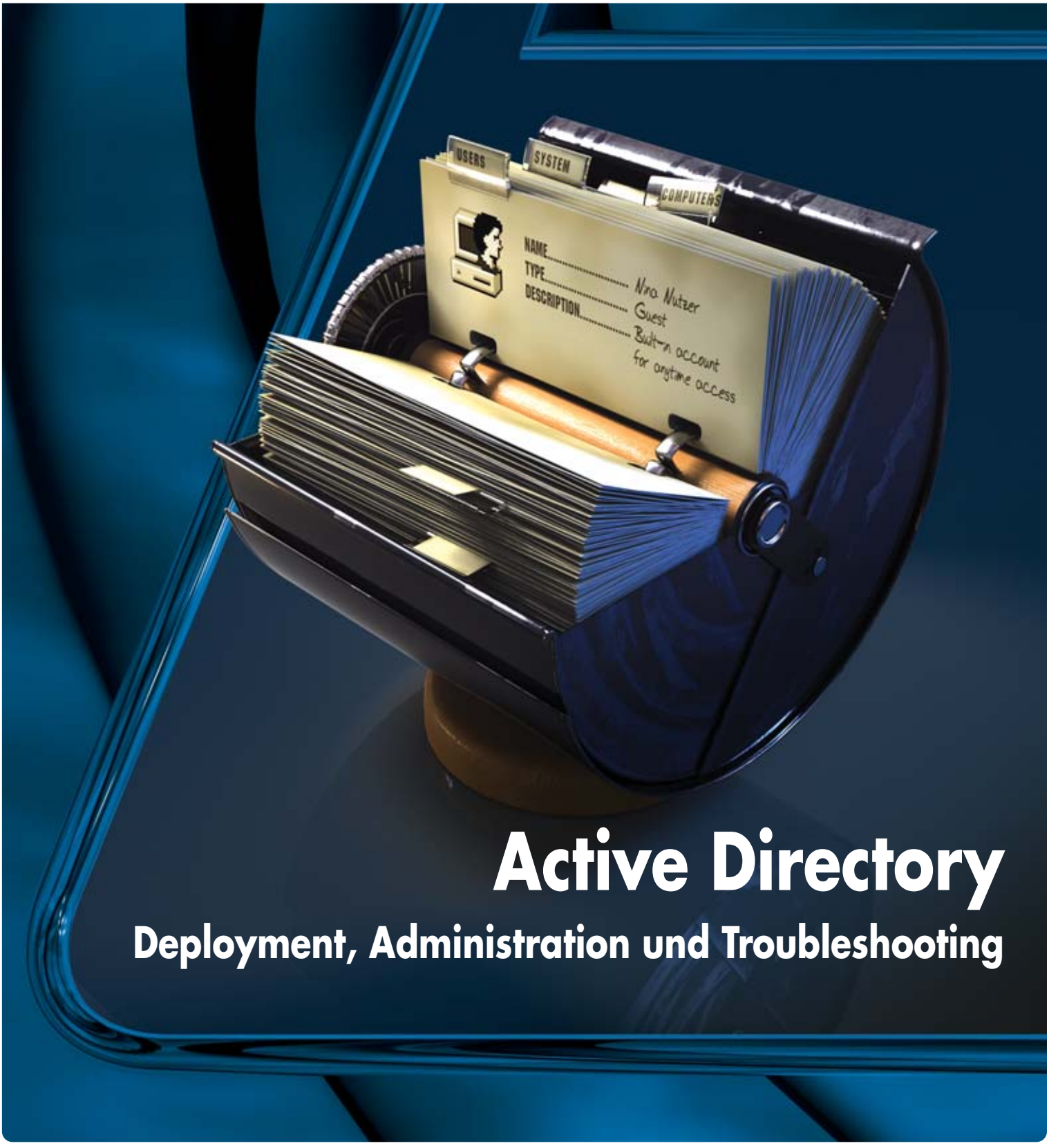
IT-ADMINISTRATOR.DE

Sonderheft II/2010

€ 29,90 ISSN 1614-2888

IT administrator sonderheft



Active Directory

Deployment, Administration und Troubleshooting

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes Sonderheft nur Euro 19,90 – und müssen keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März und Oktober jeden Jahres das jeweilige IT-Administrator Sonderheft und mit Ihrer Dezemberausgabe die jeweilige Jahres-CD mit allen Monatsausgaben des Jahres im PDF-Format zugestellt.

Als bestehender Jahresabonnent können Sie hier upgraden:

www.it-administrator.de/abonnements/aboupgrade/

Oder Sie sind Neukunde? Hier können Sie bestellen:

www.it-administrator.de/abonnements/jahresabo/

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München
Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

EDITORIAL

"Jetzt ist meine gesamte Domäne funktionsuntüchtig..."

Liebe Leser,

4 Uhr 39 Montagmorgen: Seit fünf Stunden steht das Netzwerk still, um 7 Uhr kommen die ersten Kollegen und benötigen einen laufenden Domänencontroller zur Anmeldung. Nur davon kann keine Rede sein, seit die gestrigen Wartungsarbeiten gründlich in die Hose gingen. Der geplante Ersatz eines alten DC klappte ganz gut: Zunächst diesen mit DCpromo aus dem Netz entfernen, die DHCP- und DNS-Dienste auf einen anderen DC schieben und anschließend den neuen Domänencontroller in die bestehende Struktur integrieren. Doch dann das Chaos – die Shares \sysvol und \netlogon sind weg! Eine Anmeldung am DC ist nicht mehr möglich …

Dieser Hilferuf eines verzweifelten Administrators findet sich im Web bei der Recherche nach Sysvol-Problemen. Aber mal ganz ehrlich: Beim Gedanken an ein solch grausames Ende einer mehr oder weniger als Routineaufgabe zu bezeichnenden Tätigkeit wachsen sicher so manchem Admin graue Haare. Eine winzige Unaufmerksamkeit oder ein Quäntchen fehlendes Spezial-Know-How, und schon ist das Active Directory zerschossen. Und Spezial-Know-How benötigt der Active-Directory-Administrator an vielen Stellen: Sei es die Replikation, Backup und Recovery oder die Gruppenrichtlinien im SYSVOL-Verzeichnis, das dem Admin aus unserem Katastrophenszenario so übel mitgespielt hat.

Sicher wäre es vermessen zu behaupten, der Administrator aus unserem Beispiel hätte sich mit diesem Sonderheft problemlos aus seiner misslichen Lage befreit. Dennoch bietet Ihnen unser Sonderheft "Active Directory" praxisnahes, erprobtes Wissen zu den Zusammenhängen und internen Mechanismen des Verzeichnisdienstes und darüber hinaus viele Ansatzpunkte, wenn doch einmal Troubleshooting notwendig ist. Für die große Praxisnähe bürgen auch unsere Autoren Ulf B. Simon-Weidner und Florian Frommherz – beide Microsoft MVP mit zahllosen Consultingstunden und Notfalleinsätzen zum Active Directory auf dem Buckel.

Und Übrigens: Unserem verzweifelten Admin wurde letztendlich auch von einem MVP aus der Patsche geholfen. Wir hoffen, dass die Lektüre dieses Sonderhefts Ihnen derartige lange Nächte erspart. Viel Spaß beim Leser wünschen

Daniel Richey John Pardey Lars Nitsch

INHALT

ACTIVE DIRECTORY-DESIGN & STRATEGIE

ADMINISTRATION & SCRIPTING

SECURITY

INHALT

OPTIMIERUNG & TROUBLESHOOTING

RUBRIKEN

Florian Frommherz lebt in Süddeutschland an der Grenze zur Schweiz und arbeitet als Systems Engineer bei ControlTech Engineering, einem Ingenieurbüro in Liestal in der Schweiz. Dort hat er auch sein BA-Studium Informationstechnik absolviert, bevor er sich anschließend Kundenprojekten, auch in der Softwareentwicklung mit .NET, widmete.

Bereits zu Studienzeiten zählten Gruppenrichtlinien und Active Directory zu seinen Kerntätigkeiten und Schaffensfeldern. Seine Lieblingsthemen umfassen heute Softwaredeployment, AD- und LDAP-Anfragen und die Nutzung des Verzeichnisses in eigenen Anwendungen. Darüber hinaus beschäftigt er sich mit AD- und GPO-Performance und der Planung und dem Design neuer Gesamtstrukturen und Domänen.

Durch seine freiwillige Mithilfe in technischen Foren und den Microsoft-Newsgroups in den vergangenen sieben Jahren wurde Frommherz in den letzten vier Jahren regelmäßig zum Most Valuable Professional (MVP) für Gruppenrichtlinien ernannt – einem der jüngsten MVPs im "Windows Server"-Bereich. Dies ermöglicht es ihm, in frühen Entwicklungsphasen tiefes Produkt-Knowhow aufzubauen und es in Online-Communities mit anderen Mitgliedern zu teilen.

Bleibt ihm freie Zeit, ist er als Autor für Fachartikel in Magazinen und Blogs wie faq-o-matic.net oder den Blogs des AD-Supportteams in Deutschland oder dem Group Policy-Team in Redmond tätig. Auch steuerte er in der Vergangenheit mehrere Fachartikel zu bekannten deutschen IT-Portalen bei.

Florian Frommherz

Ulf B. Simon-Weidner arbeitet als Senior Consultant für den IT-Infrastrukturdienstleister Computacenter in Deutschland. Ende 1998 wurde er mit dem Thema Active Directory konfrontiert, was ihn seither faszinierte. Seit damals unterstützt er vor allem Unternehmen bei Strategieplanung, Integrationsthemen und der Migration der Infrastrukturen auf die aktuellen Microsoft Betriebssysteme und rund um Active Directory. Mittlerweile ist er überwiegend auf internationaler Ebene tätig, betreut aber auch zahlreiche Unternehmen in Deutschland. Außerdem hält er Vorträge und Schulungen und beschäftigt sich in naher Zusammenarbeit mit der Produktgruppe in Redmond mit den zukünftigen Technologien.

Als Fachautor hat er einige Bücher bei MS-Press (mit)geschrieben und ist beim IT-Administrator einer der Autoren der ersten Stunde: Seinen ersten von zahlreichen Artikeln veröffentlichte er im Dezember 2004. Sein Engagement in den internationalen Communities wurde bereits siebenmal mit der Auszeichnung "Microsoft Most Valuable Professional" (MVP) für "Windows Server – Directory Services" anerkannt. Sein Wissen vermittelt er auf zahlreichen Konferenzen wie der Microsoft TechEd USA und Europa, der "The Experts Conference" (vormals Directory Experts Conference) in USA und Europa sowie zahlreichen Events wie dem Windows Server 2008 Launch und IT-Administrator Workshops. Seine Zertifizierungen beinhalten den Microsoft Certified Trainer (MCT) sowie für Windows NT 4.0, 2000 / XP und Windows Server 2003.

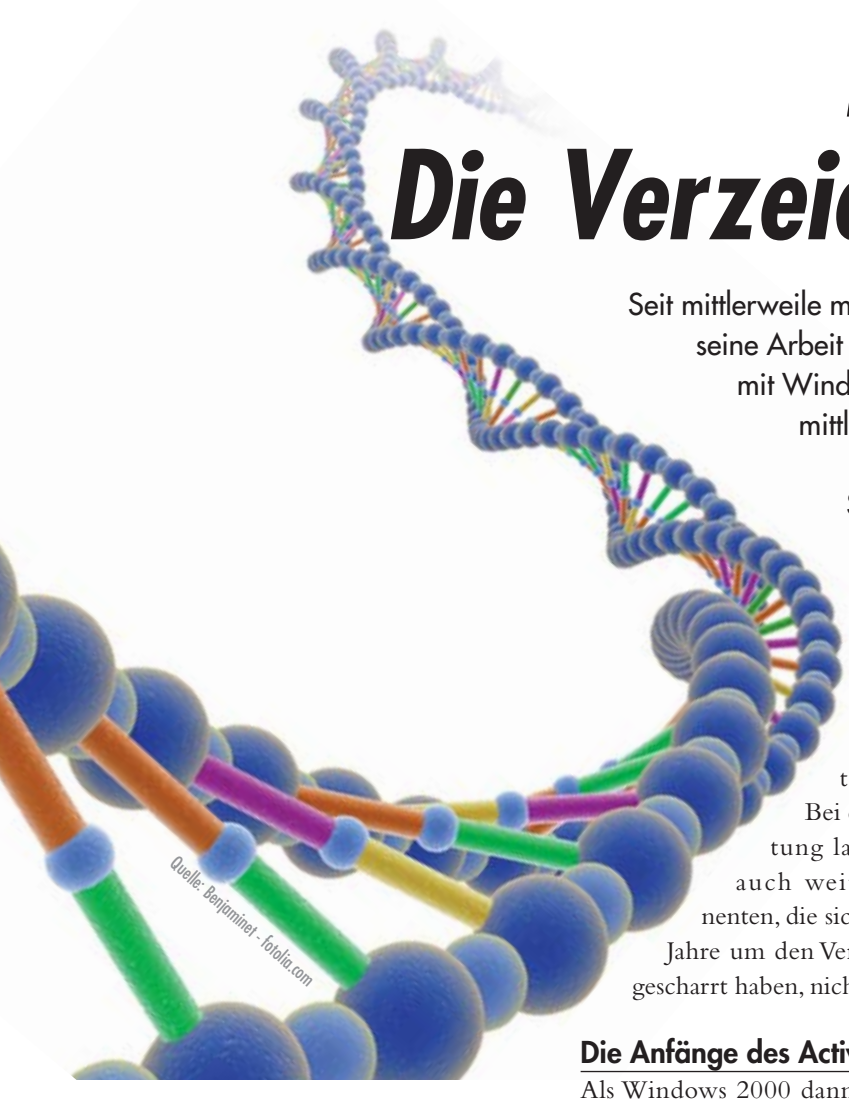
Auch privat setzt sich Simon-Weidner mit Themen rund um die Microsoft-Technologien auseinander und nimmt aktiv an verschiedenen Communities sowohl online wie auch offline teil. Er beschäftigt sich mit dem Aufbau von Communities zum Wissensaustausch innerhalb und außerhalb von Unternehmen. Ansonsten verbringt er seine Freizeit gerne draußen, seine Hobbys sind Tauchen, Tanzen, in angenehmer Gesellschaft grillen sowie die bayerischen Seen und Biergärten genießen. Seinen Weblog zu Directory Services / Active Directory veöffentlicht er unter www.msmvps.com/UlfBSimonWeidner.

Ulf B. Simon-Weidner

Neben unseren beiden Sonderheft-Autoren Ulf B. Simon-Weidner und Florian Frommherz tragen auch weitere Autoren des IT-Administrator die Auszeichnung MVP. Doch was steckt eigentlich hinter dem Titel? Als "Most Valuable Professional" dürfen sich all jene IT-Experten bezeichnen, die sich in der Microsoft-Community besonders verdient gemacht haben, etwa durch Artikel in Magazinen, Buchveröffentlichungen, Vorträge oder in Online-Foren. Personen, deren fachliche Kompetenz sowie deren Bereitschaft und Fähigkeit aufgefallen ist, anderen bei der optimalen Nutzung der Microsoft-Technologien zu helfen, können dann von Mitgliedern der technischen Communitys, von aktuellen und ehemaligen MVPs und von Microsoft-Mitarbeitern als Kandidaten für die Auszeichnung "MVP" nominiert werden. Ein Gremium aus Mitgliedern des MVP-Teams und der Microsoft-Produktgruppen bewertet im Auswahlverfahren anschließend die Fachkenntnisse der Kandidaten sowie das bereitwillige Engagement in der Community in den vergangenen 12 Monaten. Das Gremium beurteilt dabei Qualität, Menge und Relevanz der Beiträge der MVP-Kandidaten. Aktive MVPs unterziehen sich jedes Jahr denselben Prüfungen wie neue Kandidaten.

Microsoft Most Valuable Professional

MVP
Microsoft®
Most Valuable
Professional



Entwicklung des Active Directory

Die Verzeichnis-Evolution

Seit mittlerweile mehr als zehn Jahren verrichtet das Active Directory seine Arbeit als Verzeichnisdienst im Windows Server. Erstmals mit Windows 2000 Server veröffentlicht, ist das Verzeichnis mittlerweile eine maßgebliche Infrastrukturkomponente der meisten Unternehmen. Als Auftakt zu diesem Sonderheft möchten wir die Entwicklungsstufen des Verzeichnisdienstes betrachten und auch weniger bekannte Eigenschaften und Zusammenhänge des Active Directory darstellen.

An seinem ersten Arbeitstag schickte sein Chef den Autor dieses Beitrags, Ulf B. Simon-Weidner, direkt auf eine NT5-Preview-Schulung. Von "NT5" hatte er bis zu dem Tag nichts gehört, aber es klang spannend. Wie sich herausstellte, war NT5 der Nachfolger von NT4 und wurde später zu Windows 2000 umbenannt. Und so entblätterte sich an den ersten Tagen seines Arbeitslebens das "Active Directory" vor ihm. Fasziniert von dieser Technologie und dem vorgestellten "geplanten Migrationsweg" (der zu diesem Zeitpunkt sehr abenteuerlich klang), organisierte er sich für die Weihnachtsferien einen Beta 3 Release-Kandidaten, erarbeitete sich den Migrationsweg selbst und ist seitdem fasziniert von der Technologie des Active Directory.

Im Folgenden betrachten wir den Werdegang des Active Directory (AD) von den damaligen, ersten Schritten bis heute. Bei dieser Betrachtung lassen wir aber auch weitere Komponenten, die sich im Laufe der Jahre um den Verzeichnisdienst gescharrt haben, nicht außer Acht.

Die Anfänge des Active Directory

Als Windows 2000 dann Anfang 2000 offiziell öffentlich erhältlich war, brachte der Verzeichnisdienst eine Menge neue Technologien mit, um die gewachsenen NT4-Domänenstrukturen abzulösen. Domäneninhalte waren nun strukturierbar und nicht mehr flach, DNS wurde zentrale Komponente für die Namensauflösung von Systemen und Diensten. Zudem ermöglichte Microsoft endlich die administrative Delegation.

Domänenstrukturen sollten im Active Directory Hierarchien folgen, anstatt wirren Spinnennetzen zu gleichen. Jeder Domänencontroller durfte schreiben, ganz im Gegensatz zu NT4, wo es immer einen Primären Domänencontroller geben musste. Das AD zeigte sich skalierbar und redundant, ohne auf einem Cluster zu basieren. Der Client-Logon sowie die Replikation des Verzeichnisdienstes "verstanden" Netzwerktopologien, Subnetze, Standorte und wenn notwendig sogar Stundenpläne.

Microsoft integrierte zahlreiche zusätzliche Technologien im AD: Unter dem Motto "If it moves – script it" wurden Administratoren ermutigt, Änderungen lieber per Skript zu implementieren (damit diese in Testumgebungen verifiziert werden können und Tippfehler beim produktiven Change seltener vorkommen) und die Windows Management Instrumentation, VBScript und Jscript waren im Serverbetriebssystem enthalten. Gruppenrichtlinien ermöglichten die Konfiguration von Clients und Servern und konnten über unterschiedlichste Mechanismen unterschiedliche Hardware, Rollen oder Benutzertypen berücksichtigen. Sogar zur Softwareverteilung sollten sie verwendet werden. Sicherheit wurde dabei großgeschrieben, und so konnten selbst die Sicherheitseinstellungen bis hin zur IPsec-Verschlüsselung über GPOs gesteuert werden. Darüber hinaus ließen sich Sicherheitstemplates anwenden, die einen Client relativ offen lassen, bis hin zum Client für hohe Sicherheitsanforderungen in der Personalabteilung oder Kiosk-Systemen. Schließlich waren auch Sicherung und Wiederherstellung des Verzeichnisdienstes – letzteres zumindest teilweise – berücksichtigt.

Auch wenn Windows 2000 für Großunternehmen entworfen wurde – einige von Ihnen erinnern sich vielleicht an ein Projekt von Microsoft und Compaq, bei dem sämtliche Telefonbuchdaten der USA und Kanada in ein AD geladen wurden, um die Skalierung zu testen – für eben diese war es aber noch nicht in allen Bereichen ausgereift genug. Gruppen durften maximal rund 5.000 Mitglieder haben, die Replikationsstruktur war nicht ganz so optimiert. Viele Unternehmen hatten Angst vor "Schema-Updates", da selbige zu einer Reinitialisierung des Globalen Katalogs führten und bei großen Mengen nicht innerhalb von normalen Change-Zeiten repliziert wurden. Aber es war deutlich sicherer und stabiler als NT4, das es auf insgesamt sechs Servicepacks brachte (und häufig war zu hören, dass es vor SP4 nicht einsetzbar war). Windows 2000 hingegen hat bis zu seiner unlängst abgelaufenen Lebenszeit "nur" vier Servicepacks erhalten.

