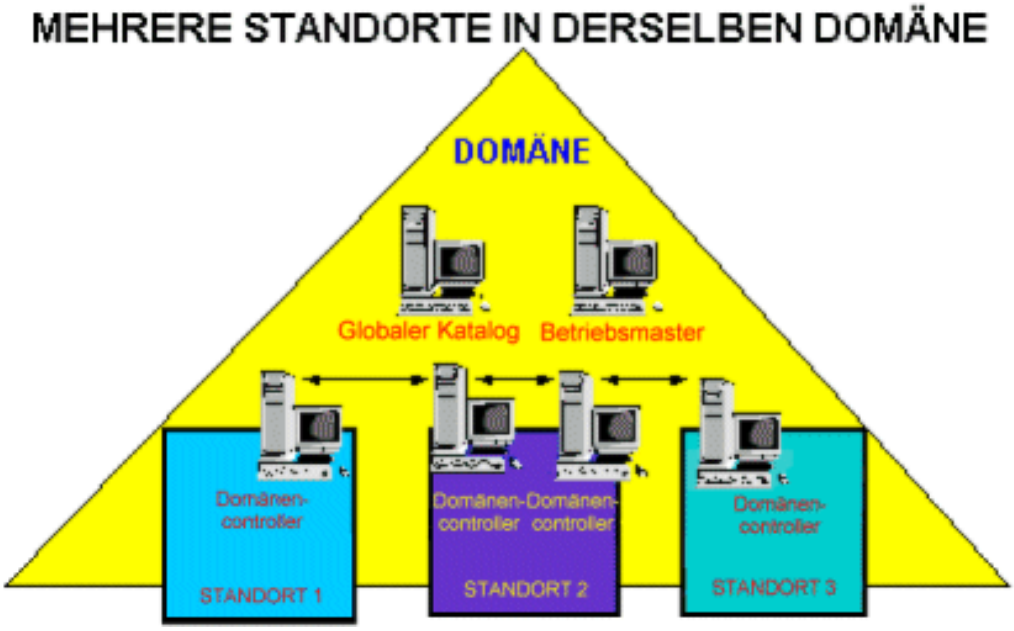
Die Struktur des physischen Netzwerkes von Active Directory basiert auf dem Vorhandensein einer Einheit, die als Standort bekannt ist. Der Administrator hat die Aufgabe, Standorte zu entwerfen, mit denen eine optimale Netzwerkleistung sichergestellt werden kann. Ein Standort besteht aus einem oder mehreren IP-Subnetzen (Internet Protocol), die durch zuverlässige Hochgeschwindigkeitsverbindungen verbunden sind. Die als ausreichend eingeschätzte Geschwindigkeit kann dabei unterschiedlich sein. In kleinen Netzwerken kann eine Verbindung mit einer Geschwindigkeit von 128K Bit/s ausreichend sein, während die Bandbreite für ein großes Netzwerk eine Geschwindigkeit von 3Mbit/s oder mehr betragen müsste. Es ist die Aufgabe des Administrators, festzulegen, bei welcher Geschwindigkeit der Leistungsverlust durch den Netzwerkverkehr minimal ist. Standorte sollten auf der Grundlage dieser Voraussetzung erstellt werden. Während viele Subnetze zu einem einzelnen Standort gehören können,

