

# Active-Directory-Verwaltung in Windows 2003

› Mit dem Active Directory verwalten Sie beim Windows 2003 Server Computer und Benutzerkonten. Welche Management-Konsole für welche Aufgabe zuständig ist, zeigt dieser Beitrag.

› VON THOMAS WOELFER

Um das Active Directory benutzen zu können, müssen Sie auf einem Windows 2003 Server - dabei gehen alle Versionen außer der Web-Edition - in der Server-Verwaltung die Funktion "Domänencontroller (Active Directory) installieren" auswählen. Dadurch ernennen Sie diesen Server zum Domain-Controller, der dann die Active-Directory-Funktionen zur Verfügung stellt.

Im Zuge der Installation werden automatisch alle lokalen Benutzerkonten gelöscht: Auf einem Active-Directory-Server können nur noch Active-Directory-Konten verwendet werden. Das schafft gleich das erste Problem bei der Arbeit mit dem Active Directory: Direkt nach der Installation des Domänen-Controllers tritt es ein.



Anzeige

Im Zuge der Erstinstallation hat man ein Administrator-Passwort vergeben und will nun weitere User einrichten. Doch die Benutzerverwaltung ist nicht aufzufinden. Es gibt keinen entsprechenden Eintrag im Startmenü, und auch der gewohnte Ast in der Computerverwaltung ist verschwunden. Das ist ärgerlich, denn ohne die Möglichkeit, User-Accounts einzurichten, macht die ganze Sache nicht viel Sinn. Was ist also zu tun?

Die Antwort auf diese Frage wirft ein klares Licht auf die Veränderung eines Netzwerks durch die Einführung von Active Directory: Es gibt keine "alte" Benutzerverwaltung mehr. Genauso wenig wie einen Server-Manager und ähnliche Komponenten aus der Zeit vor dem Active Directory, denn die Verwaltung der Accounts - genau wie die der Rechner im LAN - erfolgt ab sofort über das Active Directory.

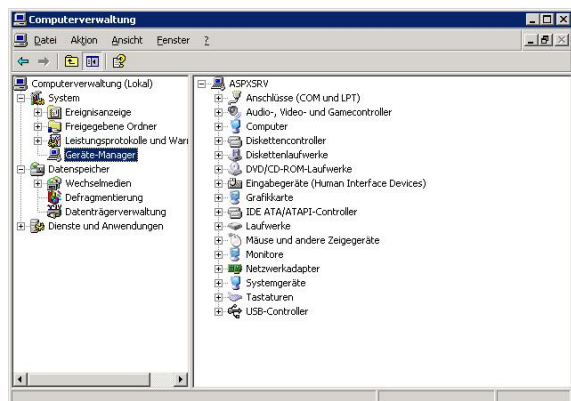
## › Aus für den Benutzer-Manager

Der Benutzer-Manager ist also überflüssig und daher weggefallen - dafür gibt es aber drei neue Anwendungen im Menü "Verwaltung", die mit dem Active Directory zu tun haben. Bei den drei Anwendungen handelt es sich um "Active Directory Standorte und Dienste", "Active Directory Domänen und Vertrauensstellungen" sowie "Active Directory Benutzer- und Computer".

Bevor Sie nun diese drei Anwendungen untersuchen, sollten Sie zunächst über eine weit wichtigere Angelegenheit als über das Anlegen neuer Accounts nachdenken: die Sicherung Ihres Active Directory.

Das Active Directory wird im Laufe der Zeit alle Informationen über Server, Active-Directory-Server, sonstige Computer sowie über die Benutzer aufnehmen. Diese Informationen sind obendrein mit einer Vielzahl von Eigenschaften ausgestattet: Ein Benutzer-Account ist beispielsweise nicht einfach nur eine Kombination aus User-Name und Passwort, sondern enthält ein Menge zusätzlicher Daten, wie etwa E-Mail, Telefonnummer und postalische Adresse oder auch Angaben über die Art und Weise der

Computerbenutzung. Dazu zählen zum Beispiel RAS-Rückrufmöglichkeiten, Anmelde-Scripts und auch ein spezielles Profil für die Nutzung von Terminaldiensten.