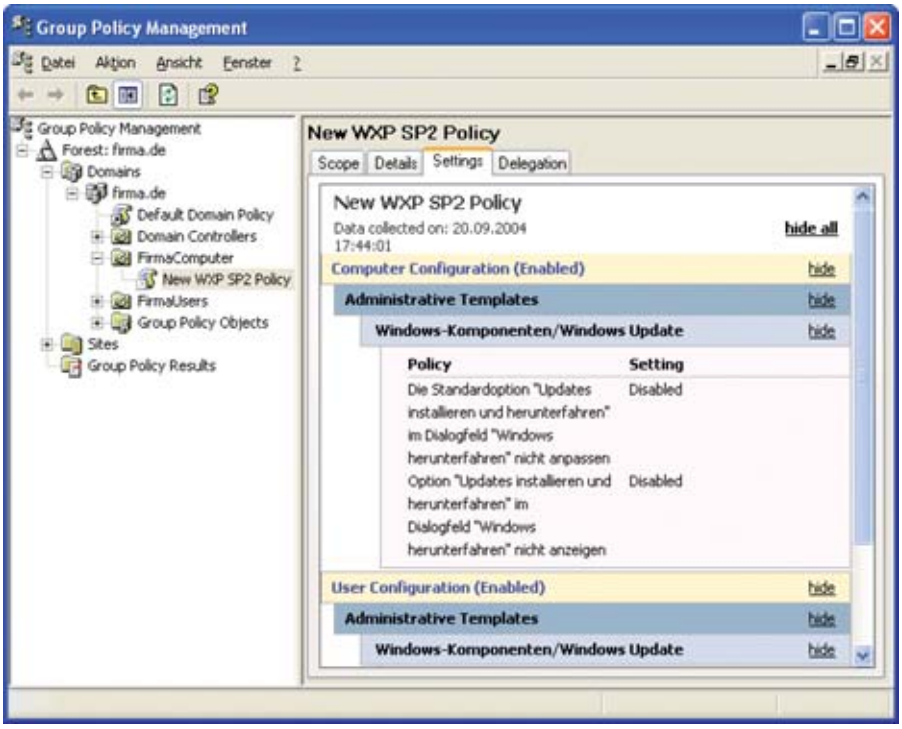


Bild 2: Die Gruppenrichtlinienverwaltungskonsole ermöglicht erstmals eine umfassende und vernünftige Administration von GPOs

AD in Windows Server 2003

Die nächste Version des AD berücksichtigte dann auch die Anforderungen von Großunternehmen besser, da Microsoft bei großen Implementierungen in entsprechenden Umgebungen Erfahrungen sammeln konnte: Windows Server 2003 wurde, nach einer Arie von Namensgebungen (von dem Codenamen Whistler über "Windows.NET Server" und "Windows.NET Server 2003" hin zum endgültigen Namen) im Mai 2005 öffentlich verfügbar.

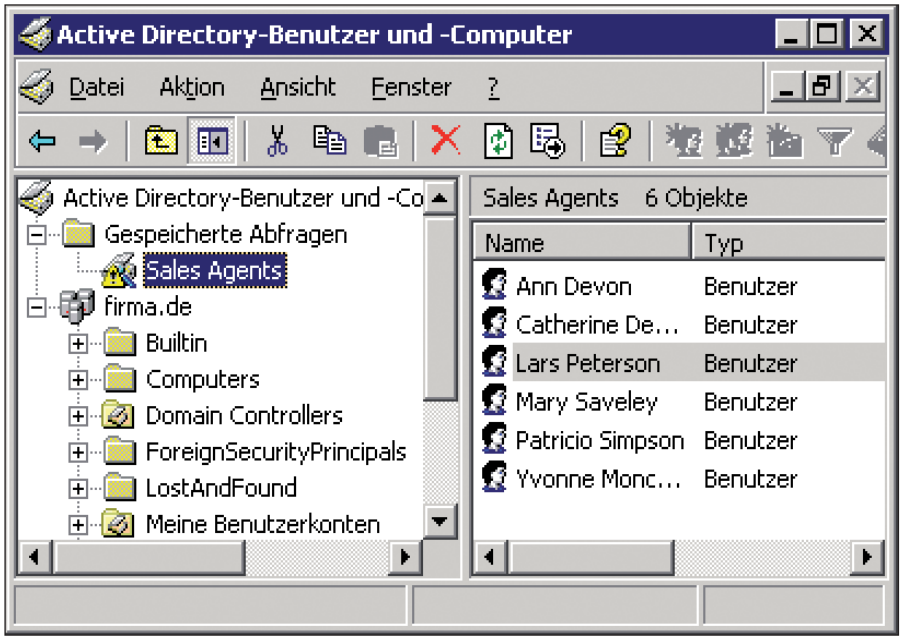


Bild 1: Gespeicherte Abfragen beim Windows Server 2003

Jetzt war die Anzahl von Mitgliedern einer Gruppe nicht mehr auf 5.000 beschränkt, und zugleich wurden nicht mehr alle Gruppenmitglieder auf einmal repliziert, sondern nur noch die Änderungen (Linked Value Replication). Der Algorithmus zur Berechnung der Replikationstopologie wurde vereinfacht und damit auch verbessert. Um die Datenbankgröße im AD zu vermindern, erfolgte neben den Verknüpfungen der Links dasselbe auch für die Sicherheitseinstellungen der AD-Objekte, so dass diese nicht mehrfach mit jedem Objekt gespeichert wurden. Beim Aufbau eines Domänencontrollers ließ sich jetzt auch eine Datensicherung eines DCs verwenden ("Install from Media"), Gesamtstruktur-übergreifende Vertrauensstellungen wurden möglich (Forest-Trust) und DNS wurde bei Bedarf automatisch nach Best Practices installiert. Dies ermöglichte die Replikation von DNS-Namensräumen unabhängig von Domänengrenzen. Conditional Forwarder und Stub-Zones machten es dem Administrator einfacher, seine DNS-Infrastruktur zu entwerfen und über seine Infrastruktur-

grenzen hinweg besser auf Änderungen zu reagieren. Zusätzlich vereinfachten "Gespeicherte Abfragen" in Active Directory-Benutzer und -Computer sowie Kommandozeilen-Tools (wie DSQuery, DSGet et cetera) die Administration. Außerdem waren die ersten Versuche eines globalen Servermanagers enthalten.

Die mit Windows XP SP2 gestartete Security-Initiative kam mit Windows Server 2003 SP1 dann auch beim Server-Betriebssystem an: Die Windows Firewall wurde ebenso integriert wie ein Security Configration Wizard und viele Einstellungen des Betriebssystems wurden auf "Secure-by-default" gesetzt.

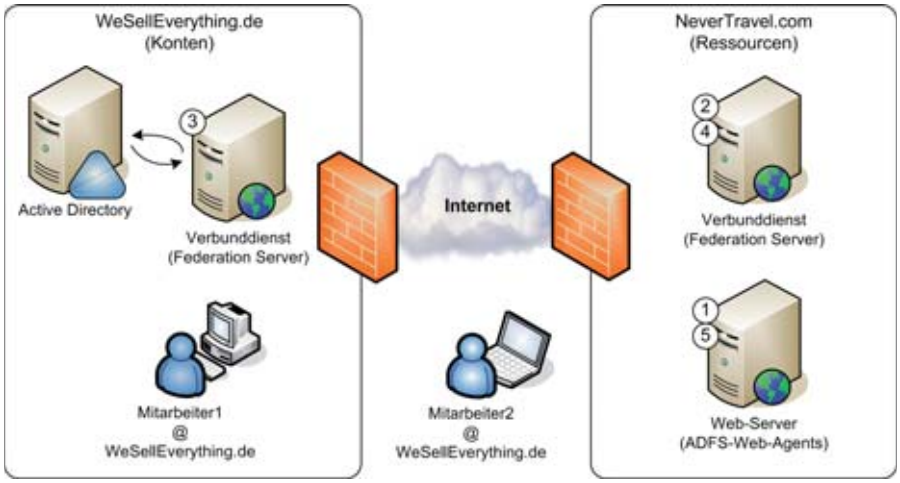


Bild 3: Active Directory Federation Services ermöglichen einen Single Sign-On über Unternehmensgrenzen hinweg und sind zusammen mit ADAM seit Windows Server 2003 R2 optionale Komponenten des Betriebssystems

Im Nachgang zu Windows Server 2003 wurden einige Komponenten auch über das Web verfügbar. Die Gruppenrichtlinienverwaltungskonsole vereinfachte endlich in vielen Bereichen die Administration der GPOs. Und als kleiner Bruder des Active Directory wurde auch ADAM – oder Active Directory / Application Mode – veröffentlicht. ADAM bot für Anwendungen und Entwickler viele der Vorteile des AD: Einen Multi-Master-Verzeichnisdienst, der sich über die gleichen Schnittstellen wie AD programmieren lässt, aber unabhängig von dem Infrastrukturdiensten repliziert und mehrere Instanzen auf einem Server oder sogar Client ermöglicht. Allerdings ist es kein Domänencontroller, kann keine Computerobjekte und Gruppenrichtlinien verwalten und ist somit "nur" als Verzeichnisdienst für Anwendungen gedacht. Mittels Proxy-Objekten lassen sich aber neben den eigenen Benutzern auch AD-Benutzer einer Domäne verwenden, um Zugriff auf Anwendungen zu steuern. ADAM wurde für Anwendungen wie Internet Security and Acceleration Server oder zusammen mit MIIS/ILM/FIM bei den Unternehmen häufiger als "Meta-Directory" verwendet – um Informationen über Anwender an einer zentralen Stelle zu sammeln und synchron zu halten.

Im März 2006 erfreute Microsoft die Öffentlichkeit mit der nächsten "neuen" Version des Serverbetriebssystems – dem Windows Server 2003 R2. Dieser wurde parallel mit den 64-Bit-Versionen entwickelt und basierte von Anfang an auf dem SP1. Im Endeffekt ist die 32-Bit-Version von R2 auch kein neues Betriebssystem, sondern nur eine Erweiterung der Windows-Komponenten, die im Produkt integriert sind.

Im Active Directory hatte sich fast nichts geändert (lediglich ein Bug machte die mit SP1 von 60 auf 180 Tagen erhöhte Lebenszeit von gelöschten Objekten bei der ersten Installation einer Gesamtstruktur wieder rückgängig). Aber zum ersten Mal war ADAM eine optionale Komponente des Betriebssystems und musste nicht mehr separat heruntergeladen werden.

Neu waren auch die "Active Directory Federation Services": Sie ermöglichen eine unternehmensübergreifende Verwendung von Benutzerkonten. So können zum Beispiel Anwender eines Unternehmens sich auf der Webseite ihres Reisebüros authentifizieren, ohne sich separat anmelden zu müssen. Über die Authentifizierung im eigenen Unternehmen, Internet-Technologien wie Umleitungen und signierten Cookies können die Administratoren beider Unternehmen sicherstellen, dass nur diejenigen Informationen für die Anwendung des Geschäftspartners verwendet werden, die gewährleisten, dass der Anwender noch im Unternehmen ist. Weitere neue Features, die zwar nicht direkt mit dem AD zu tun haben, aber die Infrastrukturadministration vereinfachen, waren neue Möglichkeiten beim Distributed File System (DFS): Die DFS-Replikation, die nur Dateiänderungen repliziert, sowie Verwaltungskonsolen wie das Druckermanagement, das erstmals eine zentrale Verwaltung von Druckservern und das Verknüpfen von Druckern über Gruppenrichtlinien ermöglichte.

Verwandte Technologien

Parallel zu der Entwicklung des Active Directory mit dem Betriebssystem gibt es weitere Komponenten, die in diesem Zusammenhang nennenswert sind. Als erstes sind hier die Zertifikatsdienste zu erwähnen. Diese gibt es seit Windows 2000, sie sind aber von Version zu Version verbessert worden. Heutzutage werden Zertifikate auch für Domänencontroller immer wichtiger. LDAP ist dagegen ein Protokoll, das im Klartext sendet. Besser ist es daher, LDAPS (oder LDAP via SSL/ TLS) zu verwenden, hierzu benötigt der Domänencontroller aber ein SSL-Zertifikat. Auch für das Encrypted File Protocol (EFS) sollten Zertifikate verwendet werden, wenn im Unternehmen das Verschlüsseln von Daten erlaubt ist – ansonsten droht Da-

tenverlust, wenn die Administration dieses Feature nicht berücksichtigt und keinen Key für den Recovery-Administrator anlegt. Andere Dienste wie Federation Services Proxy (seit 2003 R2) oder BranchCache im Hosted Mode unter Windows Server 2008 R2 benötigen ebenfalls Zertifikate. Auch im Client-Bereich ist dies wichtig, zum Beispiel für zertifikatsbasiertes Wireless LAN oder für Smartcard-Authentifizierung. Mit Windows Server 2003 konnten die Zertifikatsdienste entsprechende Zertfikate automatisch an Domänenmitglieder ausrollen. Seit Windows Server 2008 lassen sich die Dienste auch clustern und das "Online Certificate Status Protocol (OCSP)" ermöglicht es, gesperrte Zertifikate besser abzufragen.

Durch die Windows Rights Management Services (RMS) können Unternehmen sicherstellen, dass sensible Informationen vertraulich behandelt werden: E-Mails oder Office-Dokumente werden entsprechend markiert, so dass nur bestimmte Benutzer ihre Inhalte lesen, drucken oder weitersenden dürfen. Der Administrator kann hierfür sogar Vorlagen erstellen. Weiterhin ist es möglich, Ablaufdaten einzurichten, so dass eine Datei in den nächsten Tagen noch geschrieben werden kann, aber dann nur noch lesbar ist. Da dies in den Dateiformaten mit enthalten ist und die Dateien verschlüsselt sind, ist die Sicherheit auch dann gegeben, wenn die Dateien beispielsweise per E-Mail die Unternehmensgrenzen verlassen.

Natürlich gibt es noch zahlreiche weitere, mit dem Active Directory verwandte Technologien. Zahlreiche Applikationen, von Exchange über Voice-over-IP bis hin zu Hardwarekomponenten speichern Daten heutzutage im AD. Sie integrieren sich über Kerberos oder LDAP-Authentifizierung, verifizieren Benutzer und E-Mailadressen, um unerwünschte E-Mails aus dem Unternehmen fern zu halten, oder bieten zusätzliche Möglichkeiten zum Monitoring, zur Verwaltung oder zur Datensicherung und Wiederherstellung. Besonders beim Thema Authentifizierung lässt sich eine erhöhte Sicherheit erreichen wenn eine Anwendung die Windows-integrierte Authentifizierung beherrscht, sich über Kerberos oder Federation Services anmeldet. In diesen Fällen kann dann einfach ein Single Sign-On durchgeführt werden und es ist nicht nötig dass sich der Benutzer separat mit einem Benutzernamen und Passwort authentifiziert.

Ansonsten besteht noch die Möglichkeit, dass sich Applikationen per LDAP authentifizieren (präferiert über LDAP via SSL/TLS, damit die Kommunikation auch verschlüsselt abläuft). Dies ist zwar dann keine integrierte Authentifizierung oder Single Sign-On, aber zumindest "Single Credentials", also gleicher Benutzername und Passwort (die Authentifizierung läuft gegen das Active Directory, aber transparent für den Benutzer). Und umso weniger Passworter Benutzer für ihre tägliche Arbeit benötigten, desto eher sind sie gewillt, kompliziertere und sichere Passwörter zu wählen (was nicht heißt, dass sie nicht hierzu erzogen werden müssten).

Synchronisation der Daten

Im Jahr 1999 – also noch vor dem öffentlichen Erscheinen von Windows 2000 – hatte Microsoft eine Firma namens "ZoomIt" gekauft. ZoomIt war damals der führende Hersteller einer Meta-Directory-Software. Das übernommene Produkt, das eine Weile als "Microsoft Metadirectory Services (MMS)" Kunden unentgeltlich zur Verfügung gestellt wurde, ermöglicht die Synchronisation von Verzeichnisdiensten. Eigentlich alle Unternehmen speichern die Daten ihrer Benutzer nicht nur in einem Verzeichnisdienst, sondern in unterschiedlichsten Repositories. So gibt es häufig eine Applikation der Personalabteilung, sei es in einer Datenbank oder über einen Host. Dann gibt es E-Mailsysteme, manchmal SAP, Telefonlösungen und unterschiedlichste Anwendungen.

MMS, das später als Microsoft Identity Information Services (MIIS) neu geschrieben wurde, dann im Identity Lifecycle Manager (ILM) und neuerdings im Forefront Identity Manager (FIM) aufgegangen ist, bildet die Datendrehscheibe oder Synchronisations-Engine zwischen den unterschiedlichen Verzeichnisdiensten. Er stellt sicher, dass die Informationen in allen Verzeichnisdiensten synchron gehalten werden. Dazu wird zunächst definiert, welche Daten in welchen Quellen liegen und wer für welche Daten autoritativ ist (zum Beispiel das E-Mailsystem für die E-Mailsdresse, die Personalabteilung für den Job-Titel, und Windows für das Passwort). Dann wird der Datenfluss zwischen den unterschiedlichen Verzeichnisdiensten eingerichtet, auch eine Transformation der Daten (zum Beispiel generieren des Logon-Namens über den ersten Buchstaben des Vornamens und weitere sieben aus dem Nachnamen) ist dabei automatisierbar.

Auch Provisioning und Deprovisioning kann das Produkt bei entsprechender Konfiguration übernehmen: Provisioning ist hierbei der Vorgang, durch den ein Benutzer im Unternehmen seinen Account erhält (die Personalabteilung erstellt einen Eintrag für einen neuen Mitarbeiter im HR-System und muss diesen als Nächstes als Benutzer in allen relevanten Systemen anlegen: AD-Konto, Notes-Postfach, Update des Intranet-Telefonbuchs, SAP-Account et cetera). Deprovisioning bezeichnet den Vorgang, ein Benutzerkonto aus dem Unternehmen zu entfernen oder zumindest zu deaktiveren. Dabei können wir festhalten, dass das Provisioning eher nice-to-have ist, Deprovisioning aber zwingend erforderlich, um Anforderungen bezüglich Sicherheit oder Richtlinien zu genügen.

AD-Neuerungen in Windows Server 2008

Die nächste Version des Active Directory kam dann mit Windows Server 2008 im Mai 2008 auf den Markt. Dieser wurde ebenfalls gleich mit Service Pack 1 aus-

geliefert, da auf der Clientseite Windows Vista vorher erschien und die Serverversion und das Service Pack für den Client parallel entwickelt wurden. Microsoft hatte beschlossen, Client- und Serverversionen wieder gleichzeitig herauszubringen. Daher kamen das Vista SP1 und Windows Server 2008 mit SP1 gleichzeitig auf den Markt.

Windows Server 2008 ließ eindeutig erkennen, dass das Active Directory mittlerweile schon den Anforderungen von Groß- und Kleinunternehmen gerecht wurde, die verbesserten Funktionen betrafen längst nur noch Details. Um die Diensten von Domänencontrollern auch in unsicheren Umgebungen anbieten zu können, hält der "Schreibgeschützte Domänencontroller" (Read-Only Domänencontroller, RODC) eine Kopie des AD, die lediglich gelesen werden kann. Der RODC repliziert Änderungen nur zu sich, jedoch nicht weiter, und hält in der lokalen Kopie des AD normalerweise keine Benutzer- oder Computerpasswörter vor. Soll der RODC in verteilten Standorten eingesetzt werden, lässt sich festlegen, welche Passworte er sich merken darf, damit ein Logon auch ohne WAN-Verbindung möglich ist. Fine Grained Password Policies ermöglichen dem Administrator erstmals ohne Zusatztools, unterschiedliche Passwortrichtlinien für unterschiedliche Anwendergruppen (Administratoren, Servicekonten, Manager, HR) zu definieren und erzwingen.