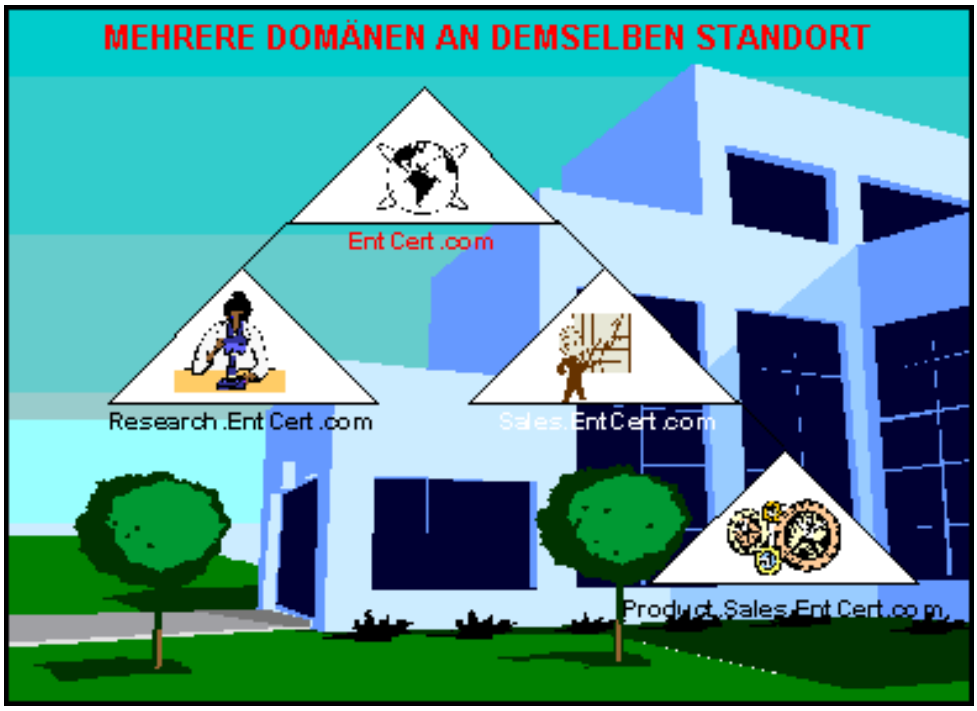
kann ein einzelnes Subnetz nicht mehrere Standorte umfassen.

Die primäre Bedeutung des Standortes liegt in der Sicherstellung schneller und wirtschaftlicher Datenübertragung, besonders da die effiziente Replikation von Verzeichnisdiensten davon abhängt. Die physische Struktur von Active Directory steuert, wann und wie Replikation stattfindet. Dies gilt sowohl für die Replikation innerhalb eines Standortes als auch für die standortübergreifende Replikation. Die Leistung des Netzwerkstandortes hat auch Auswirkungen auf den Speicherort von Objekten und die Anmeldeauthentifizierung. Beim Anmelden von Benutzern am Netzwerk können die Benutzer durch die vorherige Zuweisung von Subnetzinformationen den nächsten Standort eines Domänencontrollers erreichen.

Der Systemadministrator verwendet das Snap-In Active Directory-Standorte und -Dienste, um die Topologie von Replikationsdiensten zu verwalten. Bei der internen Standortreplikation stellt die definierte Hochgeschwindigkeitsverbindung in der Regel eine schnelle Bereitstellung sicher. Bei der externen Standortreplikation ist die WAN-Bandbreite möglicherweise erheblich langsamer. Durch die Standortstruktur ist die Verwaltung der Zeitpläne für die Active Directory-Replikation zwischen Standorten möglich.

Bitte beachten Sie, dass es zwischen den Grenzen eines Standortes oder einer Domäne keine formale Beziehung gibt. Ein Standort kann über mehrere Domänen verfügen, eine Domäne kann mehrere Standorte enthalten. Darüber hinaus müssen Standorte und Domänen nicht denselben Namespace verwalten.

