TEC WORKSHOP

Link: https://www.tecchannel.de/a/active-directory-unentbehrliche-helfer-fuer-admins,443285

Active Directory: Unentbehrliche Helfer für Admins

Datum: 24.07.2006
Autor(en): Thomas Wölfer

Für das Active Directory liefert Microsoft nicht nur die beigepackten Verwaltungsprogramme mit, sondern hat auch weitere Werkzeuge zu bieten. Leider sind diese Tools teilweise gut versteckt. In diesem Beitrag erfahren Sie, wo Sie die Tools finden und wie Sie die wichtigsten Werkzeuge richtig nutzen.

Genau wie schon in Windows 2000 ist das Active Directory (AD) eine Schlüsselkomponente von Windows Server 2003. Darin sind User, User-Gruppen, Computer, Domänen, Organisationseinheiten und Sicherheitsoptionen gesichert. Weil Active Directory dementsprechend wichtig und umfangreich ist, kommt der Wartung eine zentrale Rolle zu. Neben den allgemein bekannten Tools gibt es eine ganze Reihe von zusätzlichen Programmen, die das Leben des Administrators deutlich erleichtern.

Microsoft hat die Werkzeuge für Active Directory allerdings ungeschickt platziert: Teilweise stecken sie in den Windows Support Tools, die sich auf der CD befinden, und zum Teil finden sie sich in den Tools des Windows Server Resource Kits, die man etwa bei **Microsoft herunterladen kann**[1].

Abgesehen davon, dass die Tools in verschiedenen Verpackungen auftauchen, wirken sie auch ein wenig so, als hätte es keine besondere Planung bei der Herstellung gegeben: Die Funktionalität der Programme überlappt sich teilweise, und Programme, die als Kommandozeilen-Alternative für GUI-Lösungen vorgestellt werden, stellen zum Teil nicht den kompletten Funktionsumfang zur Verfügung – und umgekehrt. Positiv dagegen ist, dass alle Werkzeuge kostenlos zu haben sind.

Größtenteils sind die besprochenen Programme ein Teil der Windows 2003 Server Support Tools. Sie installieren diese nachträglich, wenn Sie die Datei SUPTOOLS.MSI im Verzeichnis

```
/Support/Tools
```

der Windows 2003 Server CD ausführen. Alternativ finden Sie die aktuelle Version **hier bei Microsoft**[2]. Falls ein Programm nicht Teil dieser Sammlung ist, gehen wir gesondert darauf ein.

1. ADSI Edit - die vielseitige Management-Konsole

Bei **ADSI Edit** handelt es sich um ein Snap-in für die Management-Konsole, das einen Low-Level-Editor für das Active Directory darstellt. Auf den ersten Blick wirkt das Programm wie eine etwas hässlichere Variante der normalen Active-Directory-Werkzeuge aus den administrativen Tools, doch in Wirklichkeit gehen dessen Fähigkeiten weiter: Das Programm stellt die AD-Struktur als Baum dar, wobei der Inhalt der einzelnen Knoten jeweils im rechten Fensterbereich angezeigt wird.

Für jedes Objekt stehen zwei Editoren zur Verfügung. Mit dem einen lassen sich sämtliche Attribute des Objekts anzeigen und ändern, mit dem anderen sind die auf das Objekt anzuwendenden Rechte bearbeitbar. Die Rechte sind auch mit den normalen AD-Tools zu editieren, an die Attribute eines Objekts kommen die Standardtools jedoch nicht heran.

ADSI Edit ist in den Microsoft Windows Support Tools enthalten.

2. Mit anderen Servern verbinden

Von Haus aus verbindet sich ADSI Edit mit der Domain, an der der Administrator momentan angemeldet ist. Per „Connect“-Befehl aus dem Objektmenü der Wurzel des AD-Baums besteht aber auch die Möglichkeit, sich mit einem anderen Server zu verbinden. Einmal verbunden, kann das Programm als Browser über den Inhalt des Active Directory bis hinunter zu den einzelnen Attributen eines einzelnen Objekts verwendet werden.

ADSI Edit ist oft das einzige Tool, mit dem eine bestimmte Aufgabe durchgeführt werden kann. Ein beliebtes Beispiel dafür ist die Art und Weise, in der die Namen von Benutzern des AD angezeigt werden. Standardmäßig erfolgt die Anzeige in der Reihenfolge „Vorname, Nachname“ – mit ADSI Edit kann der Administrator diese Anzeige so ändern, dass stattdessen für neu angelegte Benutzer „Nachname, Vorname“ als Format verwendet wird.