Das AD wird wie die anderen Rollen im Server jetzt über den Servermanager eingerichtet und verwaltet. Zahlreiche Detailverbesserungen in der Benutzeroberfläche vereinfachen dabei die Arbeit des Administrators. Die Überwachung kann der Nutzer so einrichten, dass sowohl alte wie auch neue Werte bei Änderungen von Eigenschaften protokolliert werden. Und mit den Active Directory-Snapshots ist es möglich, zu jedem Zeitpunkt sogenannte Schnappschüsse des AD zu erstellen. Diese (oder auch Datensicherungen) erlauben dem Administrator, die Daten zu späteren Zeitpunkten vergleichend zu betrachten. So kann er feststellen, welche Änderungen erfolgt sind oder welche Datensicherungen die richtigen Daten für eine Wiederherstellung erhalten und diese mittels Scripting sogar direkt für Wiederherstellungen oder Versionierungen im AD verwenden.

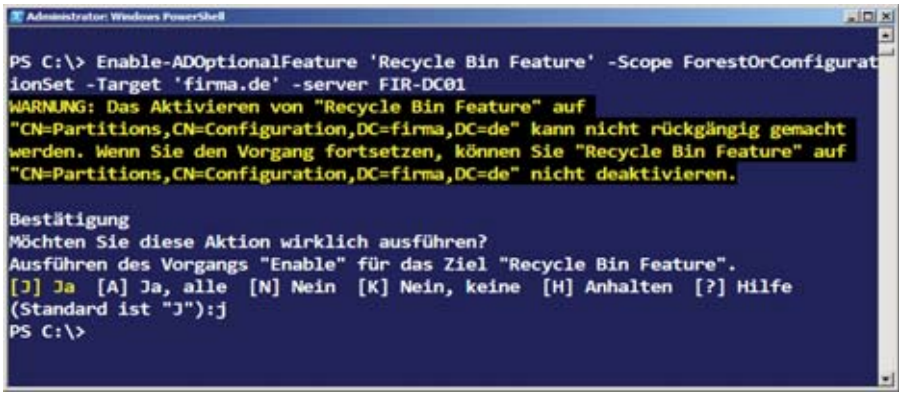


Bild 4: Windows Server 2008 R2 bietet endlich eine allumfassende Verwaltung über die PowerShell, manchmal jedoch zu Lasten der grafischen Benutzeroberfläche

Für die zentrale Verwaltung von Clients und Servern mit Hilfe von Gruppenrichtlinien ist die Gruppenrichtlinienverwaltungskonsole endlich fester Bestandteil des Betriebssystems. Zusätzlich ermöglichen Neuerungen im Bereich Gruppenpolicies das Mappen von Laufwerken, das Setzen von geplanten Aufgaben, das Einrichten von Verzeichnissen und Dateien, das Zuordnen von Druckern abhängig vom aktuellen Standort oder die Nutzung von Stromsparoptionen und vieles mehr.

Im DNS wurden ebenfalls Neuerungen implementiert. So werden große Zonen im Hintergrund aus dem AD geladen und der Server braucht nach einem Neustart nicht mehr so lange, bis er online ist. IPv6-Support ist quer durch das Betriebssystem in allen Rollen gewährleistet. Des Weiteren unterstützt die neue Version des DNS auch RODC. Das Feature "Global-Names-Zone" ermöglicht eine zonenübergreifende Kurznamensauflösung (für die Unternehmen, die WINS immer noch nicht loswerden konnten / wollten). Auch in der Benutzeroberfläche bekommen die Admins kleine Bonbons, so wird zum Beispiel der Zeitstempel der letzten Registrierung von Einträgen in der Übersicht der Einträge angezeigt und die "Bedingten Weiterleitungen" (Conditional Forwarder) können auch über die Benutzeroberfläche so eingerichtet werden, da sie sichtbarer sind und im AD repliziert werden.

Fazit

Das Active Directory hat in über zehn Jahren Evolutionen erfahren. Mit vielen Ambitionen gestartet, sollte es Großunternehmen beim Ablösen wirrer NT4-Domänenlandschaften unterstützen und dabei gleichzeitig die Infrastrukturen verbessern. Dabei sollte das AD über unterschiedliche Administrationsgruppen hinweg zu verwalten sein. Anfangs führte jedoch das eine oder andere Manko dazu, genau diesen Kundenkreis abzuschrecken. In unterschiedlichen Versionen hat das AD in diesem Bereich Verbesserungen erfahren, unterstützte gleichzeitig moderne Anforderungen, ist sicherer, verwaltbarer, nicht zuletzt individualisierbarer geworden.

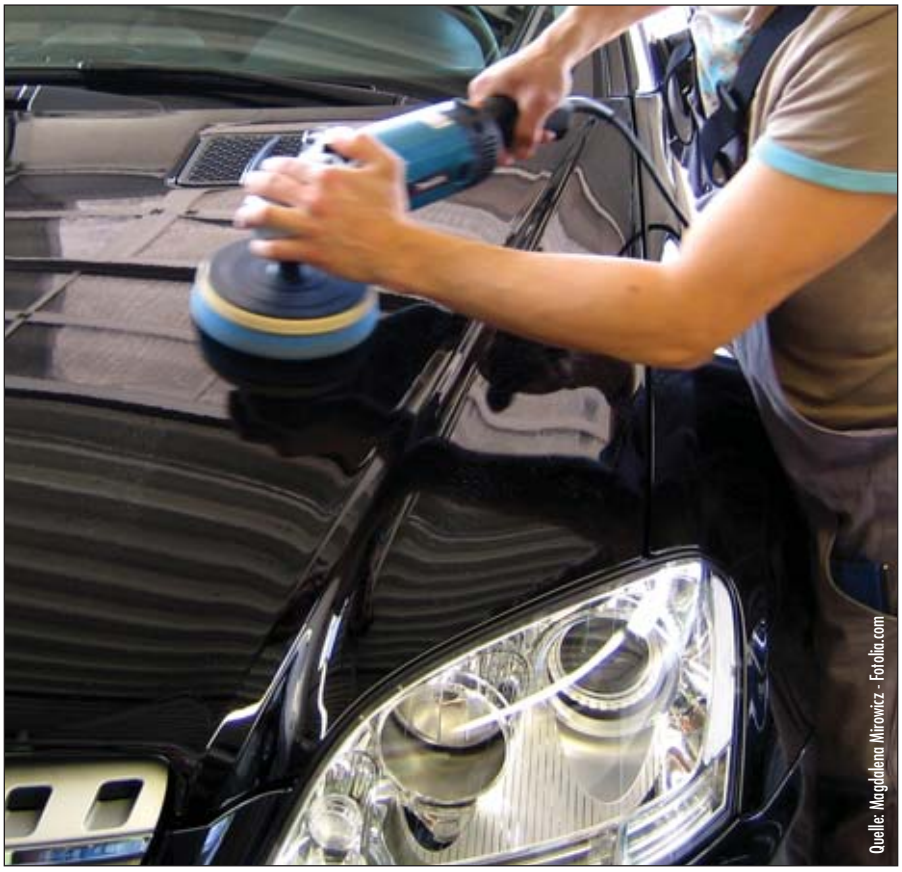
Heute ist das Active Directory die Kernkomponente in fast jeder Windows-basierenden Infrastruktur. Lesen Sie im nachfolgenden Beitrag, welche Neuerungen der Windows Server 2008 R2 im Active Directory mitbringt. *(jp)*

Neuerungen im Active Directory unter Windows Server 2008 R2

Verzeichnisdienst in neuem Glanz

Windows Server 2008 R2 springt mit einer ganzen Reihe an Neuerungen aus dem Startblock. Neben grundsätzlichen Erweiterungen wie etwa der Einführung von Hyper-V 2.0 oder einer aufgebohrten PowerShell haben sich die Entwickler aus Redmond auch ausgiebig dem Active Directory (AD) gewidmet und dem Verzeichnisdienst – neben einer neuen Admin-Console – eine Menge sinnvoller Funktionen verpasst.

Alle Jahre wieder, wenn Microsoft ein neues Server-Betriebssystem auf den Markt bringt, halten Administratoren Ausschau nach Funktionen und Werkzeugen, die ihnen ihre tägliche Arbeit erleichtern. So liest sich auch diesmal die gesamte Liste mit Erweiterungen recht spannend und der eine oder andere wird sicher wieder Brauchbares finden. So zum Beispiel beim Active Directory: Erweiterungen wie der Offline-Domänenbeitritt, ein Papierkorb oder gar das nagelneue Active Directory-Verwaltungscenter versprechen, die administrativen Tätigkeiten zu vereinfachen.


Quelle: Magdalena Mirowicz - Fotolia.com

Offline-Domänenbeitritt

Bislang kontaktierte ein Client einen Domänencontroller, wenn sein Computerkonto einer Active Directory-Domäne hinzugefügt wurde. Eine bestehende Netzwerkverbindung war hierfür unumgänglich. Diese Zeiten sind jetzt vorbei und bei der Installation muss hierauf keine Rücksicht mehr genommen werden. Zumindest gilt dies für Windows 7 und Windows Server 2008 R2 Computerkonten. Der Domänenbeitritt lässt sich bei diesen Installationen auf den Zeitpunkt des ersten Rechnerstarts verlagern, auch ist kein sofortiger Neustart mehr erforderlich. Die hierzu notwendigen Schritte erledigen Sie mit dem neuen Befehlszeilentool *dsjoin.exe*. Im ersten Schritt kommt das Tool auf einem Admin-PC zur Ausführung. Hierbei legt es Informationen in einer Konfigurationsdatei ab und erstellt die Metadaten für das Computerkonto im AD. Während der Installation des Clients verarbeitet dieser dann ebenfalls mit *dsjoin.exe* die zuvor erstellte Konfigurationsdatei und das Computerkonto ist nach dem abschließenden Neustart des Rechners online.

Neues Verwaltungscenter

Seit der ersten Version des AD ließen sich die Objekte mit der Management Console "AD Benutzer und Computer" bearbeiten. Lange Zeit war dies ein adäquates Werkzeug und erfüllte meist seinen Zweck. Mittlerweile ist es allerdings recht angestaubt und im heutigen Enterprise-Umfeld gerade bei vielen Domänen kaum

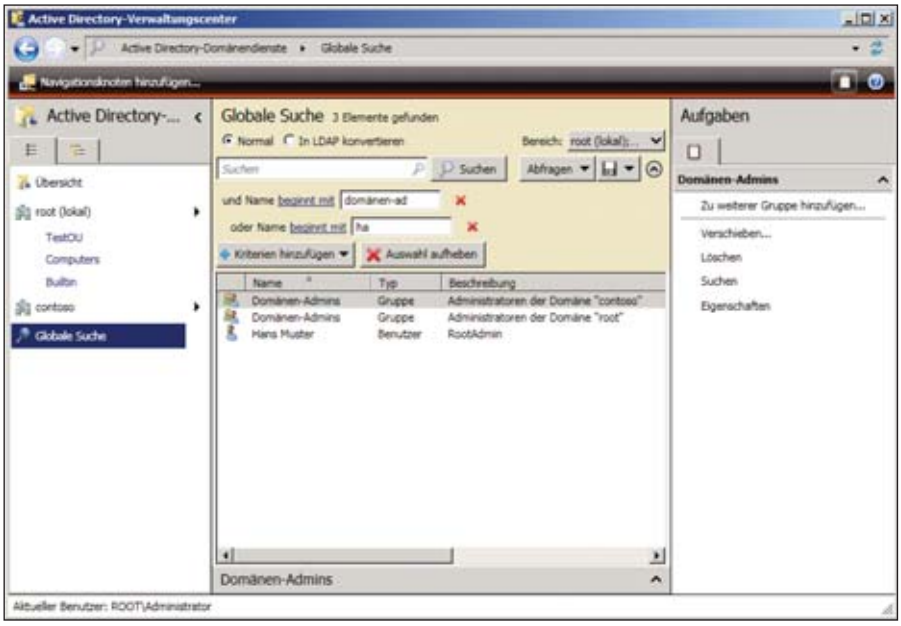


Bild 1: Noch nie war das Suchen im AD so einfach. Dank des neuen AD-Verwaltungscenters funktioniert dies nun auch domänenübergreifend.

mehr hilfreich. Das neue AD-Verwaltungscenter schafft hier Abhilfe. Es folgt nicht mehr dem Prinzip der Microsoft Management Console (MMC), sondern ist eine eigenständige Applikation, deren intuitiver Aufbau die ersten Schritte erleichtert. Nach ein paar Klicks sollte sich jeder auskennen, dem das Active Directory vertraut ist. Im linken Teil des Programmfensters zeigt sich der Navigationsbereich. Je nach Vorliebe des Administrators sind hier zwei Darstellungsarten möglich: Einmal die gewohnte Konsolenansicht, bei der sich die Knoten selektieren und dadurch ein- und wieder ausblenden lassen. Des Weiteren gibt es eine Listenansicht, die sich einer flachen Darstellungsart bedient. Unabhängig von der gewählten Ansicht ist der Startpunkt für die Navigation immer frei wählbar. Anders als beim bekannten AD-Benutzer und -Computer, dessen Darstellung immer beim Domänenknoten beginnt. Ausgangspunkt in der Navigation kann eine beliebige Organisationseinheit sein, aber auch Container und sogar andere Domänen aus der Gesamtstruktur sind hier zugelassen. Im Verwaltungscenter "Navigationsknoten" genannt, lassen diese sich zu jeder Zeit frei definieren. Damit ist schon eine der Stärken genannt: Die Darstellung in der GUI ist nicht mehr auf eine Domäne fokussiert, hier sind die aufgeführten Informationen aus der Gesamtstruktur beliebig kombinierbar.

In punkto Navigation und Suche gibt es aber noch weitere Raffinessen. Die globale Suche beispielsweise orientiert sich an den Navigationsknoten, die sich zum Zeitpunkt der Suche im Navigationsbereich befinden. Auf diese Art lässt sich selbst in den größten ADs mit hunderttausenden von Objekten schnell das Objekt der Begierde orten. Abgerundet werden die neuen Möglichkeiten durch aufgabenbasierte Filterkriterien, die anzuzeigende Objekte im Detailbereich zusätzlich eingrenzen. Objekte, die durch eine Suche gefunden wurden, lassen sich durch Mehrfachselektion in einem Schritt bearbeiten. Hier ist der Spielraum ebenfalls nicht auf eine Domäne begrenzt und die zu bearbeitenden Objekte dürfen verschiedenen Domänen der Gesamtstruktur entstammen.

Auffällig sind die Änderungen im Detailbereich zu einem Objekt. Beispielsweise bei der Darstellung der Benutzerinformationen. Hier hat Microsoft auf die bisherige, in Karteireiter geordnete Darstellung verzichtet. Der Weg geht hin zu einer Ansicht, die versucht, möglichst viele Informationen in einem Fenster zu bündeln. Dies ist letztendlich eine Frage des Geschmacks. Trotzdem fällt es angenehm auf, dass bei der Suche nach bestimmten Informationen zu einem Objekt das lästige Durchklicken durch die verschiedenen Tabs nicht mehr notwendig ist.

Das AD-Verwaltungscenter verrichtet seine Arbeit auf Basis von darunterliegenden Powershell-Skripten. Dabei ist allerdings schade, dass sich die Befehle nicht anzeigen lassen. Mit dieser Möglichkeit ließe sich für PowerShell-Unerfahrene der Zugang

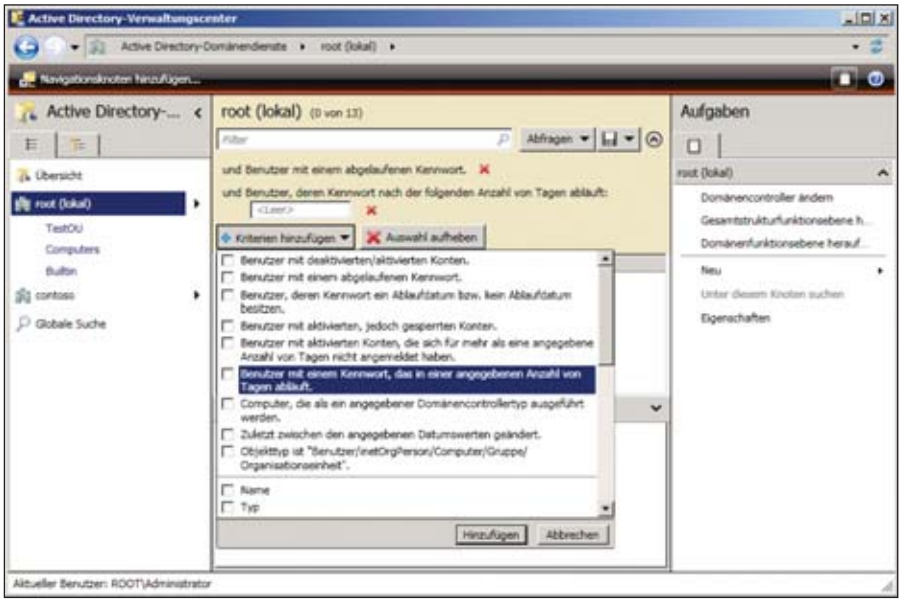


Bild 2: Aufgabenbasierte Filterkriterien im AD-Verwaltungscenter vereinfachen wiederkehrende Arbeitsschritte

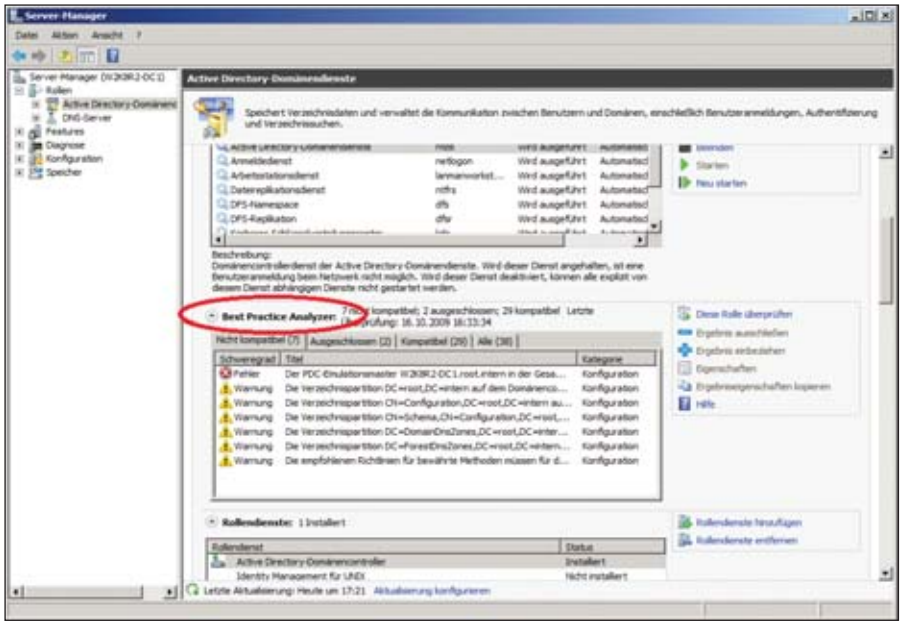


Bild 3: Der Best Practice Analyzer untersucht die aktuelle Umgebung und zeigt anhand von Microsoft-Empfehlungen Verbesserungspotenzial

zu dieser Sprache ebnen. Desweiteren ließen sich hierdurch Aktionen grundsätzlich designen, um sie dann im Anschluss für ein Skript an beliebige Bedürfnisse weiter anzupassen. Laut Microsoft ist dies eine Option für eine künftige Version.

Fehlkonfigurationen schnell erkennen

Der Best Practice Analyser (BPA) ist für verschiedene Dienste von Windows Server 2008 R2 verfügbar. Neben dem Active Directory lassen sich die Terminal Services, DNS oder auch die AD-Zertifikatsdienste in Bezug auf Fehlkonfigurationen hin untersuchen. Die Funktionsweise ist schlicht: Der BPA vergleicht vorgegebene Regelsätze mit dem, was er in der aktuellen Umgebung vorfindet. Bei Abweichungen quittiert er diese mit Warnungen oder gar Fehlern. Die Einstufung ist fest vorgegeben und folgt den Best Practices von Microsoft. Unter der Haube des BPA arbeiten ebenfalls PowerShell-Skripte, welche die umfangreichen Tests im Active Directory durchführen. Allerdings ist im Fehlerfall der BPA nicht das richtige Tool, um mögliche Ursachen für Probleme aufzuspüren. Der Einsatzzweck dürfte eher nach größeren Installationen gegeben sein oder aber einfach nur, um von Zeit zu Zeit zu sehen, ob noch alles richtig tickt.