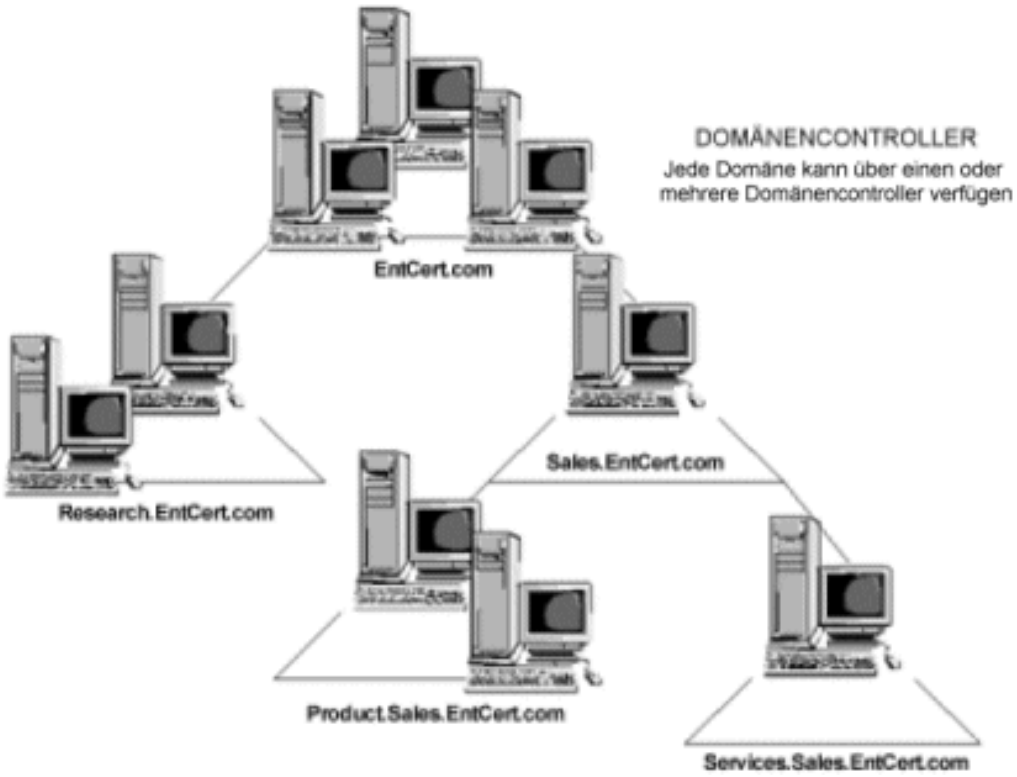




Domänencontroller

Ein Domänencontroller ist ein Server mit einer Kopie des Active Directory. Alle Domänencontroller sind Peers und verwalten replizierte Versionen des Active Directory für die Domäne. Der Domänencontroller spielt bei der logischen und der physischen Struktur des Active Directory eine wichtige Rolle. Er organisiert die Objektdaten der Domäne in einem logischen und hierarchischen Datenspeicher. Er wird zur Authentifizierung von Benutzern verwendet, bietet Antworten auf Abfragen zu Netzwerkobjekten und führt die Replikation von Verzeichnisdiensten durch. Die physische Struktur stellt die Mittel für die Übertragung dieser Daten über miteinander verbundene Standorte bereit.

Active Directory ersetzt den in Windows NT verwendeten Mechanismus als primären Domänencontroller (PDC) und sein Gegenstück, den Sicherungsdomänencontroller. Alle Domänencontroller verwenden nun gemeinsam eine Multimaster-Peer-to-Peer-Verknüpfung, die Kopien des Active Directory enthält. Ein weiterer großer Unterschied zu Windows NT besteht darin, dass alle Domänencontroller in Windows 2000 über Lese- und Schreibberechtigungen für das Active Directory verfügen. In älteren Versionen verfügte nur der PDC Lese- und Schreibberechtigungen und initiierte die Replikation. Jeder beliebige Active Directory-Domänencontroller kann den Replikationsvorgang initiieren, wenn neue Daten hinzugefügt werden.



Eine Active Directory-Domäne kann über einen oder mehrere Domänencontroller verfügen, die die Replikation der Verzeichnispartition bereitstellen. Aus folgenden Gründen kann eine Domäne über mehrere Domänencontroller verfügen:

- Am physischen Standort ist eine bessere Benutzerkonnektivität erforderlich.
- Der Umfang der Benutzeraktivität macht die Erstellung mehrerer Domänencontroller erforderlich.
- Der Wunsch nach verbessertem Failover und Redundanz von Informationen.

Beim Erstellen mehrerer Domänencontroller muss der Systemadministrator auch berücksichtigen, dass durch Replikationsverkehr die hinzugefügte Netzwerklast erhöht wird. Trotz dieser Erhöhung wird empfohlen, dass allen Domänen und alle Standort über mehrere Domänencontroller verfügen. Dadurch werden die Redundanz der logischen und physischen Struktur und Fehlertoleranz bereitgestellt. Sowohl wichtige Domäneninformationen als auch geografische Standortkonnektivität müssen geschützt werden.

Ein Domänencontroller wird während der Installation von Active Directory einem Standort zugewiesen. Der Speicherort des Standortes bleibt so lange unverändert, bis der Administrator manuell den Domänencontroller zu einem anderen Standort verschiebt. Der Speicherort eines Domänencontrollers an einem Standort ist Teil der Active Directory-Replikationstopologie und anderer Systemanforderungen.

Während die Zuweisung eines Domänencontrollers zu einem bestimmten Standort konsistent ist, können Clientsysteme geändert werden. Wenn ein Clientcomputer gestartet wird und durch DHCP eine IP-Adresse zugewiesen wird, kann die Standortmitgliedschaft zu einem anderen Subnetz wechseln.

