

Active Directory in Windows 2003

› Das Active Directory ist der zentrale Verzeichnisdienst von Windows Server 2003. Es sorgt für die Authentifizierung und gibt den Zugriff auf Ressourcen frei. Wir besprechen die beteiligten Komponenten und Funktionen.

› VON THOMAS WOELFER

Genau wie schon in Windows 2000 ist das Active Directory eine Schlüsselkomponente von Windows Server 2003. Bei Active Directory handelt es sich um einen Verzeichnisdienst, der zwei Netzwerkfunktionen erfüllt. Zum einen ist das die Möglichkeit des Single-Sign-on, und zum anderen lassen sich Ressourcen im Netzwerk gruppieren und besser auffinden.

Das Active Directory speichert Informationen über Objekte im Netzwerk. Bei diesen Objekten handelt es sich um User, User-Gruppen, Computer, Domänen, Organisationseinheiten und Sicherheitsoptionen. Diese Informationen können veröffentlicht werden und stehen dann den Nutzern des gesamten Netzwerks zur Verfügung.

Dabei werden die Informationen auf Rechnern gespeichert, die Domain-Controller (DC) genannt werden. Auf diese Informationen können Netzwerkanwendungen oder andere Dienste zugreifen. Jede Domain kann auch mehrere Domain-Controller haben. In diesem Fall werden die Informationen automatisch unter allen Controllern repliziert. Man kann eine Information also in einem beliebigen DC ändern, ohne sich um die anderen kümmern zu müssen. Diese erhalten ohne weiteres Zutun des Administrators die vorgenommenen Änderungen.

Sinnvollerweise betreibt man ein Active Directory aus Gründen der Verfügbarkeit mit mindestens zwei Domain-Controllern - fällt einer aus, so stehen die Informationen und Anmeldemöglichkeiten automatisch durch den zweiten Domain-Controller zur Verfügung, ohne dass die Nutzer davon etwas mitbekommen.

› Unterschiedliche Informationsarten

Die Daten, die zwischen den einzelnen Domain-Controllern repliziert werden, lassen sich in drei Gruppen unterteilen: Domain-spezifische Daten, Konfigurationsdaten und Schemadaten.

Bei den **Domain-spezifischen** Daten handelt es sich um Informationen über die Objekte in der Domain - also um Informationen, die man typischerweise in einem Verzeichnisdienst erwarten würde: E-Mail-Accounts, Benutzer- und Computerattribute sowie Ressourcen, die im Netz veröffentlicht wurden. Neu angelegte Benutzer landen in Form von Account-Daten und dazugehörigen Attributen in den Domain-Daten, Änderungen an solchen Daten spiegeln sich ebenso im Verzeichnis wider.

Bei den **Konfigurationsdaten** handelt es sich um Informationen über die Topologie des Verzeichnisses. Das sind zum Beispiel eine Liste aller zugehörigen Domains, eine Angabe über die Position der Domain-Controller und Informationen über die Position des globalen Katalogs.

Die **Schemadaten** sind eine formale Definition aller Objekte und Attribute, die im Verzeichnis gespeichert werden können. Dabei kommt der Windows Server 2003 mit einem vordefinierten Schema, in dem bereits eine ganze Reihe von Objekten und Attributen definiert ist. So enthält das Vorgabeschema von Haus aus Definitionen für

Benutzer, Computer und Sicherheitseinstellungen. Das Schema kann von Administratoren um eigene Definitionen erweitert werden, etwa vorhandene Objekte um neue Attribute. Auch neue Objekte lassen sich definieren. Im Normalfall wird man in einem kleinen Netz aber über die Vorgabe ausreichend mit Definitionen versorgt sein.

› Single Logon mit Authentifizierung

Das Active Directory verfügt über ein eingebautes Sicherheitsmodell, das auf Logon-Authentifizierung und Zugangskontrollen für Objekte im Netzwerk basiert. Ein angemeldeter Benutzer kann auf Objekte im ganzen Netzwerk zugreifen, sofern er die Zugangsrechte für die gewünschten Objekte besitzt. Dabei lassen sich Benutzer in Gruppen zusammenfassen, denen der Administrator Gruppenrechte erteilt. Hat eine bestimmte Gruppe also Zugriff auf eine bestimmte Ressource und gehört ein gegebener Benutzer zu dieser Gruppe, so hat er automatisch ebenfalls Zugriff auf diese Ressource.