Der BPA hat sich übrigens gut versteckt. Er befindet sich im Server Manager bei den installierten Rollen. Unterhalb der Rolle "Active Directory Domänendienste" lässt er sich aufrufen und die analysierten Daten können dort direkt eingesehen oder in die Zwischenablage kopiert werden. Möglichkeiten für einen Report oder einen Export der ermittelten Informationen sind nicht vorgesehen. Nachteilig ist das kleine Fenster, das innerhalb des Servermanagers einen gedrängten Eindruck hinterlässt.

Endlich da: Der Papierkorb für AD-Objekte

Gelöschte Objekte im AD gibt es immer wieder und dies lässt sich im administrativen Alltag wohl kaum vermeiden. Bislang ein Ärgernis, da der Weg, diese als "tombstoned" bezeichneten Objekte wiederherzustellen, äußerst umständlich ist. Autorisierter und nicht autorisierter Restore sind zeitaufwendig. Hinzu kommen fehlende Backlinks (Referenzen zu Infos, die nicht beim Objekt gespeichert werden, wie etwa Gruppenmitgliedschaften), um die es sich zu kümmern gilt, nachdem das gelöschte Objekt wieder an Ort

und Stelle ist. Ein solches Verfahren kann eigentlich keinem Administrator gefallen, ist doch meist Eile geboten, wenn ein Objekt versehentlich gelöscht wurde.

Mit R2 hat das Active Directory nun einen Papierkorb an Bord und die Arie zur Wiederherstellung gelöschter Objekte ist deutlich kürzer. Einfach gesagt: Wird ein Objekt gelöscht, wird es nicht wie bisher zum Tombstoned-Objekt, sondern verweilt noch eine Zeit (standardmäßig 180 Tage, analog zur Tombstone-Lifetime) im Papierkorb. Dies ist quasi eine Zwischenstufe vor dem bisher bekannten Löschprozess. Erst danach werden die Backlinks entfernt, was bedeutet, dass ein im Papierkorb befindliches Objekt, wie etwa ein Benutzerkonto, noch über alle Informationen verfügt, nachdem das gelöschte Konto wiederhergestellt wurde. Der Papierkorb als solches ist in der GUI der verschiedenen Admin-Tools übrigens nicht aufzutreiben. Seine Bedienung vollzieht sich ausschließlich über ein Cmdlet namens "Restore-ADObject". Voraussetzung für den Papierkorb ist, dass die Funktionsebene für die Gesamtstruktur auf den neuen Level Windows Server 2008 R2 heraufgestuft wurde und dass der Papierkorb grundlegend aktiviert ist.

Das Cmdlet zum Wiederherstellen gelöschter Objekte bietet eine Menge weiterer Möglichkeiten, die über die Funktion eines einfachen Papierkorbes hinausgehen. Daher lohnt es sich, in einer ruhigen Minute damit herumzuspielen, um für den Ernstfall gerüstet zu sein. Unabhängig vom Papierkorb und R2 lassen sich AD-Objekte übrigens vor versehentlichem Löschen schützen. Hierzu muss diese Option in den Objekteigenschaften entsprechend vermerkt sein.

Sonstige Neuerungen

Wer so oft wie es geht auf die Maus verzichten möchte, für den hat Microsoft rund 30 zusätzliche Cmdlets in das Active Directory Modul für die Powershell gepackt. Die gleichnamige Eingabeaufforderung lässt sich über das Startmenü aufrufen und eine Übersicht über alle Cmdlets liefert das Kommando *Get-Command *-AD**. Die Liste ist mittlerweile recht umfangreich und derjenige, der die Cmdlets geschickt einzusetzen weiß, hat jenseits der grafischen Verwaltungswerkzeuge ganz andere Möglichkeiten, sein AD zu administrieren. Mit dem Kommando *Get-Help {cmdlet name} -Full* lässt sich eine detaillierte Hilfe zu einem bestimmten Cmdlet anzeigen.

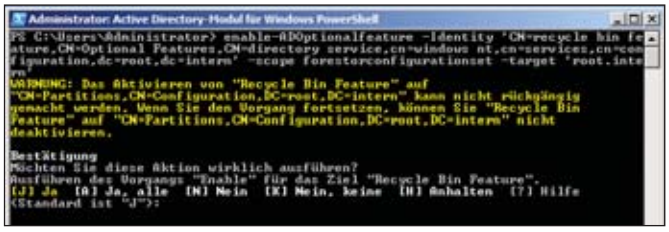


Bild 4: Auf einen grafischen Papierkorb müssen Admins verzichten. Bislang erfolgt die Bedienung ausschließlich über die PowerShell.

Managed Service Accounts sind ein weiteres neues Feature in R2 mit der Möglichkeit, die Administration von Dienstkonten weitestgehend zu automatisieren, einschließlich der Verwaltung des Kennwortes für das Dienstkonto. Damit dürfte endlich Schluss sein mit hängenden Diensten auf Applikationsservern, die nicht starten, weil das Passwort in der Domäne zurückgesetzt wurde oder gar das Konto gesperrt ist. Bei den Managed Service Accounts handelt es sich wiederum um eine neue Funktion, die ohne GUI daherkommt und deren Bedienung ausschließlich über Powershell-Befehle erfolgt.

Eine Technet-Webseite [1] bietet diverse Step-by-Step Guides an, die anhand praktischer Beispiele in die neuen Funktionen des Active Directories einführen. Zudem findet sich dort ein Migrationsleitfaden [2], der auf die wesentlichen Aspekte bei einem Wechsel eingeht und abhängige Dienste wie etwa DNS, die bei einer Migration auch Thema sind, nicht ausklammert.

Blick in die Zukunft

Spätestens jetzt dürfte der Zeitpunkt gekommen sein, an dem sich AD-Administratoren mit der Powershell auseinandersetzen sollten. Microsoft zeigt mit der Entwicklung des R2-Servers, dass die Powershell zunehmend an Bedeutung gewinnt. Die neue Powershell-basierte GUI und die Tatsache, dass bestimmte Funktionen ausschließlich per Powershell auszuführen sind, so etwa die Administration der Managed Service Accounts, sprechen eine deutliche Sprache. Entscheider, die vor der Wahl stehen, ihre Active Directory zu erneuern, können es langsam angehen lassen. Nachdem das Schema (mittels *adprep.exe* auf der Server- DVD) angepasst wurde, lässt sich der erste R2-Domänencontroller der Domäne hinzufügen. Der weitere Ausbau kann sukzessive erfolgen. Zu beachten ist nur, dass bei bestimmten Funktionen die Funktionsebene der Gesamtstruktur auf höchstem Level sein muss und in diesem Release keine DCs älterer Versionen mehr zulässig sind.

Fazit

Der neue Server von Microsoft bringt im Bereich Active Directory gewinnbringende Neuerungen. Allein das AD-Verwaltungscenter ist es wert, seinem AD einen Windows Server 2008 R2 DC zu spendieren. Offline-Domänenbeitritt oder der Papierkorb runden die gelungenen Funktionen im Bereich Active Directory ab. Wie bei kaum einem anderen neuen Betriebssystemrelease empfiehlt es sich diesmal, die neuen AD-Funktionen in einer Versuchsumgebung durchzuspielen. Die Powershell-Befehle sind mitunter recht zickig und ihr Umgang verlangt Geduld. Diese wird allerdings belohnt. *(ln)*

Von Klaus Bierschenk

[1] Windows Server 2008 R2 Active Directory
http://technet.microsoft.com/de-de/library/dd378801(WS.10).aspx

[2] Migrationsleitfaden für Server 2008 R2
http://technet.microsoft.com/de-de/library/dd379558(WS.10).aspx

Links

Active Directory-Strategien

Eine Frage der Planung

Eine Active Directory-Infrastruktur kann beim Entwurf weitestgehend frei gestaltet werden. Daher können Verzeichnisdienste so unterschiedlich sein wie ihre Unternehmen. In diesem Beitrag stellen wir Ihnen einige AD-Szenarien mit ihren jeweiligen Besonderheiten vor.

Quelle: kinara - Fotolia.com

Das Active Directory (AD) ist mittlerweile knapp zwölf Jahre alt – mit Windows 2000 Server hatte es im Dezember 1999 den Status "Release to Manufacturing" erreicht. Das Konzept war damals in der Microsoft-Welt recht neu:

- Domänen, die hierarchische Strukturen haben und DNS benötigen
- Ein Verzeichnis, das innerhalb einer Domäne auch hierarchisch untergliedert werden kann
- Eine Administration, die sich für Teilbereiche komplett delegieren lässt
- Gruppenrichtlinien, von denen nicht nur eine existiert, sondern eine Vielzahl und die fast alle Konfigurationseinstellungen für Clients und Server auch benutzerbasiert vorgeben können.

War das Active Directory von Anfang an sowohl für große, weltweit verteilte Unternehmen als auch kleine Firmen mit nur einem Standort ausgelegt, musste es sich zunächst noch weiterentwickeln. Nach und nach optimierte Microsoft den Verzeichnisdienst und es kamen die ersten Best Practices dazu heraus, wie Verzeichnisse für unterschiedliche Anforderungen idealerweise einzurichten sind. In diesem Beitrag werden wir einige gebräuchliche Modelle vorstellen.

Überlegungen zu Domänenmodellen

Beim Entwurf eines Domänenmodells muss der Administrator verschiedene Kriterien berücksichtigen:

- Wie sieht die Administrationsstruktur aus? Während früher eine Domäne als Sicherheitsgrenze galt, zählt heute die Gesamtstruktur als Verteidigungslinie – Domänenadministratoren fremder Domänen in der gleichen Gesamtstruktur könnten sich Rechte in anderen Domänen erschleichen.
- Wie ist die erwartete Größe der Active Directory-Datenbank?
- Wie sieht die globale Vernetzung aus? Gibt es irgendwo langsame und unzuverlässige WAN-Leitungen, oder ist die Infrastruktur schnell mit redundanten Leitungen ausgestattet?
- Wie arbeiten und reisen die Mitarbeiter? Sind die Mitarbeiter eher an dem Standort, dem sie primär zugeordnet sind, reisen sie eher innerhalb von Deutschland, Europa oder weltweit?
- Welche Anwendungen werden in den verschiedenen Standorten benötigt?

Dies sind nur einige von zahlreichen Überlegungen, die Sie beim Design eines Domänenmodells berücksichtigen müssen.

Als Microsoft mit Windows 2000 die erste Version des Verzeichnisdienstes vorstellte, hieß es, die Domäne sei eine Sicherheitsgrenze, da die Administration mit den Domänenadministratoren für jede Domäne getrennt werden könne. Delegation und Berechtigungen lassen sich auch für jede Domäne einzeln festlegen. Doch dann wurde eine Sicherheitslücke bekannt: Ein Domänenadministrator kann sich über die Rechte auf die SID-History einen Security Identifier (SID) des Domänenadministrators einer fremden, vertrauten Domäne zum eigenen

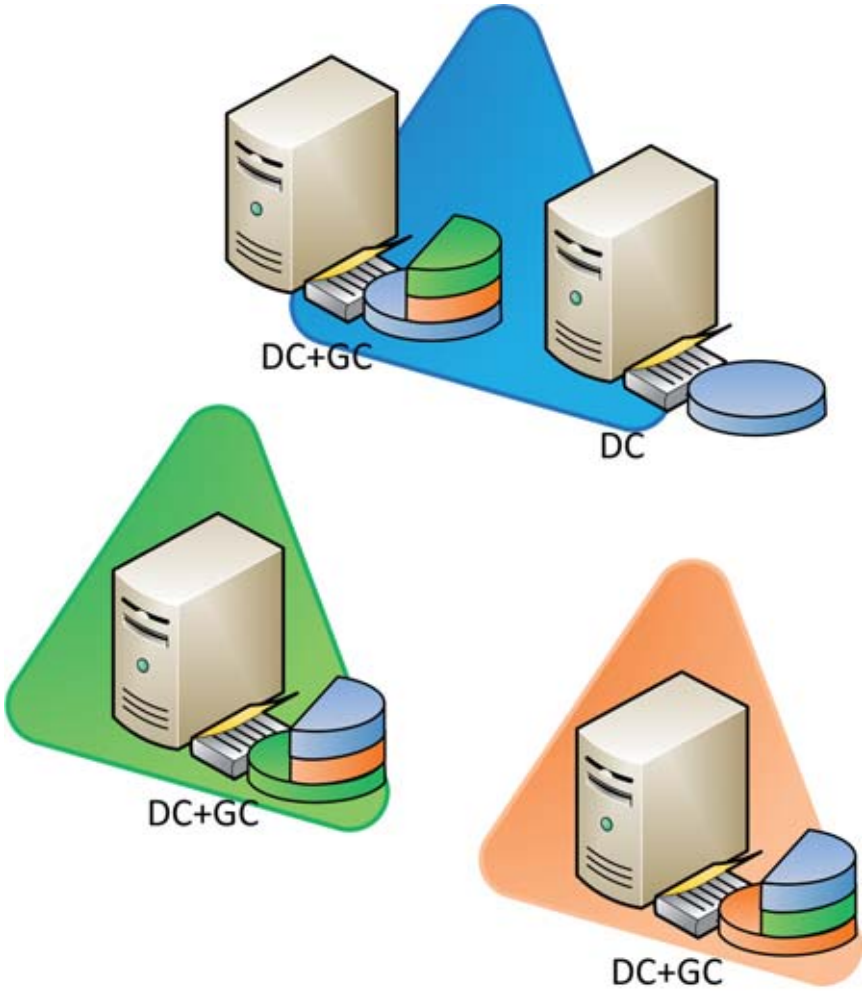


Bild 1: Domänencontroller enthalten immer alle Daten der eigenen Domäne. Sind sie zusätzlich Globaler Katalogserver, enthalten sie einen Teil von Informationen der anderen Domänen in der Gesamtstruktur.

Konto hinzufügen. Da sich dies in den Vertrauensstellungen einer Gesamtstruktur nicht vermeiden lässt, gilt nun die Gesamtstruktur als Sicherheitsgrenze. In der Realität sollte zwischen einer versehentlichen Fehladministration und der absichtlichen Sabotage unterschieden werden. Falls es Befürchtungen in Unternehmen gibt, dass sich Administratoren über derartige Wege Rechte erschleichen könnten, sollte sich das Unternehmen eher Gedanken über sein Personal denn über vermeintliche Sicherheitsgrenzen machen.

Datenbankgröße und Globaler Katalog

Jedes Objekt im Active Directory wird innerhalb der Domäne, in der es erstellt wurde, zwischen allen Domänencontrollern voll repliziert. Damit Objekte aber domänenübergreifend auffindbar sind, gibt es den Globalen Katalog (GC). Dieser ist eine Option bei DCs. Sobald der GC aktiviert ist, erhält er einen Teil der Eigenschaften jedes Objektes der fremden Domänen in der gleichen Gesamtstruktur. Jeder Domänencontroller der gleichen Domäne hält die gleichen Daten in der Datenbank – außer er ist ein GC. Dann besitzt er weitere Daten der vertrauten Domänen. Um die Datenbankgrößen und den Replikationsverkehr in sehr großen Unternehmen zu verringern, gelten dort häufig globale Kriterien wie "eine Domäne pro Kontinent". Dies bedeutet jedoch auch, dass sich reisende Kollegen dann gegebenenfalls über WAN-Leitungen anmelden müssen.

Globale Katalogserver sind wichtig für den Anmeldeprozess sowie für einige Applikationen. Exchange ist eine solche Applikation, die einen GC nutzt. Ein GC verfügt jedoch bei einer Gesamtstruktur von nur einer Domäne über keinerlei weitere Daten. Auch reagiert er nur auf zwei weitere Netzwerkports: GC und GC via SSL. Es ist daher wichtig, möglichst viele GCs zur Verfügung zu stellen. Während bis zu

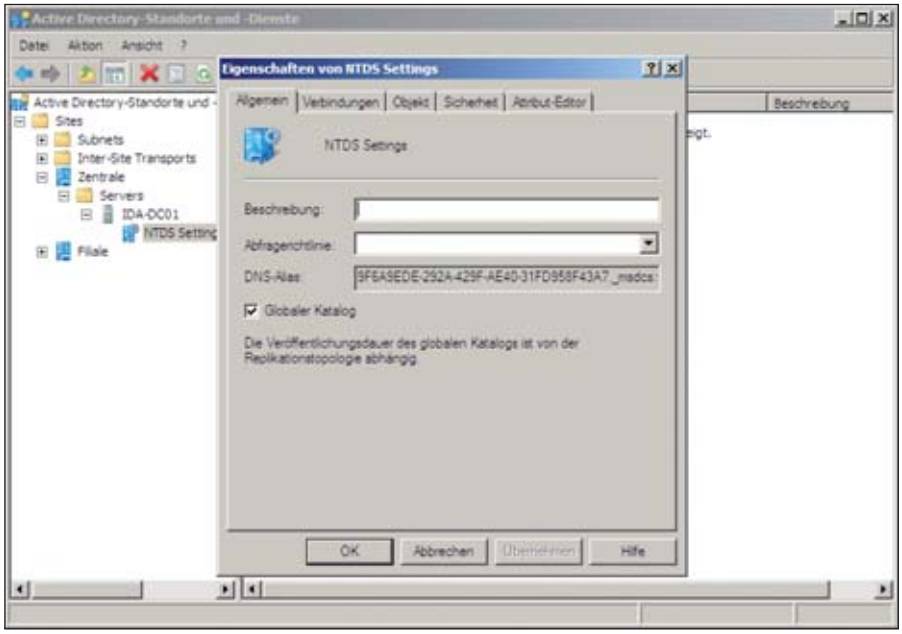


Bild 2: Die Einstellung "Globaler Katalogserver" verbirgt sich im NTDS Settings-Objekt des Domänencontrollers in "Active Directory-Standorte und -Dienste".

Bild 3: Der Infrastruktur-Master kann zum Beispiel über "Active Directory-Benutzer und -Computer" verschoben werden. Wählen Sie dazu einfach "Betriebsmaster" aus dem Kontextmenü der Domäne.

Windows Server 2003 R2 standardmäßig nur der erste Server einer Domäne ein GC war und der Administrator weitere Server manuell definieren musste, hat sich dies geändert. Mittlerweile ist bekannt, dass GCs wichtig sind und nicht immer manuell angepasst werden. Daher hat Microsoft den Standard geändert: Seit Windows Server 2008 wird jeder Domänencontroller zum GC – solange der Administrator dies nicht explizit anders einrichtet.

Auch bei der Diskussion "Infrastruktur-Master versus Global Katalog" gilt es zu verstehen: Der Infrastruktur-Master (IM) vergleicht die Inhalte seiner Datenbank mit denen eines GCs, um sogenannte Phantom-Objekte fremder Domänen (die Mitgliedern von Gruppen der eigenen Domäne sind) für Nicht-GCs zur Verfügung zu stellen. Dies ist nur notwendig, wenn mehrere Domänen existieren oder Domänencontroller existieren, die kein GC sind. In den folgenden Konstellationen wird daher gar kein IM benötigt:

- Es gibt nur eine Domäne in der Gesamtstruktur.
- Jeder Domänencontroller in der Gesamtstruktur ist GC.
- In einer bestimmten Domäne wird kein IM benötigt, wenn in dieser Domäne alle DCs auch GCs sind.

Sind jedoch Domänencontroller einer bestimmten Domäne nicht GC, dann muss der Infrastructure-Master auf einem DC liegen, der nicht GC ist.

Verschiedene Domänenmodelle

Die einzelne Domäne im Unternehmen ist das wohl üblichste Szenario. In dieser Domäne befinden sich alle Benutzerkonten, Gruppen, Computer et cetera und werden über diese verwaltet. Dies ist die einfachste Version, die angewendet werden sollte, wenn keine triftigen Gründe dagegen sprechen. Hierbei kann jeder Domänencontroller auch zum Globalen Katalogserver ernannt werden, da er keine weiteren Informationen hält, aber auf Anfragen von Applikationen diesbezüglich reagiert. Es macht jedoch keinen Sinn, DCs zu nutzen, die kein GC sind. Auch der Infrastruktur-Master hat hier keine Aufgabe.