3. Fehlersuche mit Dcdiag

Mit **Dcdiag** steht Ihnen das ultimative Diagnosewerkzeug für Active Directory zur Verfügung. Der Administrator kann damit nicht nur einen einzelnen Server, sondern auch alle Server einer Site oder im Enterprise prüfen. Das Programm ist Teil der Windows 2003 Server Support Tools. Alternativ erhalten Sie das Programm auch einzeln als **Download**[3].

Das Programm führt dabei eine Vielzahl an Tests durch. Welche das im Einzelnen sind, kann man sich mit dem Befehl

```
dcdiag /?
```

anzeigen lassen. Wird das Programm ohne Parameter aufgerufen, so führt es nur einen Teil der Tests durch. Soll ein vollständiger Test gefahren werden, verwenden Sie am besten den Kommandozeilenparameter

```
/c
```

, damit werden wirklich alle Diagnoseschritte ausgeführt. Dabei ist der Umfang an diagnostischen Meldungen mit der Option

```
/v
```

auch sehr ausführlich gestaltbar.

Die Menge an Informationen, die DcDiag ausspuckt, ist allerdings sehr umfangreich: Um damit tatsächlich etwas anfangen zu können, empfiehlt es sich, die Ausgabe von DcDiag mit dem zusätzlichen Schalter

```
/f:LogFile
```

in eine Datei umzuleiten.

4. LDP - LDAP wie Active Directory

Bei **LDP** handelt es sich um einen grafischen LDAP-Client. Das Programm verbindet Sie zum LDAP-Server in der gleichen Weise wie zum Active-Directory-Server. Anschließend haben Sie vollen Zugriff auf die LDAP-Informationen. Das Programm ist Teil der Windows 2003 Server Support Tools.

Mit Hilfe des "

Connection

"-Menüs bauen Sie die Verbindung zum Active Directory Server auf. Mit den Befehlen aus dem etwas ungünstig benannten Menü "

Browse

" können Sie den LDAP-Server nicht nur durchsuchen, sondern auch Objekte hinzufügen oder entfernen. Das Programm können Sie letztlich als "sparsamen" Ersatz für den normalen Active-Directory-Browser betrachten.

Sehr praktisch an diesem Werkzeug ist aber die Tatsache, dass alle LDAP-Anfragen und Antworten im Klartext mitprotokolliert werden. Sie können also interaktiv verfolgen, welche Auswirkungen Ihre Anfragen haben und wie das AD darauf reagiert.

5. Replmon - Übersicht über alle Replikationen

Mit **Replmon** überwachen Sie die Active-Directory-Replikation auf unterster Ebene. Weiterhin können Sie mit dem Programm die Synchronisation zweier Domain-Controller erzwingen und sich einen grafischen Überblick über die Topologie Ihres Netzes verschaffen. Replmon ist Teil der Windows 2003 Server Support Tools.

Um einen Server zu überwachen, klicken Sie auf das "Edit"-Menü und dort auf den Befehl "Add Monitored Server". So verbinden Sie sich mit Ihrem Domain-Controller. Ist die Verbindung hergestellt, präsentiert sich der Controller ähnlich wie das "Active Directory Sites and Services"-Snap-in.

Auf den ersten Blick ist das Programm ein wenig unübersichtlich, es bietet aber eine ganze Reihe an Informationen. Beim Replmon ist es in erster Linie wichtig zu wissen, dass praktisch alle Objekte mit einem Objektmenü ausgestattet sind, das den Zugriff auf eine Vielzahl von Befehlen bietet. Es lohnt sich daher auf jeden Fall, zumindest einmal jedes Objekt anzuklicken – schon allein, um herauszufinden, welche Möglichkeiten überhaupt zur Verfügung stehen.

Teilweise ist es auch so, dass Sie zuerst mehrere Klicks an unterschiedlichen Stellen durchführen müssen, bevor sich Replmon entscheidet, Informationen anzuzeigen: Greifen Sie auf jeden Fall einmal auf die Dokumentation des Programms zurück, um sich die dort aufgelisteten Beispiele anzusehen. Diese sind als erster Einstieg in die Nutzung von Replmon sehr hilfreich.

6. ADModify.Net - Allzweckwaffe mit Sicherheitsnetz

Während das zuvor vorgestellte ADSI Edit für das Feintuning des Active Directory zuständig ist, erledigt das Tool **ADModify.Net** die großen Aufgaben. Darunter fallen beispielsweise umfangreiche Änderungen über ein großes, bereits vorhandenes Directory. Dieses Programm ist nicht Teil der Support-Tools, sondern separat und kostenlos bei **GotDotNet**[4] erhältlich.