Die Rolle des globalen Katalogs

Beim globalen Katalog handelt es sich um einen Domain-Controller, der eine Kopie aller Objekte des Active Directory speichert. Außerdem enthält er die am häufigsten gesuchten Attribute aller Objekte im Verzeichnis. Der globale Katalog wird automatisch auf dem ersten DC im Verzeichnis angelegt.

Zentrale Auskunft: Der globale Katalog kann nach beliebigen Informationen durchsucht werden.

Das Auffinden von Objekten ist die wichtigste Funktion des globalen Katalogs im Active Directory. Sucht beispielsweise ein Benutzer einen Drucker "im Verzeichnis", so wird diese Suche an den globalen Katalog delegiert. Die Suche lässt sich über das Startmenü oder sonst eine Anwendung starten, die mit Active Directory umgehen kann. Sie wird dabei in allen Domains durchgeführt, die am Active Directory eines Netzwerks beteiligt sind. Die jeweiligen zugehörigen Domain-Controller kommen dabei nicht zum Einsatz: Nur der globale Katalog selbst wird für die Suche verwendet. Das beschleunigt das Auffinden der Ergebnisse.

Da das Active Directory eine ganze Menge an Informationen über die User (beziehungsweise Objekte) im Netzwerk speichern kann, dient das Verzeichnis praktisch auch als globales Adressbuch des Netzwerks. Die Suchfunktion erlaubt es, nach einer Vielzahl von Informationen zu suchen: So können Personen beispielsweise nach Ihrem Nachnamen, ihrer E-Mail-Adresse oder anderen personenbezogenen Daten gesucht

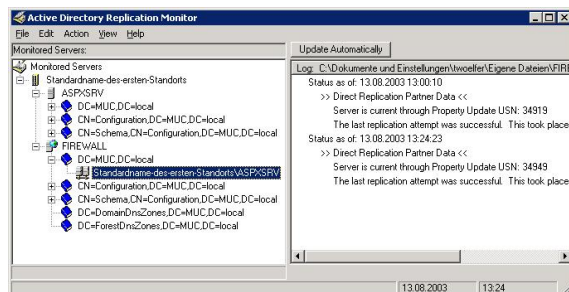
werden.

Will eine Anwendung nach Objekten im Netzwerk suchen, greift sie dafür auf das Active Directory Service Interface (ADSI) zurück.

› Replikation zwischen Domain-Controllern

Die automatische Replikation von Informationen zwischen Domain-Controllern im Active Directory umfasst mehrere Arten von Informationen: Schemadaten, Konfigurationsinformationen, Domain-Informationen und Anwendungsinformationen. Dabei können (beinahe) beliebig viele Domain-Controller gleichzeitig im Netz betrieben werden. Dieses Verfahren heißt Multi-Master-Replikation. Bei Windows 2000 gab es das noch nicht, so dass dort Veränderungen am Verzeichnis nur auf einem speziellen Rechner, dem Master Domain Controller, vorgenommen werden durften. Windows Server 2003 hingegen erlaubt die Veränderung der Informationen an einem beliebigen Domain-Controller.

Die Schemadaten und die Konfigurationsinformationen werden zwischen allen Domain-Controllern im so genannten Forest repliziert. Ein Forest setzt sich aus einer Sammlung von Domains zusammen.

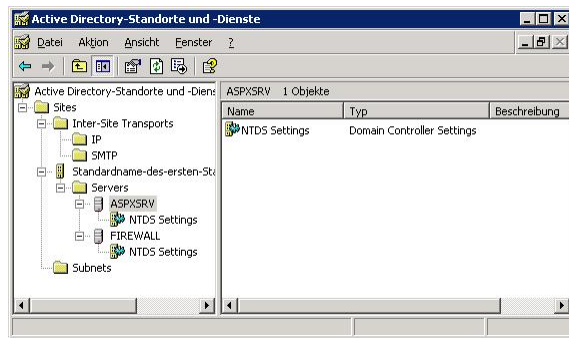


Die Replikation erfolgt automatisch: Mit dem Replication Monitor kann man die Schritte überwachen.

Die Domain-Informationen sind hingegen für jede Domain spezifisch und werden darum nur zwischen Domain-Controllern der gleichen Domain repliziert. Für die Suchfunktion wird jedoch eine Untermenge der Daten im globalen Katalog gesammelt. Die Suche erfolgt also immer im kompletten Forest beziehungsweise in allen Domains.