Ein Spezialfall stellt die einzelne Domäne mit einer leeren Rootdomäne (Empty-Root) dar. Dies stammt noch aus den Empfehlungen alter Zeiten, wo die Domäne noch als Sicherheitsgrenze angesehen wurde und Unternehmen eine leere Rootdomäne nutzen wollten, um die "Enterprise-Administration" von der Domänenadministration zu trennen. Hierbei gilt zu beachten, das die Root-Systeme, von denen meistens nur zwei bis vier Domänencontroller im zentralen Rechenzentrum stehen, nicht für den Logon verwendet werden sollten. Daher ist es wichtig, dass zum Beispiel die DNS-Domäne "_msdcs.{forest-root-domäne}" als separate Zone auf alle Domänencontroller der Gesamtstruktur repliziert wird, da diese zum einen für den Replikationsverkehr und zum anderen für das Finden der Globalen Katalogserver verwendet wird. Mehr hierzu im Beitrag "Active Directory und DNS" auf Seite 48.

Eine selten berücksichtigte Option ist der Globale Katalogserver bei einer einzelnen Domäne mit einer leeren Rootdomäne darüber. Auch hier macht es Sinn, jeden DC zum GC zu ernennen, da die Root-Domäne so gut wie keine Objekte besitzt, die für zusätzliche Daten in der Kontendomäne sorgen. Die Rootdomäne langweilt sich daher, so dass es unerheblich ist, ob die Objekte der Kontendomäne im GC repliziert werden. Bei diesem Szenario sollte auch berücksichtigt werden,

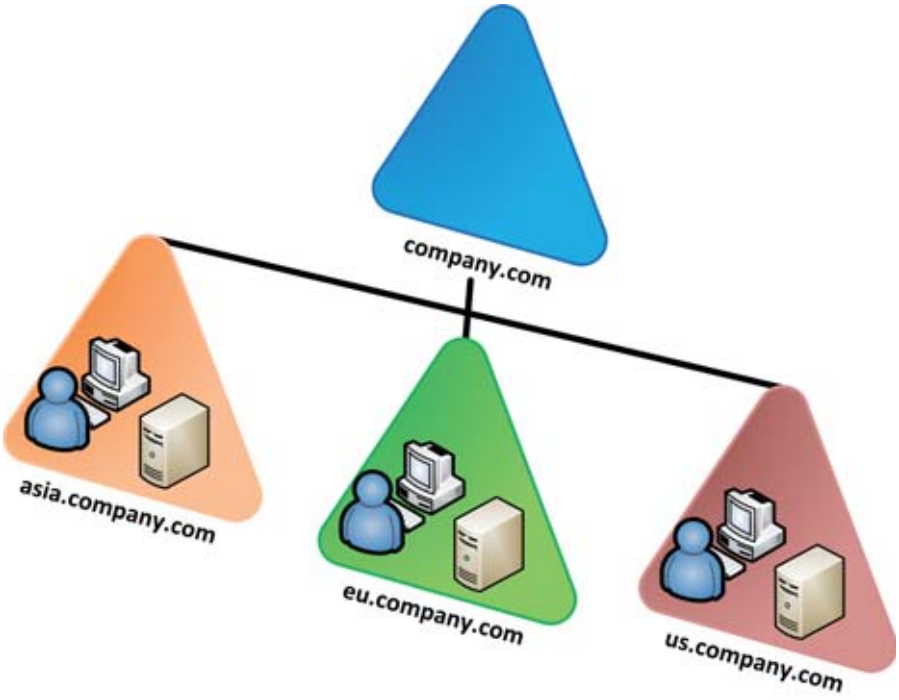


Bild 4: Eine geografische Aufteilung der Gesamtstruktur ist bei größeren Unternehmen häufig sinnvoll.

dass es möglich ist, die Rootdomäne in einen eigenen Baum zu integrieren anstatt hierarchisch über die Kontendomäne. So ist es denkbar, dass die Firma den eigenen DNS-Namen als Kontendomäne und einen künstlichen Namen für die Rootdomäne verwendet (wie "firma.de" und "root.loc").

In größeren Umgebungen kann die Aufteilung der Benutzer in mehrere Domänen sinnvoll sein. Hier kommt dann auch die leere Rootdomäne zum Einsatz. Allerdings ist die Struktur in diesem Fall dann häufig hierarchisch aufgebaut, einschließlich mehrerer Subdomänen mit Benutzerkonten sowie weiteren Objekten. Dabei ist es in der Regel nicht sinnvoll, die Domänen etwa nach Geschäftsbereichen zu sortieren, da Sie vermeiden sollten, dass Benutzerkonten "migriert" werden müssen – etwa, weil es eine Umstrukturierung gegeben hat oder Mitarbeiter neue Aufgaben im Unternehmen wahrnehmen. Meist ergibt aus diesem Grund eine geografische Aufteilung, zum Beispiel nach Ländern oder Kontinenten, mehr Sinn. Eine weitere Option ist, neben den geografischen Domänen eine "Ressourcendomäne" für Applikationen bereitzuhalten.

Jenseits der Gesamtstruktur

Neben den unterschiedlichen Domänenmodellen innerhalb einer Gesamtstruktur gibt es auch Gründe, aus einer solchen Gesamtstruktur auszubrechen. Ein Szenario wäre, wenn unterschiedliche Unternehmen in einem Konzern zwar im Netzwerk zusammenarbeiten, aber aus häufig historischen Gründen getrennte Domänen und Gesamtstrukturen nutzen. Dann geht es darum, wie diese Unternehmen zusammenarbeiten können. Hier reichen die Szenarien vom Austausch der Kontaktinformationen für Exchange über Webapplikationen, die Active Directory Federation Services oder ein zentrales Metadirectory benutzen, Vertrauensstellungen bis hin zu unabhängigen Ressourcen-Gesamtumgebungen. Dies kann auch für neue Implementierungen ein interessanter Ansatz sein, wenn Sie sich das Ausgliedern oder Eingliedern von Betrieben vereinfachen möchten.

Des Weiteren kann es für einzelne oder mehrere Applikationen hilfreich sein, in einer separaten Gesamtstruktur als Ressourcendomäne betrieben zu werden. Wenn die Applikation zum Beispiel Schema-Updates benötigt, die Sie im produktiven Forest nicht durchführen möchten oder wenn die Applikation für mehrere Umgebungen unabhängig zur Verfügung gestellt werden soll. Gleiches gilt auch, wenn die Anforderungen, zum Beispiel das Sicherheitsmodell betreffend, nicht in der normalen Umgebung erfüllt werden können. Diese Ansätze gehen dann schon in die Richtung Private Cloud. In diesen Fällen müssen Sie dann häufig auch über die Verzeichnisdienstsynchronisation nachdenken. Exchange in einem Ressourceforest etwa benötigt "Schattenbenutzer", mit denen die Mailbox verknüpft werden kann. SharePoint benötigt ebenfalls einen Benutzer oder Federation Services für die Authentifizierung und manche Unternehmensanforderungen eventuell nur einen Abgleich von Benutzer- und Kontaktinformationen. Um die Inhalte von Verzeichnisdiensten zu synchronisieren oder gar Passwörter abzugleichen, bieten sich die Produkte "Identity Integration Feature Pack" (frei von Microsoft verfügbar), Forefront Identity Manager (nicht frei, dafür sehr mächtig, auch mit Self-Service Verwaltung von Gruppen), Software von Drittherstellern oder eigens entwickelte Skripte an.

Active Directory in der DMZ

Immer mehr Unternehmen möchten ihr Active Directory auch in der Demilitarisierten Zone (DMZ) einsetzen. So gibt es Applikationen, die auch dort ein Active Directory benötigen. Durch den Einsatz von AD in der DMZ hat das Unternehmen unter anderem die folgenden Vorteile:

- Benutzerkonten können übergreifend verwaltet werden, Passwortwechsel erzwungen, unterschiedliche Passwortrichtilinien verwendet und Konten zentral gesperrt werden.
- Die volle Benutzer- und Gruppenverwaltung lässt sich für Benutzerkonten und Computer verwenden.
- Über Gruppenrichtlinien kann sichergestellt werden, dass die Systeme nicht nur anfangs gehärtet sind, sondern auch gehärtet bleiben.
- Über Gruppenrichtlinien lässt sich zusätzlich zu den Firewall-Appliances auch die lokale Firewall verwenden, um den Applikationsverkehr zu steuern.
- Kerberos ist als Authentifizerungsprotokoll einsetzbar.
- Linux- und Unix-Derivate können sich bei Bedarf auch an der Windows-Domäne authentifizieren.

Ohne das Active Directory wären diese Systeme eher schlecht verwaltbar, durch das Active Directory in der DMZ können Sie die Sicherheit erhöhen.

Um Computer in der DMZ in ein Active Directory aufzunehmen, gibt es verschiedene Möglichkeiten:

- Sie beitreiben ein vollwertiges AD in der DMZ, unabhängig vom AD im Intranet. Hierbei herrscht das Risiko, dass beschreibbare DCs in der DMZ stehen. Diese müssen besonders geschützt werden, ein mehrstufiger Ansatz für die DMZ wäre empfehlenswert.
- Ein vollwertiges AD für die DMZ steht hinter der Firewall im Intranet. Damit sind die Domänencontroller im Intranet, und die Computer in der DMZ können sich dagegen authentifizieren. Jedoch muss die Firewall hierfür stärker geöffnet werden.
- Ein Read-Only Domänencontroller der Intranet-Domäne in der DMZ erhöht die Sicherheit, allerdings sind alle Konten (aber nicht deren Passwörter) in der DMZ hinterlegt.
- Ein Read-Only Domänencontroller der DMZ-Domäne in der DMZ repliziert mit einem vollen Domänencontroller im Intranet, hat gegebenenfalls eine Vertrauensstellung zu der

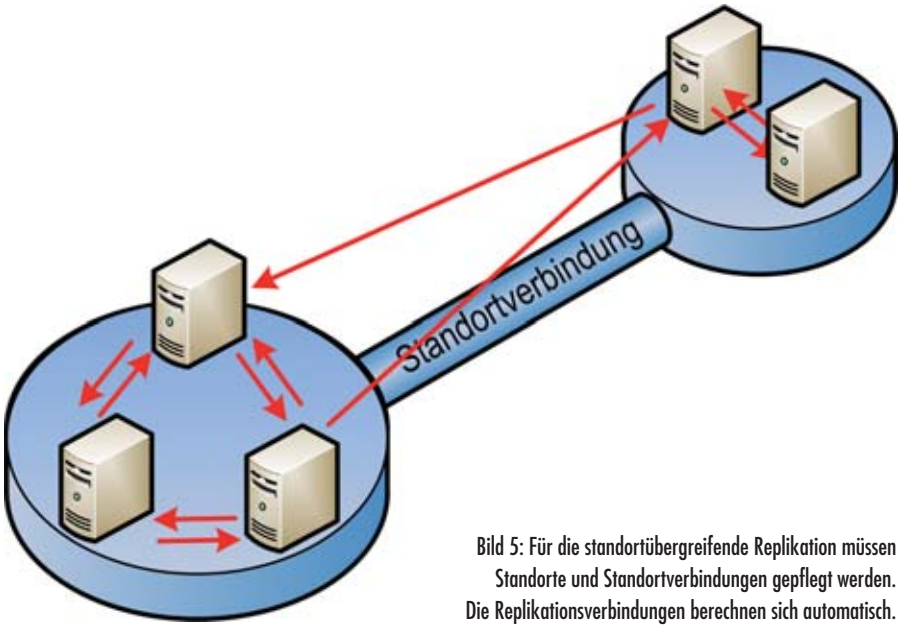


Bild 5: Für die standortübergreifende Replikation müssen Standorte und Standortverbindungen gepflegt werden. Die Replikationsverbindungen berechnen sich automatisch.

Intranet-Domäne: Dieses Szenario bietet einen RODC, keine Kennwörter in der DMZ, aber Domänenkonten könnten sich über die Vertrauensstellung anmelden.

Es gibt einige Szenarien, die hierfür in Frage kommen, jedoch müssen diese auf die genauen Anforderungen des Unternehmens abgestimmt werden, da unterschiedliche Applikationsanforderungen und Sicherheitsanforderungen differenzierte Maßnahmen benötigen. Welche Optionen es hierfür für die Firewall gibt, steht im Artikel "Replikation und Firewalls" auf Seite 152.

Active Directory für Außenstellen

Neben Unternehmen mit wenigen, großen Standorten gibt es auch Firmen mit ganzen Filialstrukturen, in denen aber häufig nur wenige Mitarbeiter arbeiten. Hierbei gilt es abzuwägen:

- Wie ist die Netzwerkanbindung der einzelnen Standorte? Wie zuverlässig ist diese?
- Welche Applikationen benötigen die Benutzer in diesen Standorten?
- Welches Datenvolumen erzeugen die Anwendungen zwischen welchen Systemen?
- Wo entstehen Daten, die gesichert werden müssen?
- Welche Anwendungen können sinnvoll verwendet werden, wenn die WAN-Leitung ausgefallen sind, abhängig davon, ob ein Server dezentral oder zentral steht? So kann ein dezentraler E-Mailserver, der zwar E-Mails von den Anwendern empfängt aber nicht weiterleiten kann, häufig als überflüssig betrachtet werden, während ein dezentraler Druckserver häufig Sinn macht.

Diese und viele weitere Fragen helfen bei der Entscheidungsfindung bezüglich der Zentalisierung von Servern. Insgesamt eine knifflige Situation, bei der Sie eine Menge Variablen abzuwägen haben. Häufige Diskussionen beinhalten auch dezentrale Dateidienste, Verteilung von Software-Updates bis hin zu Internet-Proxys. Entweder handelt es sich um Daten, die Sie den Anwendern zur Verfügung stellen möchten, oder um Daten, die Sie unternehmensweit bereitstellen müssen.

Im Bezug auf die Verteilung von Domänencontrollern oder schreibgeschützen Domäencontrollern müssen Sie zudem abwägen, inwieweit diese dezentral Sinn machen oder zentralisiert werden können. Stehen Applikationsserver in den Standorten, die Domänencontroller verwenden? Wie lastintensiv sind diese? Welche Dienste stehen den Benutzern zur Verfügung wenn:

- die WAN-Leitung offline ist?
- ein Domänencontroller vor Ort stünde?
- sich die Benutzer "nur" über Cached Credentials lokal anmelden?

Häufig sind in Außenstellen keine dezentralen Server vorhanden. Dann lohnt auch ein Domänencontroller nicht. Oder er hat gleichzeitig die Rolle als lokaler Druckserver und BranchCache inne, um Netzwerkdaten aus der Filiale zwischenzuspeichern. Auf alle Fälle sollten Sie über obige Punkte nachdenken, und mit Hilfe der Antworten Ihre Standorte und Dienste planen.

Active Directory-Replikation

Damit das Active Directory seine Daten konsistent auf allen DCs identisch halten kann, müssen die Domänencontroller replizieren. Hierbei werden nicht die Inhalte der Datenbank direkt von den DCs übertragen, sondern "die Applikation" Active Directory kümmert sich darum. Um die Replikationsinfrastruktur korrekt aufzubauen, ist es wichtig, die Standorte zu definieren. Als Faustregel gilt: Jeder physikalische Standort sollte auch ein Active Directory-Standort sein, es sei denn, dass verschiedene Active Directory Standorte mit LAN-Geschwindigkeit miteinander verbunden sind. Dann ist es egal, welchen Domänencontroller welchen Standortes die Clients verwenden.

In dem Fall können Sie diese Standorte in einem logischen Active Directory-Standort zusammenfassen. Umgekehrtes gilt für Kleinststandorte, in denen kein Domänencontroller oder sonstiger Server (der die Standorttopologie berücksichtigt) läuft. Diese können dann mit dem nächsten, größeren Standort zusammengefügt werden. Ein Standort definiert sich über die IP-Subnetze, die dem physikalischen Standort zugeordnet sind – im AD müssen sie allerdings gepflegt werden.

Damit die Replikationsstruktur richtig berechnet werden kann, müssen die Standorte über Standortverbindungen miteinander verbunden werden. Hierbei gilt zu beachten: Besteht eine Standortverbindung zwischen mehr als zwei Standorten, so werden diese zufällig, gegebenenfalls maschenförmig oder im Kreis miteinander replizieren. Dies ist nicht weiter schlimm, viele Unternehmen möchten jedoch die Replikationsstrecken genau kennen. Hierfür sollte dann jede Standortverbindung nur genau zwei Standorte beinhalten.

Dies führt dazu, dass über die Standortverbindung hinweg eine eingehende und eine ausgehende Replikationsverbindung erzeugt werden. Um genau festzuschreiben, welche Server dies auf der einen oder sogar beiden Seiten sein sollen, können Sie Bridgeheadserver definieren. Mehr dazu im bereits erwähnten Artikel "Replikation über Firewalls" auf Seite 152.

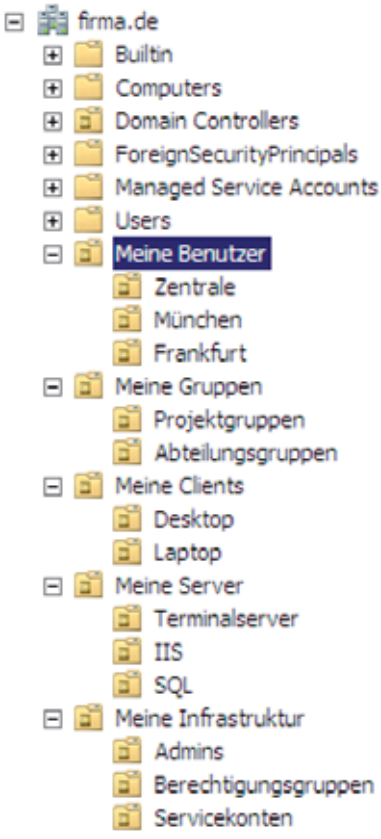


Bild 6: Das OU-Design sollte sich zunächst an der administrativen Struktur und erst danach an Gruppenrichtlinien orientieren

Struktur der OUs entwerfen

Um eine OU-Struktur zu entwerfen, sollten zunächst die administrativen Aufgaben verteilt werden:

- Gibt es Helpdesks für einen Teil der Benutzerverwaltung?
- Pflegen die Teilprojekte ihre Gruppen selbst?
- Gibt es Techniker, die Computer zur Domäne hinzufügen sollen?
- Ist jemand für Telefonie zuständig und pflegt diese Werte?
- Gibt es Standortadministratoren, die teilweise die Benutzerpflege Ihrer Benutzer übernehmen, und auch teils eigene Maschinen zur Domäne nehmen und eigene Gruppen verwalten?
- Wer erstellt die Gruppenrichtlinien?
- Wer bestimmt, welche Passwortrichtlinie für ein Benuzterkonto gelten soll?

Eine OU-Struktur sollte, beziehungsweise muss, immer zuerst am administrativen Rollenmodel ausgerichtet werden, damit Berechtigungen delegiert werden können (siehe hierzu den Beitrag "Sicherheit und Delegation im AD" auf Seite 117). Dann sollten Sie überlegen, wo welche Gruppenrichtlinien angewendet werden sollten. Dies ist allerdings nur zweitrangiges Kriterium beim Entwickeln eines OU-Models. Bedenken Sie auch, dass der Anwender die OU-Struktur normalerweise nicht sieht. Es macht also keinen Sinn, diese an einer Abteilungsstruktur auszurichten, es sei denn, es gibt Abteilungsadministratoren.

Die OU-Struktur ist rein technisch und bestimmt primär, wie administrativ delegiert werden kann, und sekundär, wie Gruppenrichtlinien angewendet werden können. Häufig ergeben die Überlegungen ein OU-Model, in dem in der ersten Hierarchieebene zuerst nach den unterschiedlichen Objekttypen unterteilt wird: Benutzer, Gruppen, Clientcomputer und Server. Sie sind gut beraten, parallel eine OU anzulegen (zum Beispiel namens "Infrastruktur"), in dem administrative Konten, Dienstekonten, Gruppen für höhere administrative Aufgaben wie AD-Delegation sowie Server erstellt werden, deren Verwaltung auf keinen Fall delegiert werden, sondern nur den Domänenadmins vorbehalten bleiben soll. Damit vermeiden Sie, dass ein Gruppenverwalter sich zum Mitglied einer solchen macht und über diese Mitgliedschaft seine eigenen Berechtigungen im AD verändern kann.