Active Directory-Replikation

Die Active Directory-Replikation zwischen Domänencontrollern wird durch den Systemadministrator standortbasiert verwaltet. Wenn Domänencontroller hinzugefügt werden, muss ein Replikationspfad

eingerichtet werden. Die Konsistenzprüfung (Knowledge Consistency Checker, KCC) verwendet einen Prozess, der mit Komponenten der Active Directory-Replikation gekoppelt ist, um dieses Ziel zu erreichen. Bei der Konsistenzprüfung handelt es sich um einen dynamischen Prozess, der auf allen Domänencontrollern zum Erstellen und Ändern der Replikationstopologie ausgeführt wird. Falls ein Domänencontroller einen Fehler aufweist, erstellt die Konsistenzprüfung automatisch neue Pfade zu den verbleibenden Domänencontrollern. Der Systemadministrator kann auch manuell durch die Konsistenzprüfung einen neuen Pfad erzwingen.

Die Active Directory-Replikation verwendet RPC (Remote Procedure Call) über IP, um die Replikation innerhalb eines Standortes durchzuführen. Die standortübergreifende Replikation kann entweder RPC oder SMTP (Simple Mail Transfer Protocol) für die Datenübertragung zwischen Standorten verwenden. Standardmäßig wird bei der Replikation zwischen Standorten das Protokoll RPC verwendet. Wenn eine Replikation zwischen Domänen stattfinden soll, wird vom Active Directory nur SMTP verwendet.

Standortübergreifende und standortbegrenzte Replikation

Es gibt zwischen der internen und standortübergreifenden Replikation von Domänencontrollern unterschiedliche Replikationsaspekte zu beachten. Theoretisch ist die Netzwerkbandbreite an einem Standort für den gesamten Netzwerkverkehr ausreichend, der mit der Replikation und anderen Active Directory-Aktivitäten in Verbindung steht. Durch die Art der Definition eines Standortes muss das Netzwerk zuverlässig und schnell sein. Ein Prozess zur Änderungsbenachrichtigung wird initiiert, wenn Änderungen an einem Domänencontroller auftreten. Der Domänencontroller wartet einen konfigurierbaren Zeitraum, der standardmäßig fünf Minuten beträgt, bis eine Meldung an seine Replikationspartner weitergeleitet wird. Während dieses Zeitintervalls übernimmt der Domänencontroller weiterhin Änderungen. Sobald die Partnerdomänencontroller eine Meldung empfangen, kopieren sie die Änderung vom ursprünglichen Domänencontroller. Falls nicht genügend Änderungen während eines konfigurierbaren Zeitraumes gemeldet wurden (standardmäßig sechs Stunden), wird eine Replikationssequenz gestartet, um sicherzustellen, dass alle möglichen Änderungen mitgeteilt wurden. Bei der Replikation mit einem Standort werden nicht komprimierte Daten übertragen.

Bei der standortübergreifenden Replikation wird vorausgesetzt, dass möglicherweise Netzwerk-Konnektivitätsprobleme vorhanden sind, einschließlich unzureichender Bandbreite und Zuverlässigkeit und erhöhter Kosten. Daher lässt Active Directory zu, dass das System zur Art, Häufigkeit und dem Zeitpunkt der standortübergreifenden Replikation Entscheidungen trifft. Alle zwischen den Standorten übertragenen Replikationsobjekte sind komprimiert. Während dadurch die Menge des Datenverkehrs möglicherweise um 10 bis 25 % verringert wird, ist dies vermutlich nicht ausreichend, um eine ordnungsgemäße Replikation zu garantieren.

Verhindern von Konflikten bei der Datenreplikation

Active Directory gibt einen eindeutigen Bezeichner aus, der als USN (Update Sequence Number) bezeichnet wird. Jede an einem Objekt durchgeführte Änderung erhält eine USN. Diese Zahl wird dann schrittweise mit jeder nachfolgenden Änderung am Objekt erhöht. Für jede Eigenschaft eines Objekts wird ebenfalls eine USN ausgegeben. Eine Quelldomäne teilt dem Peer-Domänencontroller regelmäßig USN-Sequenzänderungen mit. Die neueste USN wird dann bei jedem Domänencontroller registriert, um den aktuellen Status eines Objekts sicherzustellen. Active Directory verwendet nur dann einen Zeitstempel, wenn fast zur gleichen Zeit Änderungen an einem Objekt durchgeführt werden. Um in

diesem Fall Datenkonflikte zu vermeiden, wird standardmäßig die Änderung mit dem neuesten Zeitstempel repliziert. In allen anderen Fällen beachtet Active Directory den Prozess der Zeitstempelvergabe nicht.