› Optimierung der Replikation

Die Replikation der Informationen im Netz kann dabei durch die Verwendung von so genannten Sites optimiert werden: Sites strukturieren die Hosts im Active Directory anhand ihrer Netzwerkverbindungen. Innerhalb einer Site werden Daten häufiger repliziert als zwischen verschiedenen Sites. Bei der Replikation zwischen Sites werden die Daten obendrein komprimiert, was die benötigte Bandbreite weiter verringert. Die Aufteilung eines Active Directory in Sites ist zum Beispiel dann sinnvoll, wenn es mehrere geografisch voneinander getrennte lokale Netze gibt, die dennoch zu einem gemeinsamen Active Directory gehören: Zwischen diesen örtlich getrennten Netzen besteht tendenziell nur eine langsame Netzwerkverbindung - daher wird man für diese Verbindung nur ein Minimum an Datentransfer wünschen.



Räumliche Einteilung: Um den Netzwerk-Traffic zwischen verschiedenen Standorten zu reduzieren, lassen sich in Windows 2003 so genannte Sites definieren.

Gleichzeitig ist es in einem solchen Fall so, dass alle beteiligten Sites wohl über einen eigenen Administrator verfügen: Legt der Administrator einer Site einen neuen Benutzer an, dann erfahren das die Domain-Controller innerhalb dieser Site am schnellsten. Da es aber ohnehin die Domain-Controller sein werden, bei denen sich der neue Benutzer anmeldet, spielt es keine große Rolle, dass die anderen Sites die neuen Benutzerinformationen erst ein wenig später erhalten.

› Besondere Server: Betriebs-Master-Funktionen

Das Active Directory unterstützt wie erwähnt die Multi-Master-Replikation der Daten des Verzeichnisses zwischen allen Controllern in der Domäne. Dabei sind im Prinzip alle Controller untereinander Peers. Allerdings gibt es einige wenige Änderungen, die nicht auf einem beliebigen Domain-Controller durchgeführt werden können. Stattdessen müssen diese auf einem speziellen Host, dem so genannten Betriebs-Master, durchgeführt werden. Andere Domain-Controller akzeptieren diese Änderungen nicht. Der Betriebs-Master hat fünf unterschiedliche Funktionen, die so genannten Betriebs-Master-Funktionen. Diese heißen in der Literatur auch manchmal FSMO-Funktionen (Flexible Single Master Operations). Diese Funktionen sind zwar auf mehrere Domain-Controller verteilbar - es darf aber immer nur einen Domain-Controller geben, der eine bestimmte Funktion ausübt.

Der Schema-Master

Der DC mit der Funktion des Schema-Masters verwaltet alle Änderungen und Aktualisierungen am Schema. Da das Schema zur Gesamtstruktur des Active Directory gehört, kann es insgesamt nur einen Schema-Master geben. Um das Schema zu ändern oder zu erweitern, ist der Zugriff (und das Zugriffsrecht) auf den Schema-Master notwendig.

Der Domain-Namen-Master

Der DC, der als Domain-Namen-Master fungiert, ist für die Verwaltung der Domain-Namen der Gesamtstruktur des Active Directory zuständig. Soll eine neue Domain zum Verzeichnis hinzukommen oder soll eine vorhandene gelöscht oder umbenannt werden, so muss dies mit Hilfe des Domain-Namen-Masters geschehen. Genau wie beim Schema-Master kann es in der Gesamtstruktur des Verzeichnisses nur einen Domain-Namen-Master geben.

› Domain-weite Betriebs-Master

Die weiteren Betriebs-Master-Funktionen sind nicht auf die Gesamtstruktur anzuwenden, sondern beziehen sich auf einzelne Domains. Jede Domain innerhalb der Gesamtstruktur muss genau einen Domain-Controller mit den folgenden Betriebs-Master-Funktionen enthalten:

Der RID-Master

Der RID-Master (RID = Relative ID) ist für die Vergabe von eindeutigen IDs für alle Domain-Controller einer Domain zuständig. Diese IDs werden zum Beispiel später beim Anlegen von SIDs (Security ID) für neue Objekte im Verzeichnis beziehungsweise der

Domäne benötigt.

Der PDC-Emulations-Master

Der PDC-Emulations-Master emuliert, wie der Name schon vermuten lässt, einen Primary Domain Controller (PDC). Gibt es im Netz NT4-Workstations, dann brauchen diese einen PDC. Da der Windows 2003 Server das Konzept der PDCs nicht mehr kennt, emuliert der PDC-Emulations-Master eben einen solchen.

Sind im Netz auch noch BDC (Backup Domain-Controller) vorhanden, repliziert der PDC-Emulations-Master Änderungen auf diese Rechner.