In der zweiten Ebene wird dann so aufgeteilt, wie es nach obigen Fragen sinnvoll erscheint. Das kann zum Beispiel bei Benutzern nach Standorten der Fall sein (bei Standortadmins), bei Gruppen nach deren Funktion (Projektgruppen oder Abteilungsgruppen), bei Clients nach Standort und Unterscheidung nach Deskop oder Laptop für Gruppenrichtlinien. Auch bei Servern mit einer Differenzierung nach Aufgaben (Terminal- server, Web-Server, E-Mailserver et cetera) macht dies Sinn, um die Serveradministration der entsprechenden Fachabteilung zu delegieren. Die Verwendung von Built-In-Gruppen wie Kontenoperatoren, sollten Sie jedoch vermeiden, da diese zu hohe Rechte erlangen: Sie können überall in der OU-Struktur (also auch in unserer eigentlich den Domänenadministratoren vorbehaltene OU) Benutzer, Gruppen und Computer erstellen, löschen und verwalten. Besser ist es, hierfür eine eigene Gruppe zu schaffen und dieser die Rechte zu geben.

Fazit

Im Active Directory lassen sich zahlreiche Unternehmensanforderungen abbilden. Es gibt unterschiedlichste Szenarien, sei es im Domänenmodel, mit unterschiedlichen Gesamtstrukturen, bei der Replikationsinfrastruktur oder im OU-Design. Vor allem Private Cloud-Ansätze mit Ressourcendomänen, bei der Zusammenarbeit mehrerer Gesamtumgebungen, oder Thematiken rund um die DMZ sind immer häufiger zu finden. Obwohl viele Active Directory Infrastrukturen unterschiedlich aussehen, gibt es meist Best Practices, die es zu berücksichtigen gilt. *(dr)*

Quelle: shocktactor - Fotolia.com

Versionierung von Active Directory-Domänen und -Forestlevel verstehen

Level Up

Mit der Veröffentlichung mehrerer Windows Server-Versionen über die Jahre hinweg hat Microsoft seinen Verzeichnisdienst stets verbessert und neue Funktionen hinzugefügt. Jede Iteration des Server-Betriebssystems seit Windows Server 2003 bringt Erweiterungen im Active Directory mit sich. Diese Erweiterungen sind teils Verbesserungen bestehender Systemtools oder Technologien sowie Funktionsweisen des Verzeichnisses. Abhängig davon, ob lokale oder verteilte Komponenten zu diesen Erweiterungen gehören, müssen Domänencontroller, die Domäne oder die Gesamtstruktur Voraussetzungen erfüllen, um neue Features nutzen zu können. Verbesserungen in der Active Directory-Replikation, die alle Domänencontrollern der Domäne oder gar der Gesamtstruktur nutzen, müssen sowohl von bestehenden als auch neuen Domänencontrollern unterstützt und angewendet werden. Dieser Workshop zeigt Ihnen, wie Sie die Active Directory-Domänen- und -Forestlevel ermitteln und welche dedizierten Features die einzelnen Server-Versionen mit sich bringen.

Seit Windows 2000 gibt es für das Active Directory (AD) den sogenannten "Funktionsmodus" ("functional levels"), anhand dessen sich neue Funktionalitäten kategorisieren und einordnen lassen. Unterschieden wird zwischen dem Domänenfunktionsmodus ("domain functional level", DFL) und den Gesamtstrukturfunktionsmodus ("forest functional level", FFL). Die Domänenfunktionsstufen bestimmen die einsetzbaren Domänencontroller (DC) in der aktuellen Domäne und aktivieren zudem neue Features. Das Aktivieren des Domänenfunktionsmodus "Windows Server 2003" ermöglicht die Nutzung neuer Funktionen, bedingt jedoch, dass alle Domänencontroller der Domäne mindestens Windows Server 2003 ausführen.

Für andere Funktionen reicht es wiederum nicht aus, den Domänenfunktionsmodus anzuheben, da sie über Domänengrenzen hinaus eingesetzt werden. Beispiele hierfür sind die Replikation oder die Umbenennung von Domänen. Hierfür müssen Administratoren den Gesamtstrukturfunktionsmodus anheben. Auch hier gelten besondere Regeln: Für ein Anheben des FFL müssen alle im Forest befindlichen Domänen bereits im gleichnamigen DFL sein.

Wechsel der Domänenstufe

Einmal aktiviert, können die Funktionsmodi nicht mehr zurückgestuft werden. Es ist eine Einbahnstraßen-Funktion, mit der Administratoren neue Funktionen freischalten und zeitgleich ältere Domänencontroller aus der Domäne ausschließen. Das Heraufstufen eines Windows Server 2003-Memberservers schlägt demzufolge fehl, wenn Administratoren den Domänenfunktionsmodus "Windows Server 2008" aktivieren. Als Mitgliedsserver dürfen sie aber dennoch weiterhin der Domäne beiwohnen.

Das Wechseln eines Funktionsmodus ist einfach: Der Domänenfunktionsmodus wird per Rechtsklick auf den Domänennamen und Auswahl von "Domänenfunktionsebene heraufstufen" in "Active Directory-Benutzer und -Computer" geändert. Für den Gesamtstrukturfunktionsmodus funktioniert dies analog im MMC-Snapin "Active Directory-Domänen und -Vertrauensstellungen" per Rechtsklick auf den gleichnamigen Hauptknoten und Auswahl von "Gesamtstrukturfunktionsebene heraufstufen". In den gleichen Dialogen sehen Sie, in welchem Modus die Domäne und die Gesamtstruktur sich gerade befinden. Welche Features genau welchen Funktionsmodus benötigen und welche Features bereits mit der Einführung eines Servers oder DCs mit einem Betriebssystem zur Verfügung stehen, zeigt die Tabelle "Funktionen der Active Directory-Versionen" am Ende dieses Artikel.

Ermittlung des Funktionsmodus mit DSQuery

Um festzustellen, welcher Domänen- oder Gesamtstrukturfunktionsmodus konfigu-

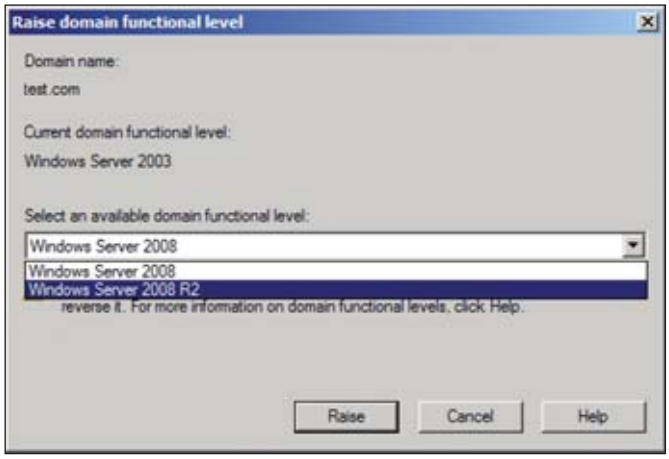


Bild 1: Das Anheben des Funktionsmodus lässt sich nur einmalig durchführen und nicht mehr rückgängig machen

riert ist, arbeiten Sie mit dem Kommandozeilenprogramm DSQuery. Die Ermittlung des Gesamtstrukturfunktionsmodus erfolgt dabei über den Befehl:

```
DSQuery * CN=Partitions,CN=
  Configuration,DC=domain,
  DC=tld -scope base -attr
  msDS-Behavior-Version
```

Wie zu erkennen ist, wird das Attribut "msDS-Behavior-Version" für die Speicherung des Modus verwendet. Der gelieferte Wert hat folgende Bedeutung:

- Wert "0" entspricht Windows 2000
- "1" = Windows Server 2003 Interim (bei Upgrades von Windows NT)
- "2" = Windows Server 2003
- "3" = Windows Server 2008
- "4" = Windows Server 2008 R2

Zur Ermittlung des Domänenfunktionsmodus nutzen Sie:

```
DSQuery * DC=domain,DC=tld -scope
  base -attr msDS-Behavior-Version
```

AD-Funktionen der verschiedenen Windows-Server

Um den heutigen Stand des AD zu verstehen und einzelne Funktionen besser einordnen zu können, ist es ratsam, sich mit seiner Geschichte auseinander zu setzen und die wichtigsten Funktionen und ihre Einführung zu durchleuchten.

Windows Server 2003

Nachdem Microsoft mit Windows 2000 das AD einführte, ist der Windows Server 2003 das erste Windows-Release, das Änderungen und neue Funktionen für das AD lieferte. Zu den Änderungen zählten überwiegend Verbesserungen, die die erste AD-Version abrundeten und auftretende Unzulänglichkeiten verbesserten.

Eines der neuen Features in Windows Server 2003 ist das Umbenennen von Domänen. Mit dem Werkzeug "Rendom" (für "REName DOMain") können Administratoren Domänen und ganze Gesamtstrukturen umbenennen und umstrukturieren. Mit dem Werkzeug taufen Sie Domänen um, verschieben Subdomänen innerhalb des Domänenbaumes oder hängen diese sogar als neuen Domänenbaum innerhalb der Gesamtstruktur an.

Ebenfalls begrüßt wurde die Möglichkeit, Gesamtstrukturvertrauensstellungen zu erstellen. Der Zugriff auf Ressourcen und Authentifizierungen zwischen AD-Forests wird mit Hilfe von Trusts erreicht. Gesamtstrukturen vertrauen sich hierbei und gewähren sich Möglichkeiten des Zugriffs und der Authentifizierung.

Wer eine große Active Directory-Umgebung mit Windows 2000-Domänencontrollern betreute, wird die beschränkende Empfehlung von maximal 5.000 Mitgliedern pro Active Directory-Gruppe kennen. Die Empfehlung beruhte auf der Anzahl der möglichen Änderungen an der AD-Datenbank während einer Transaktion und der daraus resultierenden Replikation. Windows Server 2003-Domänencontroller und der zugehörige Gesamtstrukturfunktionsmodus heben die Beschränkung durch die sogenannte "Linked Value Replication" auf.

Windows Server 2003 R2

Mit ADAM, dem Active Directory Application Mode (später Active Directory Lightweight Directory Services, AD LDS) in Windows Server 2003 R2 machte Microsoft das AD entwicklerfreundlich. ADAM ist ein kleines Active Directory – ein leichter Verzeichnisdienst, der sich als Dienst auf beliebigen Servern installieren und ausführen lässt.

Der Dienst beinhaltet dabei die Grundfunktionalität des Active Directory: ein Schema, Sicherheitsprinzipale, Organisationseinheiten und Objekte. Um Objekte aus und mit den Active Directory Domain Services replizieren zu können, bietet ADAM die Option, entsprechende Schemadefinitionen während des Setups zu installieren. Die Realisierung von Applikationen wie unternehmensweite Telefon- oder Branchenlisten ist somit ohne das AD möglich. Die Replikation zwischen ADAM und Active Directory und damit identische Objektdefinitionen in den Schemata sind die einzigen Voraussetzungen für dieses Vorhaben.

Eine weitere Verbesserung in Windows Server 2003 R2 ist die Replikation von

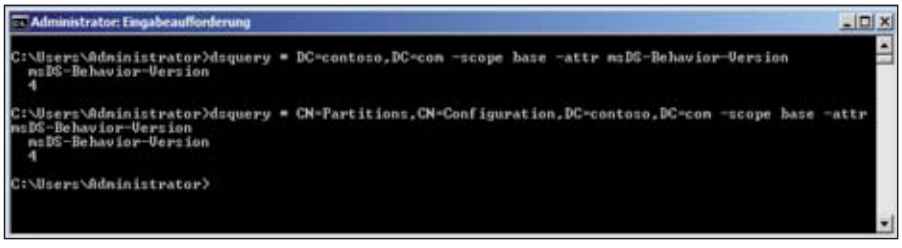


Bild 2: Funktionsmodi lassen sich am schnellsten über die Kommandozeile feststellen

DFS-Namensräumen. Bis dahin genutzte Freigaben in DFS repliziert Windows Server mit dem File Replication Service. Ein Nachteil von FRS ist die Replikation großer Daten, auch wenn sich nur Bruchteile davon änderten. DFS-R löst FRS für die Replikation für DFS-Namensräume ab und macht damit das Replikationsproblem großer Dateien mit Hilfe einer Delta-Übertragung hinfällig.

Windows Server 2008

Mit Windows Server 2008 verbesserte Microsoft das Active Directory erneut. Eines der bekanntesten neuen Features ist der Read Only-Domaincontroller (RODC). RODCs werden in standort- sowie sicherheitstechnisch schwierigen Niederlassungen eingesetzt. Der RODC ist keine Reinkarnation des Backup-Domänencontrollers aus Windows NT-Zeiten, sondern die Antwort auf komplexe Einsatzsituationen.

Sie können beispielsweise in nicht umfassend gesicherten Netzen wie etwa demilitarisierten Zonen oder Zweigstellen implementiert werden, in denen Verzeichnisdaten als potentiell unsicher eingestuft werden. Der Diebstahl eines RODC oder seine feindliche Übernahme bergen nur begrenzt Gefahr: Kennworte und andere Geheimnisse werden nicht offline geändert und zurück ins Verzeichnis gespielt, da RODCs – nur mit einer Lesekopie des Verzeichnisses ausgestattet – keine Änderungen an andere Domänencontroller replizieren. Zudem besitzt "Active Directory-Benutzer und -Computer" in Server 2008 Funktionen, die ein schnelles Exportieren der auf dem RODC angemeldeten Benutzer und Computer und dem Zurücksetzen ihrer Passworte ermöglichen.

Um das Wiederherstellen von zuvor gesicherten Verzeichniszuständen zu erleichtern, hat Microsoft einen zusätzlichen Kontext in das NTDSUtil-Werkzeug eingefügt. Mit dem "snapshots"-Kontext können Admins Schnappschüsse vom Verzeichnis erstellen und abspeichern, die später Einblicke in vergangene Zustände des Verzeichnisses geben. Diese Schnappschüsse werden verwendet, um etwa Vorher-Nachher-Vergleiche oder Untersuchungen zu veränderten Objekten anzustellen. Einblicke gewährt das mitgelieferte "Active Directory database mounting tool", das neben Schnappschüssen auch Active Directory-Backups im laufenden Domänencontrollerbetrieb als neue Instanz unter einem angegebenen Port startet. Die neue Instanz kann anschließend mit bekannten Snap-Ins wie "Active Directory-Benutzer und -Computer" lesend geöffnet und durchsucht werden. Hilfreich ist diese Funktion, wenn mehrere Backups für das Wiederherstellen eines gelöschten Objektes in Frage kommen, so dass Administratoren nicht alle möglichen Kandidaten zurückspielen müssen, um letztlich das korrekte Backup zu finden. Zudem erweist sich ein Direktvergleich mehrerer AD-Versionen bei der Wiederherstellung von Gruppenmitgliedschaften als äußerst handlich.

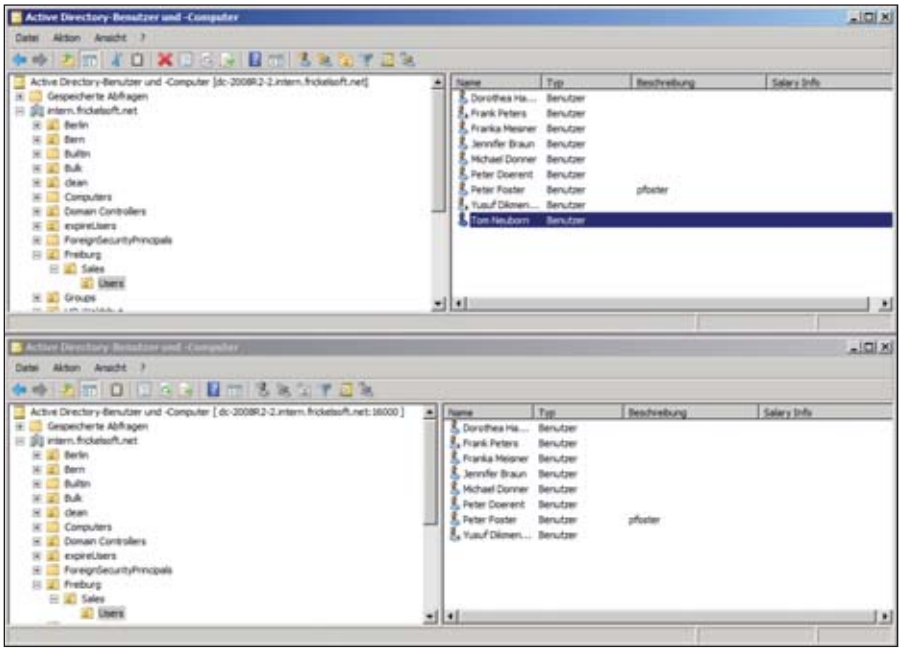


Bild 3: Mit *dsamain.exe* lässt sich ein Backup ins System einbinden und zum Vergleich mit dem Live-System nutzen

Die Beschränkung, nur eine Passwortrichtlinie pro Domäne und damit nur eine domänenweite Definition von maximalem Kennwortalter, Passwortkomplexität und Kennwortmindestalter definieren zu dürfen, hebt Windows Server 2008 auf. Mit dem Domänenfunktionsmodus "Windows Server 2008" können Sie "Password Setting Objects" erstellen und sie Benutzern, globalen Gruppen oder iNetOrgPerson-Objekten der Domäne zuweisen. Passwortrichtlinien für Außendienstmitarbeiter, Telefonsupport und die Geschäftsleitung mit unterschiedlichen Einstellungen sind somit gänzlich ohne Drittanbieterprogramme durchsetzbar.

Windows Server 2008 R2

Eines der Highlight-Features der neuesten Windows Server-Iteration ist zweifelsfrei der Active Directory-Papierkorb. Nach expliziter Aktivierung über die Powershell ist es möglich, gelöschte AD-Objekte verlustfrei wiederherzustellen – ganz ohne Backup und Drittanbietertools. Ohne Papierkorb befreit das AD zu löschende Objekte von einem Großteil ihrer Attribute und verschiebt sie in den "Deleted Objects"-Container. Die Wiederherstellung ist nur mit Hilfe eines authoritative Restores oder mit Drittanbietertools sinnvoll, denn Benutzerobjekte ohne Namen, Telefonnummer, Adresse oder Gruppenmitgliedschaften

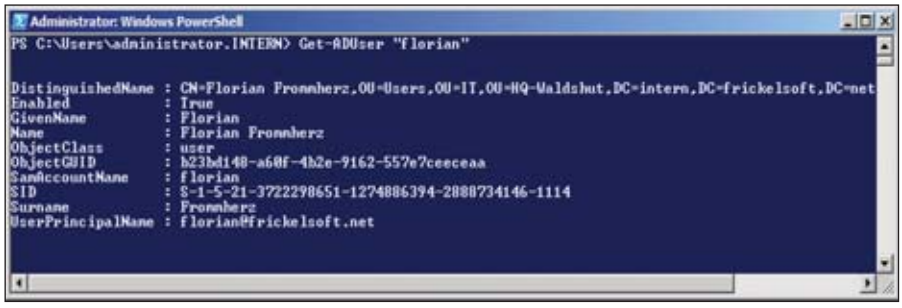


Bild 4: Mit Windows Server 2008 R2 führt Microsoft eigene Active Directory-Cmdlets für die PowerShell ein, die das Administratorleben vereinfachen

sind nahezu nutzlos. Der AD-Papierkorb macht es nun anders: Einmal aktiviert, verschiebt das AD zu löschende Objekte weiterhin in den "Deleted Objects"-Container, leert aber keines der Attribute. Das Wiederherstellen der Objekte ohne Drittanbietertools oder der Neustart in den Verzeichnisdienstwiederherstellungsmodus ist somit spielend leicht möglich und zugleich viel schneller. Es genügt ein Verschieben des Objektes an seinen ursprünglichen Ort und das Entfernen des Löschkennzeichens.

Serveradministratoren können, nachdem sie die Schemaaktualisierungen für Windows Server 2008 R2 eingespielt haben, gespannt in die Zukunft blicken. Ein bekanntes und ebenso unbeliebtes Problem lässt sich mit dem neuen Windows-Betriebssystem lösen: die Erstellung und Pflege von Dienstkonten für Windows-Dienste und -Anwendungen auf Servern. Bisher wurden Dienstkonten entweder manuell oder per Skript administriert.

Mit "Managed Service Accounts" (MSA) dürfen Administratoren Dienstkonten anlegen, die sich selbst verwalten. Die Active Directory-Passworte der Konten wechseln automatisch. Zusätzlich sorgt die Lösung dafür, dass Clients Dienste im Netzwerk finden können: Die Erstellung und Registrierung der Service Principle Names (SPNs) übernehmen MSAs gleich mit. Da MSAs vollständig mit der Powershell erstellt und verwaltet werden, ist ein skriptgesteuertes Anlegen von Dienstkonten, etwa bei der Serverinstallation, kein Problem.