ADModify.Net kann die meisten Export-, Import- und Änderungsarbeiten am Active Directory vornehmen. Auf einem Windows-2003-Rechner lassen sich auch die Terminal-Server-Attribute aus dem AD bearbeiten. Läuft zusätzlich ein Server mit Exchange ab Version 2000, verwaltet ADModify.Net zusätzlich die Attribute für die Mailbox-Rechte.

Praktisch ist die Tatsache, dass Sie alle Änderungen rückgängig machen können. Dazu protokolliert ADModify.Net jeden Vorgang in einer XML-Datei: So lange diese Datei intakt ist, können Sie die mitprotokollierten Veränderungen jederzeit wiederherstellen.

Microsoft stellt zudem eine Version zur Verfügung, die das .Net-Framework nicht benötigt. Diese wird allerdings nicht mehr aktiv weiterentwickelt. Sie finden beide Versionen von ADModify zusätzlich auf dem **Microsoft FTP-Server**[5].

7. Der EventLog und die Registry

Bei der Fehlersuche hilft vor allem die **Ereignisanzeige**: Dort hat das Active Directory unter dem Namen „Verzeichnisdienst“ eine eigene Kategorie. Was dabei oft unbekannt ist, ist die Tatsache, dass der Log-Level standardmäßig auf „0“ steht. Dadurch werden nicht alle zur Verfügung stehenden Informationen protokolliert.

Der höchste Log-Level liegt beim Wert 5. Der sollte aber wirklich nur für die Fehlersuche eingesetzt werden, denn die Menge an Protokolldaten wird dadurch recht groß. Die Log-Level können dabei für verschiedene Teile des Active Directory unterschiedlich gesetzt werden. Sie finden die entsprechenden **Registry**-Schalter unter

```
HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/NTDS/Diagnostic
```

.

8. IAdsTool - Scripting-Erweiterung für C++

So schön die fertigen Tools sein mögen – manchmal braucht man einfach ein eigenes Script, um eine bestimmte Aufgabe durchzuführen. Unter Windows stehen mehrere Script-Sprachen zur Auswahl – doch der Zugriff auf das Active Directory ist nur für C/C++-Programmierer vorgesehen. Das ist ärgerlich, denn Administratoren schreiben nur selten Programme in C/C++, sondern eben eher in einer Script-Sprache.

Dieses Manko löst Microsoft mit den **IAdsTools**-Dateien. Hier handelt es sich im Wesentlichen um eine DLL und ein Word-Dokument. Beide hat Microsoft aber gut versteckt. Die beiden Dateien finden Sie auf der Windows-2003-Server-CD im Verzeichnis

```
\SUPPORT\TOOLS\
```

. Öffnen Sie die Datei SUPPORT.CAB mit einem Packprogramm, etwa WinRAR. Innerhalb dieser CAB-Datei finden Sie die Datei

```
iadstools.dll
```

sowie die 76-Seiten starke Word-Datei

```
iadstools.doc
```

.

Die DLL enthält Funktionen und Objekte, die per Script erreichbar sind, und den Zugriff auf das AD erlauben. Die zugehörige Word-Datei enthält dann die für alle verfügbaren Funktionen, ein kurzes Script-Beispiel und die zugehörige Dokumentation. Damit steht dem eigenen Script mit Active-Directory-Zugriff nichts mehr im Wege.

9. Fazit

Bei den hier vorgestellten Active-Directory-Werkzeugen handelt es sich nur um die wirklich wichtigsten ihrer Art. Microsoft hat aber eine ganze Reihe weiterer hilfreicher Programme zu bieten. Sie sollten daher sowohl die Resource-Kit-Tools als auch die Support-Tools installieren.

Nützlich ist auf alle Fälle ein Blick in die dabei mitinstallierten Hilfedateien: Darin finden Sie die AD-Tools in eigenen Rubriken aufgeführt und erläutert. In vielen Spezialfällen werden unter Umständen die weniger wichtigen, kleineren Werkzeuge hilfreicher sein als beispielsweise das Übertool ADSI Edit. (mja)

Links im Artikel:

[1] **http://technet2.microsoft.com/WindowsServer/de/Library/a7106fe0-c31d-424d-8918-fcd502da87251031.mspx?mfr=true**
[2] **http://www.microsoft.com/downloads/details.aspx?familyid=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en**
[3] **http://www.microsoft.com/downloads/details.aspx?familyid=23870A87-8422-408C-9375-2D9AAF939FA3&displaylang=en**
[4] **http://workspaces.gotdotnet.com/ADModify**
[5] **ftp://ftp.microsoft.com/PSS/Tools/Exchange%20Support%20Tools/ADModify/**