Entfernt: Den Benutzer-Manager sucht man auf einem Domain-Controller vergeblich.

Obendrein ist ein Benutzer-Account natürlich auch mit Rechten ausgestattet. Diese Rechte legen fest, auf welche Ressourcen der Benutzer wann und in welcher Art und Weise zugreifen darf. Dabei erfolgt die Rechtevergabe auf der Basis von Gruppenmitgliedschaften: Sie werden später bestimmte Benutzergruppen anlegen und diese mit Zugriffsrechten versehen. Die einzelnen Accounts werden Mitglied einer oder mehrerer Benutzergruppen und erhalten dadurch die Rechte und Beschränkungen dieser Gruppen.

### › Gleicher Name, anderer Account

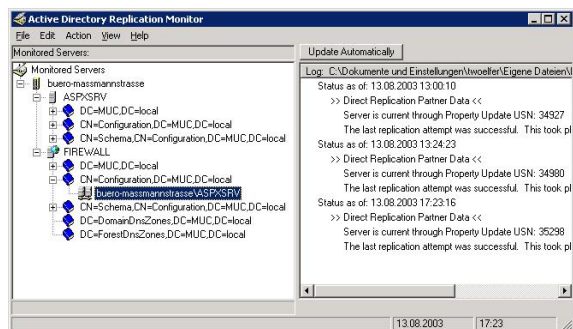
Wenn Sie einen Account aus dem Active Directory entfernen, können Sie zwar wieder einen neuen mit demselben Namen anlegen, aber effektiv handelt es sich dabei um einen komplett neuen Account. Dieser hat - trotz gleicher Anmelde-Informationen - keinen Zugriff auf die privaten Daten und Einstellungen des alten Accounts. Mit anderen Worten: Der Zugriff auf E-Mails, Anwendungskonfigurationen oder das Windows-Adressbuch ist versperrt. Um den alten Zustand wieder herzustellen, müssten Sie alle Daten zusammensuchen, die Rechte daran manuell übernehmen und dann an den neuen Account weitergeben.

Nun sind aber wie erwähnt alle Account-Informationen im Domain-Controller abgelegt. Fällt dieser aus, ist der Schaden groß: Installiert man dann nämlich - was sollte man auch anderes tun - einen neuen Domain-Controller auf einem neuen Rechner, dann sind alle Benutzer- und Computerkonten verschwunden. Um das Netz dann wieder in den Griff zu bekommen, muss man die privaten Daten aller Anwender im Netzwerk auf allen lokalen Workstations wieder manuell an deren Eigentümer übertragen: Eine Menge Arbeit für einen kleinen Festplattendefekt.

Dieses Problem ist auch Microsoft klar, und darum gibt es dafür eine einfache Lösung: Man installiert mindestens zwei Domain-Controller im Netzwerk. Sie synchronisieren sich völlig selbstständig und ohne weiteres Zutun seitens des Administrators. In der Praxis kann man auch beliebig viele Domain-Controller installieren - aber für ein kleines Netz reichen auch zwei.

### › Das Minimum: Zwei Domain-Controller

Wenn Sie erwägen, Active Directory für Ihr Netzwerk zu nutzen - und sei es noch so klein - dann sollten Sie auf jeden Fall von Haus aus davon ausgehen, dass Sie mindestens zwei Rechner dafür bereitstellen müssen. Mit weniger Hardware macht die Sache keinen Sinn. Diesem Rat sollten sie folgen, bevor Sie die tatsächliche Arbeit mit dem Active Directory beginnen: Installieren Sie zwei Domain-Controller im Netz und beginnen Sie erst danach mit der Konfiguration - das macht auf Dauer ganz sicher weniger Ärger. Außerdem kann man dann die Installation des zweiten Rechners nicht einfach "vergessen".



**Big Brother: Die Replikation zwischen den Servern kann man leicht mitverfolgen.**

Die beiden Server synchronisieren sich dabei völlig selbstständig. Sie können also zum Beispiel einen Account auf einem der Domain-Controller neu anlegen, während Sie einen anderen Account auf dem zweiten Domain-Controller löschen: Nach kurzer Zeit haben die beiden Controller wieder die gleichen Informationen - und zwar einschließlich des gelöschten und des neu angelegten Benutzers.