Wer die Entwicklung der meisten Serverprodukte aus Redmond verfolgt hat, wird keinen Zweifel daran haben, dass die PowerShell das Verwaltungswerkzeug der Zukunft sein wird. In der neuesten Windows Server-Version liefert Microsoft eigene CMDlets für die PowerShell mit, so dass das Administrieren des Active Directory überwiegend ohne Zutun von Drittanbietern klappt. Die nun in der PowerShell von Windows Server 2008 R2 eingepflegten CMDlets decken alle gängigen Wartungs- und Administrationsaufgaben ab.

Ein Beweis dafür, dass die PowerShell immer weiter Einzug in neue Versionen jeglicher Produkte aus Redmond einhält, ist die neue "Active Directory Verwaltungskonsole". Sie basiert vollständig auf den Active Directory-Cmdlets und soll in späteren Versionen das bekannte "Active Directory-Benutzer und -Computer" MMC-Snap-In ablösen. Die neue Konsole ist eine grafische Oberfläche für Managementzwecke, die einen Teil der AD-Powershell-Cmdlets abdeckt. Den vollständigen Funktionsumfang erreichen Sie aber nur über die PowerShell.

Das Hauptaugenmerk der Verwaltungskonsole sind administrative Workflows und anfallende Wartungsarbeiten, die Administratoren und Help Desk-Mitarbeiter erledigen müssen. Dabei bietet die Konsole nicht nur Ansichten zu Objekten, sondern lässt den Bediener häufige Aufgaben und Probleme lösen, ohne Kontextmenüs zu gebrauchen. Die Erstellung und Verwaltung von Benutzerkonten vereinfacht die neue Oberfläche, indem viele häufig verwendete Attribute und Eigenschaften auf einer Übersichtsseite während der Erstellung anwählbar sind. Neu sind weiterhin die Filteroptionen, die Objekte anhand vorgegebener Kriterien oder selbstgewählter Kriterien suchen. Das Filtern und Suchen gelingt dabei sowohl Domänen- als auch OU-weit. *(jp)*

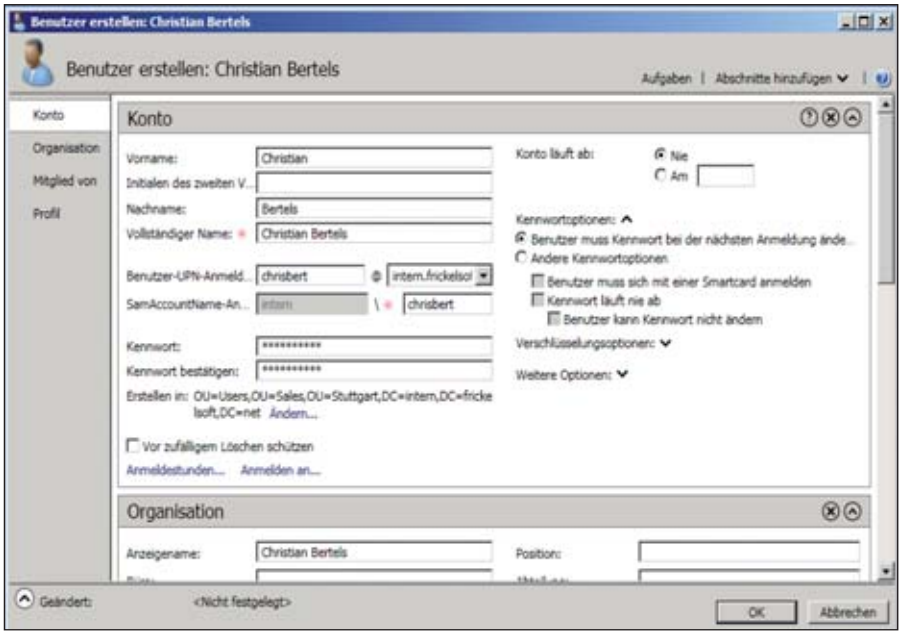


Bild 5: Die Active Directory-Verwaltungskonsole hilft durch ihren Aufbau, Verwaltungsaufgaben leichter zu erledigen

Funktionen der Active Directory-Versionen

Betriebs-system	Feature	Beschreibung	Voraussetzungen
Windows Server 2003	Umleitung der Container "Users" und "Computers"	Neu generierte Benutzer und Computer können bei ihrer Erstellung mit den Kommandozeilenprogrammen "redirusr" und "redircmp" in andere Container oder Organisationseinheiten umgeleitet werden.	DFL 2003
	Umbenennung der Domäne	Das Ändern des Domänennamen im Active Directory wird nun unterstützt.	FFL 2003
	Vertrauensstellungen zwischen Forests	Zwei Forests können mit Hilfe der Gesamtstrukturvertrauensstellung miteinander verbunden werden, um Authentifizierung und Zugriff auf Ressourcen zu ermöglichen.	FFL 2003
	Erstellen von Anwendungspartitionen	Zusätzlich zu den Standard-Partitionen der Domäne, der Konfiguration und des Schemas können weitere Partitionen für Anwendungen erstellt werden. Die Anwendungspartitionen können Daten und Konfigurationen enthalten und zwischen Domänencontrollern repliziert werden.	FFL 2003
	Linked Value Replication (LVR)	Verknüpfte Attribute werden bis zum Erlangen des "Server 2003"-Gesamtstrukturfunktionslevels stets komplett zwischen Domänencontrollern repliziert. Mit dem "Server 2008"-Funktionslevel werden nun einzelne Verknüpfungen in den Attributen repliziert. Dies löst die bisher bestehende 5.000-Verknüpfungen-Grenze auf.	FFL 2003
	Universal Group Caching	Der Authentifizierungsprozess bei Mitgliedern universeller Gruppen erfordert einen Globalen Katalog, um alle Gruppenmitgliedschaften evaluieren zu können – sonst scheitert der Logon-Versuch. Mit "Universal Group Caching" speichern Domänencontroller die Mitgliedschaften von bereits einmal angemeldeten Benutzern.	FFL 2003
	AD Quotas	AD-Quotas schränken die Erstellung von Active Directory-Objekten ein, indem Sicherheitsprinzipale nur eine vorgegebene Anzahl von Objekten pro Namenskontext erstellen dürfen.	FFL 2003
Windows Server 2003 R2	ADFS	Active Directory Federation Services (ADFS) stellt eine Single Sign-On-Lösung für Webzugriffe dar, mit der domänenfremde Benutzer anhand von Merkmalen authentifiziert werden können.	Server mit Server 2003 R2
	ADAM	Active Directory Application Mode (ADAM) ist ein schlankes Active Directory für Entwickler, das als Verzeichnis für Anwendungen verwendet wird.	Server mit Server 2003 R2
	DFS-R	DFS-R löst FRS als Replikationsdienst für DFS-Namensräume ab und verbessert die Replikation großer Datenmengen zwischen DFS-Knoten.	2003 R2 Schema-Extension und Server 2003 R2
Windows Server 2008	AD Snapshots	Per NTDSUtil lassen sich Momentaufnahmen des Active Directory erstellen und archivieren. Es können mehrere Schnapschüsse in ein laufendes System eingebunden werden, so dass ein Vergleich zwischen mehreren Schnappschüssen und dem aktuellen Verzeichnis möglich ist.	DC mit Server 2008
	Fine-Grained Password Policies	Mit dem Domänenfunktionsmodus "Server 2008" können nun mehrere Passwortrichtlinien innerhalb einer Domäne erstellt werden. Die sogenannten "Fine-Grained Password Policies" bestimmen Passwortoptionen von Benutzer-, globalen Gruppen- und iNetOrgPerson-Objekten.	DFL 2008
	Read-Only Domain Controllers	Für Standorte und Netze mit unzureichender Sicherheit werden Nur-Lese-Domänencontroller eingeführt. Sie können in Umkreisnetzwerken oder Standorten mit wenig Personal und geringen Sicherheitsvorkehrungen platziert werden. Auf RODCs kann nicht schreibend zugegriffen werden. Windows Server 2008 beinhaltet außerdem Funktionen, die ein schnelles Passwortzurücksetzen für "gestohlene" Objekte forcieren.	Ein Server 2008-DC im Hauptstandort, *Adprep* mit dem Schalter /rodcprep wurde ausgeführt
	Restartable DS	Das Active Directory kann, wie andere Dienste, gestartet und gestoppt werden. Einige Verwaltungsaufgaben lassen sich so ohne Neustart in den "Directory Services Restore Mode" erledigen.	Nur auf Domänencontrollern mit mindestens Windows Server 2008
	Neuerungen in der AD-Protokollierung	Microsoft stellt weitere, granularere Protokollierungen für das Active Directory zur Verfügung. Mit Hilfe von *auditpol.exe* lassen sich Ereignisse auf Domänencontrollern und im Verzeichnis gezielter mitschneiden.	DC mit Server 2008
	Neuerungen bei DCPromo	*Dcpromo.exe* auf Windows Server 2008 lässt den Benutzer auf einfache Art Antwortdateien exportieren und importieren, die eine Masseninstallation von Domänencontrollern vereinfachen. Ausserdem ist die Erstellung eines speziellen Mediums ohne Passwort-Geheimnissen möglich, um Read-Only Domänencontroller sicher erstellen zu können.	Server mit Server 2008
Windows Server 2008 R2	AD Recycle Bin	Der AD-Papierkorb löscht im aktivierten Zustand nicht mehr den Großteil der Attribute eines gelöschten Objektes sondern behält sie bei. Dies erleichtert das Wiederherstellen von versehentlich gelöschten Objekten.	FFL 2008 R2
	Managed Service Accounts	Neue Mitgliedsserver und Clients verfügen über die Möglichkeit, Dienstkonten in Active Directory gesichert verwalten zu lassen. Passworte der Dienstkonten werden in regelmäßigen Abständen automatisiert erneuert.	Windows 7 oder Windows Server 2008-Client (der den Dienst hostet), >= Windows Server 2003-Domänencontroller
	Backup&Restore	Die Ablösung von NTBackup durch eine imagebasierte Sicherungslösung bedingen das Umdenken und Neuevaluieren von Backups in Windows Server 2008 und Windows Server 2008 R2.	Server mit Server 2008 R2
	Offline der Domäne beitreten	Neue Clients können nun offline einer Domäne beitreten, indem die Computerkonten im Active Directory vorweg provisioniert werden. Ein bei der Provisionierung erzeugter Textschlüssel enthält alle Informationen, die ein Client beim Offline-Beitritt in die Domäne benötigt.	Windows 7 oder Windows Server 2008-Client
	Active Directory Administrative Center (ADAC)	Der Nachfolger von "Active Directory Users and Computers" basiert komplett auf PowerShell 2.0 und erleichtert mit vorgefertigten Suchfiltern administrative Aufgaben.	DC mit Windows Server 2008 R2
	PowerShell-Integration	Mit Server 2008 liefert Microsoft eine vollständige Integration der PowerShell für das Active Directory. Mit den vorliegenden CMDlets lassen sich nahezu alle Verwaltungsaufgaben per Skript lösen.	Windows Server 2008 R2

Virtualisierung von Windows-Domänencontrollern

Spiel mit dem Feuer


Quelle: Pixelio.de

Durch Virtualisierung ist der Administrator heutzutage unabhängiger von der Hardware, kann die Infrastruktur verfügbarer gestalten und ist für einen Recovery-Fall bestens gerüstet. Soll jedoch ein Windows-Domänencontroller virtuell betrieben werden, benötigt der Administrator tiefgehendes Know-how des Systems und des Active Directory. In diesem Workshop zeigen wir die spezifischen Probleme – etwa bei der Replikation oder der Netzwerkzeit – dieser Systeme auf und stellen Methoden vor, diese zu vermeiden.

Längst ist Virtualisierung nicht mehr nur ein Mittel, Produktivsysteme für Testzwecke nachzustellen oder neue Software vor dem Einsatz ausführlich auszuprobieren. Die Implementierung virtueller Maschinen und der Einsatz in produktiv genutzten Netzwerken gehört vielerorts bereits zum Alltag. Neben den Möglichkeiten, die Systeme zu konsolidieren, bietet die Virtualisierung noch einen sehr interessanten Nebeneffekt: Da die Hardware durch eine Virtualisierungsschicht abstrahiert ist, können virtuelle Gäste auf einem Virtualisierungshost heruntergefahren und auf einem neuen wieder gestartet werden. Virtualisierung auf VMware ESX oder Microsoft Hyper-V erlaubt sogar das Verschieben von virtuellen Systemen, fast ohne diese offline zu nehmen. Snapshot-Technologien speichern ein Abbild des Servers im laufenden Betrieb. Das Recovery besteht darin, die komplette virtuelle Festplatte zurückzusichern und dann das System sofort wieder zu starten. Dabei ist nicht viel mehr notwendig, als das entsprechende Computerkonto zurückzusetzen.

Geringe Last auf dem DC

Domänencontroller (DC) sind perfekte Kandidaten für die Servervirtualisierung. Der Normalbetrieb von Domänencontrollern erzeugt wenig Last auf den Prozessoren, ausgenommen sind Großunternehmen mit umfangreichen Verzeichnissen. Lediglich zyklische Dienste, die der Domänencontroller überwiegend mit der PDC-Emulator-FSMO-Rolle ausführt, benötigen mehr Rechenleistung. Der Bedarf an Leistung ist somit stark von der Benutzeranzahl und den allgemeinen Verzeichnisdienstanfragen abhängig. Anfragen auf Domänencontrollern sind absehbar und schwanken selten.

Die Allgemeinlast lässt sich jedoch indirekt durch die Verteilung der Dienste (DNS, DHCP) und die Anzahl der Domänencontroller steuern. Sind mehrere Domänencontroller verfügbar, teilen sie sich bei kluger Konfiguration Authentifizierungs- und DNS-Anfragen auf – es entsteht eine Lastenaufteilung. Der von DCs benötigte Arbeitsspeicher ist gut abschätzbar; neben dem Footprint des Betriebssystems muss Arbeitsspeicher für die Zwischenspeicherung des Verzeichnisses kalkuliert werden. Hier genügt in etwa die Größe der AD-Datenbank mit einem Zusatz für kommendes Wachstum. Obwohl Domänencontroller von Haus aus keine speicherhungrigen Dienste besitzen, sollten ihnen mindestens 2 GByte Arbeitsspeicher zur Verfügung stehen.

Um der "Best Practice"-Empfehlung gerecht zu werden, stets mindestens zwei Domänencontroller pro Domäne zu betreiben, setzen viele Administratoren auf Domänencontroller als VMs. Die DCs sind dabei schnell installiert und dank der zuverlässigen Replikation ist das Vorhaben schnell umgesetzt. Bei Domänencontrollern handelt es sich allerdings nicht einfach um Server, die einen Dienst tun. Sie sollten daher einige Besonderheiten beachten.

Problembereiche der Virtualisierung eines Dömenencontrollers

Domänencontroller stellen den zentralen Knoten der Infrastruktur dar: Sie übernehmen einerseits die Authentifikation von Benutzern, Computern und Diensten und beherbergen andererseits unternehmenskritische Daten wie E-Mailadressen oder Mitarbeiterinformationen. Den oder die Domänencontroller und damit ihre Domänendienste zu verlieren, ist tragisch und trifft Unternehmen härter als der Verlust anderer Dienste. Sind die Domänendienste nicht mehr verfügbar, scheitern nahezu alle Dienste, die auf Domänencontroller angewiesen sind oder die Authentifizierung von Benutzern bedingen: Exchange liefert keine Nachrichten mehr aus, Benutzer können sich nicht mehr an der Domäne authentifizieren und der Zugriff auf Dateiserver ist nicht gestattet.

Replikationsmechanismen beachten

Vor den genannten Szenarien schützen virtuelle DCs nur indirekt. Zwar erlauben Virtualisierungstechniken, einfacher und kostengünstiger Domänencontroller zu erstellen, doch bergen virtuelle DCs besondere Schwierigkeiten, die es vorab bewusst zu evaluieren gilt. Legen Administratoren DCs auf wenigen oder gar einem einzigen Host ab, besteht die Möglichkeit eines Single Point of Failures (SPOF). Gehostete Domänencontroller sind aus diesem Grund direkt vom Host abhängig und bei einem Ausfall der Virtualisierungslösung nicht mehr erreichbar.

Um sich vor einem SPOF zu schützen und bei möglichen Problemen mit dem Host unabhängig zu bleiben, sollten Sie virtualisierte Domänencontroller auf mehrere Hosts verteilen. Hierbei ist auch zu beachten, dass eine "Replikation" eines virtuellen Hosts nicht ausreichen muss: Viele Unternehmen haben virtuelle Hosts im Einsatz, deren Gastsysteme in einem SAN gespeichert werden, das in ein anderes Rechenzentrum repliziert wird und im Fehlerfall von dort wieder gestartet werden kann. Es ist jedoch auch schon vorgekommen, dass Fehler zwischen den SANs noch repliziert wurden und sich die Maschinen auf der anderen Seite auch nicht mehr starten ließen. Auch ein repliziertes SAN kann einen SPOF darstellen. Daher ist es wichtig, nicht nur eine Virtualisierungsinfrastruktur zu betreiben, sondern auch eine zweite, auf der die wichtigen Dienste repliziert werden. Steht nur eine Virtualisierungsinfrastruktur zur Verfügung, sollten Sie in Erwägung ziehen, nicht alle Domänencontroller zu virtualisieren und einen Teil als physische Server bestehen zu lassen.

Zu prüfen gilt außerdem, ob der virtuelle Host Mitglied der Domäne wird oder als Standalone-Server fungiert. Bei der Aufnahme in die Domäne kann ein Henne-Ei-Problem entstehen, falls sämtliche Domänencontroller als Gäste in VMs auf dem Host laufen. Wo soll sich der VM-Host anmelden, wenn sämtliche DCs noch nicht verfügbar sind? Das Gleiche gilt auch für die Backup-Server: Hier müssen Sie darauf achten, dass diese bei einem Gesamtausfall unabhängig von der Domäne die Wiederherstellung ermöglichen.

Zeitmanagement für Domänencontroller

Ein verbreitetes Problem während der Erstellung von virtuellen DCs oder des Umzugs von DCs in eine virtuelle Umgebung stellt die Uhrzeit dar. In einer Windows-Infrastruktur muss die Zeit stimmen, da das Authentifizierungsprotokoll Kerberos auf eine angeglichene Zeit besteht. Weicht die lokale Zeit der DCs mehr als die standardmäßig eingestellten fünf Minuten ab, verweigert Kerberos die Authentifizierung. Die Folge ist der Ausfall von Anmeldungen und der Stopp der Replikation zu diesem DC. Mitglieder der Domäne nutzen standardmäßig ihre Domänencontroller als Zeitgeber.

Driftet ihre Zeit ab, korrigieren diese Clients diese automatisch und passen sie der Vorgabe der Domänencontroller an. DCs untereinander synchronisieren ihre Zeit mit dem DC, der die PDC-Emulator-FSMO-Rolle ausübt. Existiert eine Mehr-Domänen-Gesamtstruktur, synchronisieren die PDC-Emulator-Besitzer ihre Zeit wiederum mit dem PDC-Emulator der Gesamtstruktur-Wurzeldomäne. Der für die Zeit verantwortliche Domänencontroller muss stets so konfiguriert sein, dass er eine verlässliche Zeitquelle kontaktieren kann, um anschließend die korrekte Zeit auf alle Systeme der Domäne zu propagieren. Ob diese Zeitquelle eine hardwarebasierte Lösung oder ein entfernter Zeitserver im Internet ist, spielt hierbei keine Rolle.

Das Problem "Zeit" beginnt mit einem Feature vieler Virtualisierungslösungen, das die Uhrzeit einer VM über den Host abgleicht. Der Host sorgt in regelmäßigen Abständen dafür, dass die Zeit seiner VMs mit der Hostzeit übereinstimmt. Es wird aktiv in die Zeit der Clients, also auch in die VM selbst, eingegriffen. Setzt der Administrator die Zeit manuell in der VM, überschreibt der Host sie kurzerhand, um die Zeitdiskrepanz zu minimieren. Das Feature kann zu Problemen führen, wenn die Zeit des Hosts von der Zeit der Domäne abweicht. Der eigentliche Mechanismus, die Zeit per Domäne zu propagieren, wird schließlich aktiv verletzt und kann für Inkonsistenzen sorgen. Wir empfehlen daher, die Zeitsynchronisation zwischen VM und Host abzuschalten. Eine weniger drastische Möglichkeit besteht darin, den Host, ob Domänenmitglied oder nicht, so zu konfigurieren, dass auch er einen Domänencontroller als Zeitquelle benutzt oder die Zeit vom gleichen Zeitserver bezieht wie der PDC der Rootdomäne.