Darüber hinaus ist der PDC-Emulations-Master auch der Rechner, der für das Synchronisieren der Zeit auf den Domain-Controllern zuständig ist. Wird die Zeit auf dem PDC-Emulator mit einer externen Zeitquelle synchronisiert (» *net time *SERVERNAME*> /setsntp: <Zeitserver> «), haben alle Rechner automatisch die richtige Uhrzeit.*

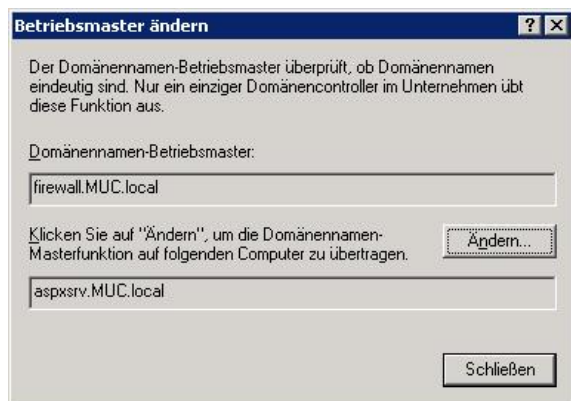
Der Infrastruktur-Master

In jeder Domäne kann immer nur ein DC die Funktion des Infrastruktur-Masters übernehmen. Er dient dazu, Objektreferenzen in seiner Domäne auf Objekte in anderen Domänen zu aktualisieren. Dabei vergleicht er seine Daten mit denen eines globalen Katalogs. Im Zuge der Replikation empfangen globale Kataloge in regelmäßigen Abständen Aktualisierungen zu Objekten in allen Domänen, so dass die Daten des globalen Katalogs stets auf dem neuesten Stand sind.

Der Infrastruktur-Master sucht veraltete Daten und fordert die aktualisierten Daten von einem globalen Katalog an. Anschließend werden diese aktualisierten Daten vom Infrastruktur-Master auf die anderen Domain-Controller in der Domäne repliziert.

› Ausfälle des Betriebs-Masters

Fällt ein Betriebs-Master aus, so ist das alles andere als unterhaltsam, denn ohne ihn ist das Netzwerk mit dem Active Directory nicht nutzbar. Bei allen anderen Funktionen des Active Directory ist der Ausfall eines Domain-Controllers hingegen kein Problem, denn dann übernimmt einfach ein anderer Domain-Controller im Netz dessen Aufgaben.



Übertragung: Ist der alte Rechner noch vorhanden, kann der Betriebs-Master ganz einfach verändert werden.

Muss eine Betriebs-Master-Funktion von einem Rechner auf einen anderen übertragen werden, kann das zwei Gründe haben: Entweder der Rechner oder die Zugänge zu diesem sind längerfristig ausgefallen, und er ist nicht mehr verfügbar, oder er soll durch einen anderen ersetzt werden. Dementsprechend gibt es zwei unterschiedliche Arten, wie man die Betriebs-Master-Funktionalität auf einen neuen Host bekommt. Steht der ursprüngliche Betriebs-Master noch zur Verfügung, so nennt man den Übergabevorgang "Übertragung". Ist der ursprüngliche Rechner dagegen nicht mehr verfügbar, heißt das "Übernahme" oder "erzwungene Übertragung".

Das Übertragen ist ein relativ einfacher Vorgang, den Sie direkt mit der jeweils passenden MMC des Active Directory durchführen können. Den Schema-Master übertragen Sie mit der Konsole für das Active-Directory-Schema, den Domänen-Master mit "Active Directory Domänen und Vertrauensstellungen" und die anderen

Betriebs-Master-Funktionen mit der Konsole "Active Directory Benutzer und Computer".

Die erzwungene Übertragung ist hingegen etwas komplizierter: Schließlich liegt der eigentliche Betriebs-Master ja nicht länger vor.

› Ausfall des Schema-Masters

Fällt der Schema-Master nur temporär aus, bemerken die Benutzer des Netzwerks das in der Regel überhaupt nicht. Nur wenn Sie versuchen, das Schema zu verändern, macht sich das Fehlen des Schema-Masters bemerkbar. Das kann auch bei der Installation einer Anwendung passieren, da AD-Anwendungen oft eigene Schema-Erweiterungen einbringen wollen. Selbst wenn Sie das Schema nicht verändern wollen, sollten Sie einen ausgefallenen Schema-Master durch einen neuen Host ersetzen. Dabei ist eines wichtig: Der ursprünglich als Schema-Master betriebene Domain-Controller darf nie wieder in das Netzwerk gestellt werden, ansonsten treten massive Störungen auf.