Die Replikation können Sie übrigens auch quasi live überwachen: Dazu gibt es auf der Windows-2003-CD im Verzeichnis *Tools* ein eigenes GUI-Programm, mit dem sich die einzelnen Replikationsschritte verfolgen lassen.

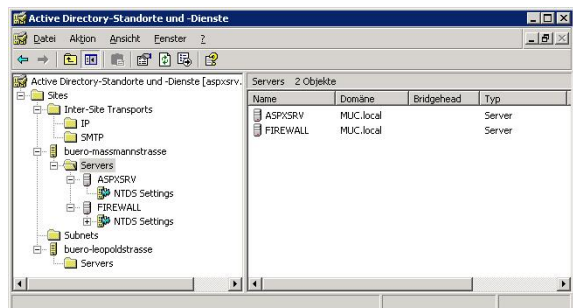
Die Verwaltung der Domain-Controller erledigen Sie am besten über einen *Remote Desktop*: Dadurch brauchen Sie nicht erst zum Server zu laufen, sondern können alle Aufgaben direkt von Ihrer Workstation aus erledigen. Da Konfigurationsänderungen nach der Installation in der Praxis so gut wie nie einen Reboot erfordern, haben Sie mit dem Remote Desktop de facto alle Konfigurationsmöglichkeiten, die Sie bei physischer Anwesenheit vor dem Server hätten.

Mit der Sicherheit zweier Active-Directory-Server im Rücken können Sie nun mit der eigentlichen Arbeit beginnen.

## › Active Directory-Standorte und -Dienste

Mit dieser Anwendung erstellen Sie neue Standorte, konfigurieren die Replikation zwischen Standorten und Domain-Controllern eines Standortes und weisen Gruppenrichtlinien für einen Standort zu.

Unter einem Standort können Sie sich genau das vorstellen, was der Name besagt: Es handelt sich um einen geographischen Ort, an dem mehrere Rechner zu einem Netz oder Subnetz zusammengefasst sind. Wenn Sie nur über ein kleines Netz - zum Beispiel im Büro - verfügen, brauchen Sie auch nur einen Standort.



**Standort-Verwaltung: Die einzelnen Standorte und die Replikation regulieren Sie mit dieser Management-Konsole.**

Für den Betrieb eines Standortes brauchen Sie mindestens einen Domain-Controller. Aus den bereits geschilderten Sicherheitsüberlegungen heraus sollten Sie aber mindestens zwei verwenden.

Bei der Installation des Active Directory über die Server-Verwaltung wird automatisch ein Standort angelegt. Dieser hat immer die Bezeichnung

"Standardname-des-ersten-Standortes". Diesen Namen müssen Sie aber nicht beibehalten, sondern können ihn per Rechtsklick in der Management-Konsole ändern.

Innerhalb des Astes dieses Standorts finden Sie einen Ordner mit dem Namen "Servers". Dieser Ordner enthält Verknüpfungen zu jedem Domain-Controller des Standortes, und für jeden Server gibt es einen weiteren Ordner für die Verbindungen zu anderen Servern. Per Default werden hier bei zwei Servern bereits automatisch Verbindungen hergestellt. Mit diesen Verbindungen legen Sie fest, auf welche Art und Weise die Replikation der Daten im Active Directory erfolgt. In einem kleinen Netz mit nur zwei Domain-Controllern werden Sie sich mit dieser Problematik nicht weiter auseinander setzen müssen: Die im Zuge der Installation vorgenommenen Einstellungen sind für den stabilen Betrieb des Netzes völlig ausreichend.

### › Active Directory: Domänen und Vertrauensstellungen

Auch diese Anwendung werden Sie eher selten benötigen, zumindest wenn Sie nur über ein kleines Netz verfügen. Die Anwendung dient der Verwaltung von Domänen und Gesamtstrukturen. Eine Domäne kann sich dabei aus mehreren Standorten zusammensetzen.