Besondere Rollen von Domänencontrollern

Einigen Domänencontrollern werden besondere Rollen zugewiesen, um eine bessere Leistung zu erzielen und Konflikte zu verringern. Während das Prinzip der Multimasterreplikation von Diensten über alle Domänencontroller die Grundlage von Active Directory bildet, werden bestimmte spezialisierte Funktionen am besten durch einen einzelnen Domänencontroller durchgeführt. Daher unterstützt Windows 2000 zwei Formen von spezialisierten Funktionen in Form des globalen Katalogs und der Domänencontroller-Betriebsmaster. Gesamtstrukturen (Forests) verwenden einen gemeinsamen globalen Katalog und gemeinsame Betriebsmaster.

Globaler Katalog

Der globale Katalog wurde für zwei wichtige Funktionen entworfen. Zunächst wird der Abfrageprozess für die Suche nach einem bestimmten Objekt durch die Identifikation von einem oder mehreren Attributen optimiert. Bei dem globalen Katalog handelt es sich um einen Domänencontroller, der Objektdaten speichert und Abfragen zu Objekten und ihren am häufigsten verwendeten Attributen verwaltet. Zweitens verfügt der globale Katalog über Daten, die die Anmeldung am Netzwerk ermöglichen. In einer Umgebung mit einem einzelnen Domänencontroller befinden sich das Active Directory und der globale Katalog auf demselben Server. Wenn mehrere Domänencontroller vorhanden sind, ist es in vielen Fällen ratsam, den globalen Katalog auf einen anderen Domänencontroller zu verschieben.

Alle Domänenstrukturen verfügen über einen globalen Katalog und müssen sich auf einem Domänencontroller befinden. Der globale Katalog speichert eine Sammlung von Informationen. Der globale Katalog speichert und repliziert Schemadaten und Konfigurationsdaten einer Domänengesamtstruktur. Der globale Katalog kann auch als Datenrepository und Modul für schnelle Objektsuchvorgänge gesehen werden. Der globale Katalog führt alle Objekte innerhalb einer Domänenstruktur oder -gesamtstruktur auf. Der Unterschied dieses Katalogs zum Active Directory besteht jedoch darin, dass er eine Liste mit einem Teil der Objektattribute enthält. Der globale Katalog enthält eine Liste der am häufigsten abgefragten oder verwendeten Objektattribute in einem abgekürzten Format, das aus einer Teilreplikation stammt. Da nur die am häufigsten abgefragten Elemente in den Katalog aufgenommen werden, kann der Speicherort von Objekten schneller aufgelöst werden, ohne dass die gesamte Quelldomäne durchsucht werden muss. Der Grund für einen dedizierten globalen Katalog liegt eindeutig darin, den Abfrageprozess von den Aktualisierungs- und Verwaltungsprozessen innerhalb eines Verzeichnisdienstes zu trennen.

Der globale Katalog unterstützt eine Reihe von standardmäßigen Objektattributen, die als am häufigsten verwendete oder abgefragte Attribute betrachtet werden. Der Vor- und Nachname von Benutzern kann beispielsweise unter diese Definition fallen. Um jedoch einer bessere Kontrolle über die definierten Attribute für eine bestimmte Domäne bereitzustellen, stellt Windows 2000 Mittel zum Ändern der Standardeinstellungen zur Verfügung. Der Systemadministrator kann das Snap-In Schemaverwaltung zum Aktualisieren der Attribute verwenden, die in der Replikation des globalen Katalogs enthalten sind.

Beim Auswählen eines Systems als Server für den globalen Katalog müssen die Kapazität und die Netzwerkkonnektivität beachtet werden. Das System sollte über ausreichende Speicherkapazität

verfügen, um die Verwaltung von mindestens einer Million Objekte zu unterstützen. Die CPU-Systemgeschwindigkeit sollte ausreichend sein, um die Verarbeitung eines stetigen Flusses von Abfragen zu ermöglichen. Microsoft gibt in seinen Publikationen 350-MHz-Systeme als ausreichend an.

Informationen zum Autor

Robert Williams ist geschäftsführender Gesellschafter von Enterprise Certified Corp. und ist unter bobw@EnterpriseCertified.com zu erreichen Dieser Artikel ist ein Ausschnitt aus *The Ultimate Windows 2000 System Administrator's Guide* ([englischsprachig], Williams & Walla, Addison Wesley 2000)