Um einen neuen Rechner als Schema-Master festzulegen, benötigen Sie das Kommandozeilentool » *ntdsutil* « . Dabei handelt es sich um ein Kommandozeilenprogramm, das einen eigenen Prompt anzeigt. Starten Sie das Programm auf dem Domain-Controller, der in Zukunft Schema-Master sein soll. Eine ausführliche Anleitung zur Verwendung dieses Programms bei der Übernahme der Schema-Master-Betriebsfunktion finden Sie in der Online-Hilfe zum Active Directory.

› Ausfall des Domänen-Namen-Masters

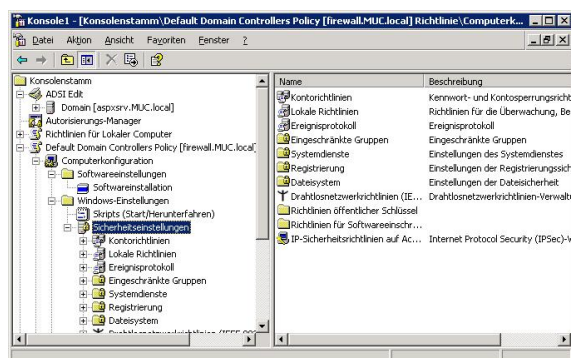
Genau wie beim Schema-Master macht sich der temporäre Ausfall des Domain-Namen-Masters für Benutzer des Netzwerks zunächst nicht bemerkbar. Erst wenn der Administrator versucht, eine Domäne hinzuzufügen oder zu entfernen, tritt ein Problem auf.

Ähnlich wie beim Schema-Master übernehmen Sie mit einem neuen Domain-Controller die Namen-Master-Funktion mit dem Programm » *ntdsutil* « - auch dazu finden Sie eine Beschreibung in der Online-Hilfe zum Active Directory. Suchen Sie dazu einfach nach den Begriffen "übernehmen domänennamen master".

Auch wenn der PDC-Emulations-Master und der Infrastruktur-Master ausfallen, können Sie deren Aufgaben von einem anderen DC übernehmen lassen: Anders als beim Schema-Master und beim Domänennamen-Master kann diese Betriebsfunktion später aber wieder an den ursprünglichen DC zurückübergeben werden, sobald dieser wieder verfügbar ist.

› Integrierte Gruppenrichtlinien

Gruppenrichtlinien (Group Policies) sind fest in das Active Directory integriert. Dazu gibt es ein eigenes Snap-in für die MMC, mit dem Administratoren Standardeinstellungen festlegen können. Diese werden dann automatisch auf Benutzer- beziehungsweise Computerkonten im Active Directory angewendet. Die Gruppenrichtlinien beeinflussen eine Vielzahl der Funktionen der Windows-Desktops im Active Directory: Angefangen von der Darstellung der Benutzeroberfläche bis hin zu Sicherheitseinstellungen lassen sich die Parameter verzeichnisweit festlegen.



Sicherheitszentrale: Die Gruppenrichtlinien werden mit einem separaten Snap-in festgelegt und gelten für alle entsprechenden Stationen und Benutzer.

Damit kann der Administrator detailliert Einfluss darauf nehmen, was ein einzelner Benutzer auf dem Rechner machen darf und was nicht. Auch bei der Sicherheitskonfiguration des Internet Explorer beispielsweise hat der Administrator weit reichende Eingriffsmöglichkeiten. Und das ist gerade angesichts der immer wieder auftretenden schweren Lücken im IE sehr hilfreich.

Mit dem Active Directory bietet Windows Server 2003 einen umfangreichen, selbstschützenden Verzeichnisdienst, der nicht nur zum Auffinden von Personen, sondern auch als Adressbuch im Netzwerk verwendet werden kann. In einem späteren Beitrag auf tecChannel.de erfahren Sie mehr über die Praxis der Arbeit mit dem Active Directory in Windows 2003. (mha)

› Weitere Themen zu diesem Artikel:

So funktionieren Verzeichnisdienste (<http://www.tecchannel.de/internet/718/index.html>)

Copyright © 2001

IDG Interactive GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Interactive GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in tecChannel unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von tecChannel aus gelinkt wird, übernimmt die IDG Interactive GmbH keine Verantwortung.