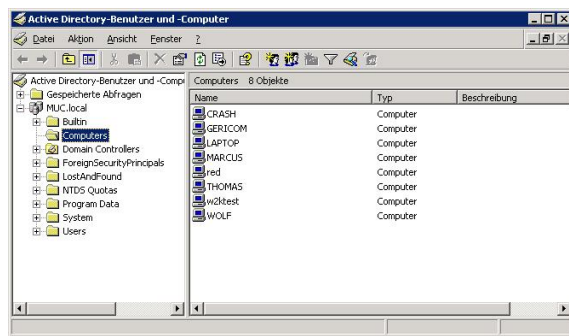
Mit der Konsole gestalten Sie die Zusammensetzung einer Gesamtstruktur. Ferner legen Sie hier die Betriebs-Master für die Domänen fest - und außerdem bestimmen Sie damit, in welchem Modus Ihr Active Directory ausgeführt wird. Dieser Modus ist in erster Linie davon abhängig, welche anderen Server sich noch in Ihrem Netzwerk befinden: Gibt es zum Beispiel noch Windows 2000 Server, dann können Sie kein reines Windows-2003-Active Directory benutzen, sondern brauchen einen Mischmodus - oder den reinen Windows-2000-Modus. Bestimmte neue Features des AD von Windows 2003 sind allerdings nur in Umgebungen nutzbar, die rein aus Windows 2003-Servern bestehen. Das sind beispielsweise das Handling von "Multi-valued Attributes" und der verbesserte Algorithmus des Intersite Topology Generator zur Optimierung der Replikation. Auch der Domain-Name darf nur in reinen Windows-2003-Umgebungen verändert werden.

Werden die Windows-2000-Server dann später aus dem Netz entfernt, können Sie den Mischmodus zu einem vollständigen Windows-2003-Server-Modus heraufstufen: Das macht man natürlich nicht sonderlich oft. Mit anderen Worten: Diese Konsole werden Sie im Normalfall nach der Installation des Active Directory getrost vergessen können. Müssen Sie hingegen mehrere Domänen verwalten und zusammenfassen, finden Sie die grundlegenden Konzepte dafür in der Online-Hilfe zu dieser Konsole.

### › Active Directory: Benutzer und Computer

Diese Konsole ersetzt im Wesentlichen die Benutzer- und die Server-Verwaltung aus den älteren Windows-Server-Versionen. Dabei wird zwischen "Computers", "Domain Controllers" und "Users" unterschieden - die Domain-Controller in Ihrem Netz sind zwar auch Computer, aber im entsprechenden Ordner nicht enthalten.

Außerdem gibt es noch einen Ordner "Builtin", der die vordefinierten Benutzergruppen enthält. Für die Rechtevergabe beim Anlegen neuer Accounts können Sie dann entweder eine oder mehrere Gruppen aus dieser Liste auswählen, oder Sie definieren eine eigene Gruppe mit selbst eingestellten Rechten. Dazu klicken Sie einfach mit der rechten Maustaste in den rechten Bereich der Konsole und wählen den Befehl "Neu/Group".



**Integriert: Die Benutzer und Computer verwalten Sie mit dieser Konsole.**

In der Gruppe "Computers" finden Sie eine Liste aller Computer in Ihrem Netzwerk. Nur die Computer in dieser Liste nehmen am Active Directory teil. Sie können die Computer vollständig über diese Liste verwalten. Dazu klicken Sie einfach mit der rechten Maustaste auf den zu verwaltenden Computer und wählen den passenden Befehl. Der öffnet dann die Computerverwaltung für den ausgewählten Computer: Dort können Sie wie gewohnt Dienste starten, anhalten und stoppen, die Leistungsprotokolle überprüfen oder auch Einsicht in die Ereignisanzeige des Computers nehmen.

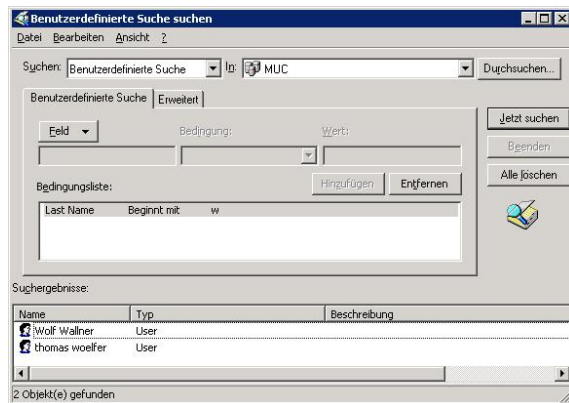
Die einzige Ausnahme bildet dabei der Geräte-Manager, denn er wird nur im Read-only-Modus ausgeführt: Da man über eine Remote-Verbindung allerdings ohnehin nur schwerlich irgendwelche Hardware aktualisieren kann, ist das wohl eher kein Problem.

Im Ordner für "Domain Controllers" tut sich nichts besonders Bemerkenswertes: Auch hier lassen sich die Rechner normal verwalten - funktional unterscheidet sich dieser Ordner nicht von "Computers".

Im Ordner "Users" erstellen, bearbeiten oder löschen Sie Benutzer-Accounts. Ein Account ist dabei im Wesentlichen die Kombination aus Benutzername und Passwort, hat aber noch eine große Menge an zusätzlichen zugeordneten Informationen. Die wichtigste davon ist die Gruppenzugehörigkeit: Diese legt Rechte und Einschränkungen fest. Da sich das Active Directory sehr gut durchsuchen lässt, empfiehlt es sich, hier so viele Informationen wie möglich über einen User beziehungsweise einen Account abzulegen - also beispielsweise die E-Mail-Adresse oder Telefonnummern. Haben Sie das getan, können Sie das Active Directory später als Adress- und Kontaktverzeichnis für die Nutzer Ihres Netzwerkes einsetzen, ohne auf spezielle weiter gehende Programme zurückgreifen zu müssen.

### › Die Suche im Active Directory

Um ein Objekt im Active Directory zu suchen, verwenden Sie einfach den Befehl "Suchen" in der Management-Konsole. Sie können dabei in allen vorhandenen Kategorien - also zum Beispiel Drucker, Benutzer, Computer und so weiter - nach verschiedenen Eigenschaften suchen. Dabei ist auch die Verwendung von Wildcards möglich. Wenn Sie zum Beispiel nach einem Drucker suchen, dessen Namen Sie nicht mehr genau kennen, von dem Sie aber wissen, dass es sich um einen HP-Drucker handelt, dessen Bezeichnung mit dem Kürzel HP beginnt, wählen Sie als Kategorie "Drucker" aus und geben als Name "HP\*" an: Das Suchresultat liefert Ihnen dann alle Drucker im Verzeichnis, die mit der Zeichenfolge "HP" beginnen.



**Gesucht - gefunden:** Mit der benutzerdefinierten Suche können Sie das Active Directory nach beliebigen Kriterien untersuchen.

Ein Sonderfall ist die "Benutzerdefinierte Suche", die einfach als Kategorie in der Kombo-Box neben dem Wort "Suche" aufgelistet ist. Damit können Sie nach beliebigen Attributen von Objekten suchen - so zum Beispiel nach den Initialen eines Benutzers oder auch nach Benutzern, deren Telefonnummern mit bestimmten Nummernkombinationen beginnen.

### › Fazit

Mit dem Active Directory haben Sie bei Windows 2003 einen einfach zu verwaltenden, aber dennoch mächtigen Verzeichnisdienst an der Hand, mit dem Sie nicht nur die Rechte von Benutzern, sondern auch die am Netzwerk teilnehmenden Computer einfach und schnell verwalten können. Die automatische Replikation der verwendeten Domain-Controller schafft außerdem ein vernünftiges Maß an Ausfallsicherheit: Die Verwaltung des Netzwerks wird mit dem Active Directory des Windows 2003 Server tatsächlich deutlich einfacher als ohne. (mha)

### › Weitere Themen zu diesem Artikel:

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

Active Directory in Windows 2003 (<http://www.tecchannel.de/betriebssysteme/1230/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.