Sicherheit durch Aufgabentrennung

Auch in Fragen der Sicherheit gibt es einige beachtenswerte Besonderheiten bei virtuellen Domänencontrollern. Oft werden mehrere unterschiedliche virtuelle Maschinen auf einem Host betrieben und von unterschiedlichen administrativen Gruppen im Unternehmen betreut. Teilweise kommt es sogar vor, dass diejenigen Mitarbeiter der IT, die für die Virtualisierung verantwortlich sind, nicht die gleichen Personen sind, die das Active Directory verwalten. Daher müssen Sie sich Gedanken um den Schutz der virtuellen Maschinen machen. Nicht jeder Daten-Admin, der seine virtuellen Fileserver administrieren will, soll Zugriff auf die DC-VM besitzen – oder sie gar umkonfigurieren können, um ihr Ressourcen zu stehlen.

Das gilt nicht nur für die virtuellen Maschinen, sondern auch für die Sicherung ihrer virtuellen Festplatten. Ihr Diebstahl lässt sich mit dem Raub eines Domänencontrollers vergleichen. Schlimmer noch: Ein gestohlener Domänencontroller fällt im Serverraum schnell auf, die unbemerkte Kopie einer virtuellen Festplatte ist jedoch nicht so leicht zu entdecken. Angreifer können eine Kopie der virtuellen Maschine anfertigen und sie dann zur Kompromittierung der Infra-

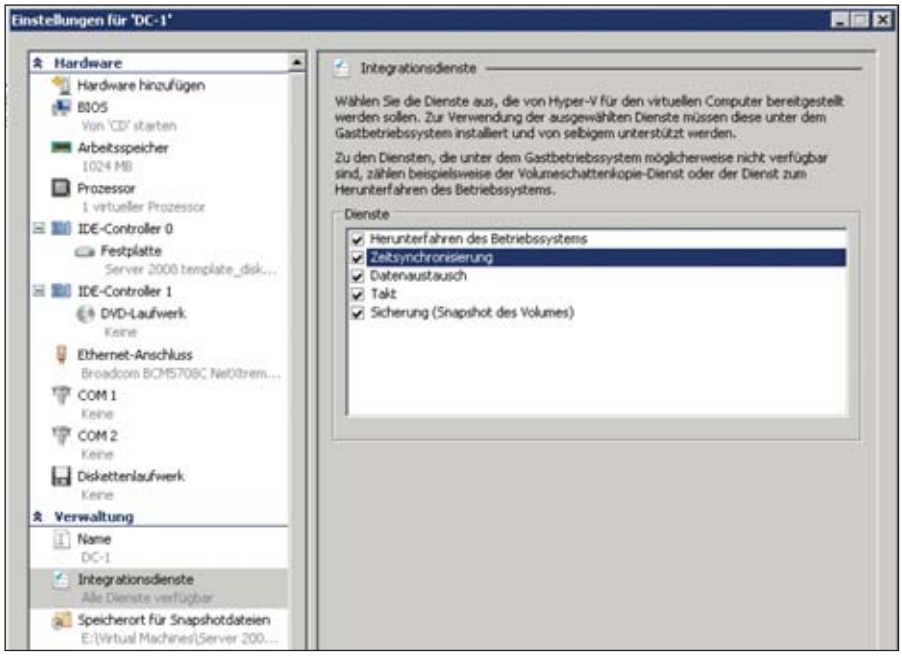


Bild 1: In den meisten Virtualisierungslösungen (hier Hyper-V) lässt sich die Zeitsynchronisation zwischen Host und VM steuern

struktur verwenden. Unternehmen sollten daher die strenge Trennung der Administration beteiligter Dienste erzwingen: Service-Administratoren dürfen sich nur auf die virtuellen Maschinen ihrer Dienste verbinden, Virtualisierungs-Administratoren kümmern sich um die Konfiguration und den Betrieb der VM-Hosts sowie deren Hardware, während das Storage-Team den Zugriff sichert und den Betrieb der Speicherlösung mit den darauf betriebenen VHDs. In überschaubaren Umgebungen reicht es, den Zugriff auf den VM-Host und die Administrationsdienste abzuschotten und sie nur ausgewähltem Personal zugänglich zu machen.

Virtuelle DCs richtig sichern

Sind die virtuellen DCs ausgerollt, wird es höchste Zeit, sich um die Wartung zu kümmern. Ein Punkt, der bei virtuellen sowie physischen Domänencontrollern gleichermaßen wichtig ist, sind Sicherungen. Virtuelle Domänencontroller in Produktivumgebungen müssen Sie stets genauso sichern wie physische Domänencontroller. Eine korrekte Sicherung ist notwendig, um das Active Directory im Falle einer Wiederherstellung in einem konsistenten Zustand zu behalten. Dabei ist es aber beim Active Directory nicht zwingend notwendig, dass jeder Domänencontroller gesichert ist. Wichtig ist, dass Sie genügend Domänencontroller jeder Domäne sichern, um in jedem Fall eine Sicherung vorrätig zu haben, von der Sie die Domäne wieder aufbauen können (oder einzelne Objekte wieder zurücksichern können). Empfehlenswert ist es auf alle Fälle, mindestens zwei nicht-FSMO-Rolleninhaber pro Domäne zu sichern und regelmäßig zu überprüfen, ob die Sicherung auch funktioniert und Sie auf die Daten zugreifen können. Andere Domänencontroller würden Sie dann durch eine Neuinstallation (oder erneutes DCPromo) zu einem DC heraufstufen, sobald ein oder zwei DCs wieder laufen. Manche Unternehmen bevorzugen es, jeden DC zu sichern und im Fehlerfall lieber mit einer Rücksicherung zu arbeiten, als das System neu zu installieren. Welchen Weg Sie wählen, ist Geschmackssache und hängt auch von den weiteren Diensten ab, die auf dem Domänencontroller laufen.

Obwohl die Replikation zwischen Domänencontrollern nahezu automatisch und sehr robust verläuft, reagiert sie auf inkonsistente Daten zwischen den DCs sehr sensibel. Microsoft liefert mit seinem Betriebssystem stets ein eigenes Sicherungswerkzeug, das Windows-Backups erstellen und zurückspielen kann. Bis Windows XP und Windows Server 2003 übernahm NTBackup diese Aufgabe, unter Windows Vista und Server 2008 dann Windows Backup. Die beiden Sicherungswerkzeuge unterscheiden sich in ihrer Grundfunktionalität dadurch, dass NTBackup dateibasierte, Windows Backup hingegen block- und imagebasierte Sicherungen des Systems erstellt. Für die Sicherung des Verzeichnisses wird der "Systemstatus" (englisch System State) benötigt, der neben systemkritischen Komponenten wie Start-, Registrierungs- und Komponentendienstdaten auch die Active Directory-Datenbank beinhaltet.

Ein Backup des Systemstatus reicht jedoch nicht aus, sondern Sie müssen auch weitere Inhalte sichern, um eine Rücksicherung praktikabel zu halten. Mehr zu diesem Thema finden Sie in den Workshops zum Directory Services Restore Mode, zum Windows Backup, zur Sicherung des Active Directory sowie zur Wiederherstellung des Active Directory. Für Virtualisierungs-Infrastrukturen sind umfassendere Lösungen mittlerweile in der Lage, die virtuelle Umgebung mitsamt ihrer virtuellen Maschinen zu sichern. Mi-

Checkliste zum Einsatz von virtuellen Domänencontrollern

- Vermeiden Sie die Möglichkeit eines Single Point-of Failure.
- Zeitdienst: Entweder konfigurieren Sie für den Virtualisierungshost (für jeden, wenn es mehrere gibt) den gleichen NTP-Server oder Sie schalten die Zeitsynchronisation aus.
- Stellen Sie sicher, dass nur die gewünschten Administratoren Zugriff auf die DCs und deren Daten haben.
- Vermeiden Sie Snapshots, zum Beispiel über direkte Datenträger.
- Partitionierung: Soll die AD-Datenbank auf eine eigene Partition? Sollen "lokale" NTBackup- oder Windows-Backups erstellt werden?

crosoft Data Protection Manager (DPM) kann mit Hilfe des Volume Shadow Copy Service (VSS) virtuelle Maschinen während des laufenden Betriebes sichern – zum Beispiel alle 15 Minuten – und kümmert sich dabei um die besonderen Bedürfnisse von SQL Server-Datenbanken oder Exchange-Servern.

Als nicht unterstützte Backup-Varianten, die das Active Directory, aber auch andere datenbankbasierte Dienste wie Exchange oder SQL in einen korrupten Zustand bringen können, gelten Funktionen wie imagebasierte Sicherungen oder Snapshots der Festplatten beziehungsweise "Undo disks". Während Snapshots bei der Erstellung und dem Betrieb von Testumgebungen ein nutzvolles Feature für den Rücksprung zu einem älteren Betriebszustand sind, können sie für das Active Directory fatale Folgen haben: das Entstehen von sogenannten "lingering objects". Dies sind "übriggebliebene Objekte", die nicht zwischen DCs repliziert werden. Die Folge sind inkonsistente Objektbestände im Verzeichnis, die zwischen Domänencontrollern variieren.

USN-Rollbacks vermeiden

Damit unterschiedliche Domänencontroller feststellen können, welche Änderungen sie von anderen Domänencontrollern replizieren müssen, kommen sogenannte "Update Sequence Numbers" (USN) zum Einsatz. Diese werden bei jeder Änderung, die ein Domänencontroller in sein lokales Active Directory schreibt, erhöht. Die USN ist also lokal an jedem Domänencontroller unterschiedlich.

Wenn ein DC repliziert, merkt er sich die zuletzt replizierte USN seines Replikationspartners (im sogenannten High Watermark Table). Bei dem nächsten Replikationszyklus fragt der Domänencontroller dann seinen Replikationspartner nach allen Änderungen, die nach derjenigen USN erfolgt sind, die er zuletzt repliziert hatte. Erhält er nun diese Änderungen, prüft der DC anhand einer Versionsnummer und gegebenfalls des Zeitstempels (AD erlaubt ja auch Änderungen auf verschiedenen DCs, wobei unter Umständen Konflikte entstehen), ob er die Änderung annimmt und schreibt diese in seine Datenbank. Dabei erzeugt er eine eigene, lokale USN, die wiederrum seinen Replikationspartnern hilft, die letzten Änderungen anzufordern.

Das Zurücksichern von Domänencontrollern mit nicht unterstützten Methoden wie Imagebackups oder Snapshots führt genau an dieser Stelle zu massiven Problemen. Anhand eines Beispiels wird die Problematik deutlich: DC-A und DC-B sind in der gleichen Domäne und replizieren deren Inhalte. Der USN-Stand der letzten Änderung liegt für DC-A bei 1734, für DC-B bei 975. Die beiden Domänencontroller kennen ihren jeweilig eigenen Stand sowie den USN-Stand des Partners: DC-A {1734, 975}, DC-B {975, 1734}. Der aktuelle Stand des Betriebssystems und aller Daten auf DC-A wird mit einem Image oder Snapshot der Festplatte festgehalten. In den folgenden Tagen nimmt ein Administrator mehrere Änderungen an der von DC-A und DC-B geteilten Partition vor, so dass mehrere Erhöhungen der USNs auf beiden Domänencontrollern und daraus resultierend mehrere Replikationsvorgänge stattfinden. Die aktuellen USN-Stände sind nun DC-A {1809, 992}, DC-B {992, 1809}. Aufgrund eines Defektes fährt das AD-Team DC-A herunter, tauscht die Hardware aus und setzt ihn mit dem festgehaltenen Image neu auf (oder schlimmer, jemand hat eine Änderung gemacht und will sie über einen Snapshot wieder rückgängig machen). Die beiden DCs haben nun folgende USN-Stände: DC-A {1734, 975} und DC-B {992, 1809}. DC-A besitzt offensichtlich den per Image gesicherten, alten Stand seines High Watermark Tables sowie der lokalen USNs. Dies ist der Zeitpunkt des sogenannten "USN-Rollback". Die zuvor unter den DCs bekannte USN von DC-A wurde durch eine nicht supportete Backuplösung wiederhergestellt – und die USN illegal auf einen alten Stand zurückgerollt. Änderungen an der Partition führen zur Erhöhung der USN auf DC-A.

Wenn jetzt DC-B bei der nächsten Replikation nach den Änderungen fragt, möchte er alle Änderungen seit USN 1809 von DC-A. Da dieser aber erst bei USN 1734 ist, gibt es keine Änderungen zu replizieren. DC-B wird somit die vorgenommenen Anpassungen von DC-A nicht aktualisieren, so dass sich das Verzeichnis in einem inkonsistenten Zustand befindet. DCs sind per Voreinstellung so konfiguriert, dass sie die Durchführung der Replikation mit potentiellen Opfern von USN-Rollbacks verweigern. Wäre dies nicht der Fall, würde DC-A verschiedene Änderungen schreiben, bis er den Stand erreicht, den DC-B erwartet, um wieder zu replizieren. DC-A hat hiermit Änderungen den anderen DCs vorenthalten, nähme aber dann plötzlich wieder an der Replikation für weitere Objekte teil. Daher ist es wichtig, dass die Replikation ausgesetzt ist, bis ein Administrator den Fehler behoben hat.

Eine weitere Folge ist eine Meldung in der Ereignisanzeige des Quelldomänencontrollers mit der ID 2095 und dem Typ "NTDS Replication". Je schneller USN-

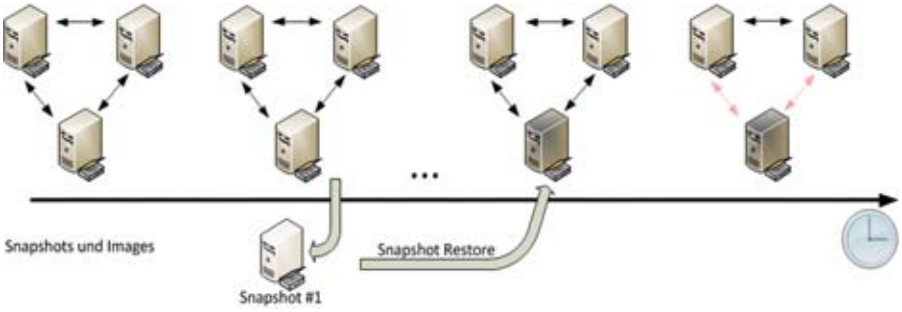


Bild 2: Schema einer möglichen Ursache eines USN-Rollbacks

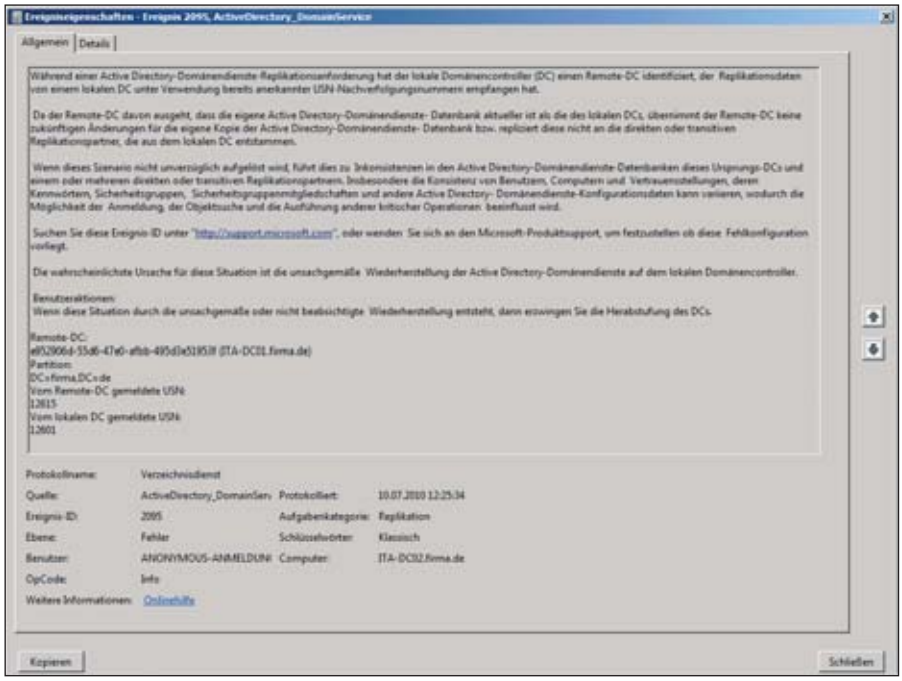


Bild 3: Das Event 2095 zeigt an, dass ein USN-Rollback stattgefunden hat, weil ein Domänencontroller unsachgemäß rückgesichert wurde. Jetzt hilft nur noch ein Herabstufen und Re-Promoten des DCs.

Rollbacks erkannt werden, desto einfacher ist es, inkonsistente "lingering objects", die nicht repliziert werden, zu minimieren und beheben.

Das Zurückspielen von Images ist nicht die einzige Methode, sein Verzeichnis mit einem USN-Rollback in Gefahr zu bringen. Virtualisierungstechnologien wie das Erstellen und spätere Zurückrollen von Snapshots sind eine ähnlich sichere Methode, das Active Directory aus dem Tritt zu bringen. Verwirft ein Administrator den aktuellen Stand des Domänencontrollers und reaktiviert einen veralteten Stand, ist der alte USN-Stand des DCs wieder aktiv.

Ebenfalls mit Vorsicht zu genießen sind Undo-Disks für virtuelle Maschinen. Undo-Disks finden Verwendung, wenn Daten von virtuellen Festplatten ab einem gewünschten Zeitpunkt in eine gesonderte virtuelle Festplatte geschrieben werden sollen. Das ermöglicht Administratoren ebenso die Möglichkeit, zu einem früheren Datenzustand zurückzuspringen. Images, Snapshots und Undo-Disks sollten nur dann eingesetzt werden, wenn der Forest aus einer Domäne mit nur einem Domänencontroller besteht. Da dies, wenn sich Administratoren an Best Practices halten, nur selten auftritt, ist auch die Verwendung solcher Sicherungen nicht notwendig.

Der Schlüssel für eine sichere, virtuelle Infrastruktur für Domänencontroller liegt darin, diese Technologien auszuschließen oder sicherzustellen, dass nur Administratoren entsprechende Möglichkeiten haben, denen das Problem bekannt ist. Ein häufig genannter Weg, um Snapshots zu vermeiden, ist es, sogenannte "linked Volumes" zu verwenden, also keine virtuellen Festplatten, sondern tatsächliche Volumes auf dem Virtualisierungshost, die an den Gast-DC durchgereicht werden. Hier stehen die Snapshot-Möglichkeiten nicht zur Verfügung.

Da nun die nicht unterstützten Sicherungsmethoden und die damit verbundenen Gefahren bekannt sind, drängt sich die Frage nach einer Aufstellung unterstützter Backuplösungen auf. Microsoft selbst führt keine Liste, nennt aber das Kriterium, das eine Backuplösung zu einer "unterstützten" macht. Das Geheimnis liegt in der "InvocationID", die jeder Domänencontroller trägt. Die InvocationID ist ein sogenannter Global Unique Identifyer (GUID), die den Domänencontroller eindeutig identifiziert (auch nach der Umbenennung). Unterstützte Backuplösungen markieren nach einer erfolgreichen Wiederherstellung der AD-Datenbank den DC, so dass er seine InvocationID beim nächsten Start ändert. Damit verhält sich der DC dann wie ein "Neuer" und handelt die Replikation mit USN und geänderter InvocationID neu aus. Sollte es notwendig sein, einen Snapshot zurück zu spielen, muss auch der Mechanismus zur Änderung der InvocationID angewandt werden.

Snapshots ohne Probleme zurückspielen

Um einen Domänencontroller über eine imagebasierte Sicherung oder einen Snapshot zurückzuspielen, können Sie die InvocationID auch manuell ändern. Um festzustellen, welche USNs von welchem DC zuletzt repliziert wurden (High Watermark Table oder Up-To-Date-Vector) verwenden Sie den Befehl *Repadmin /showutdvec*. Besonders interessant dabei ist, dass Sie mit dem zusätzlichen Parameter "/nocache" auch die eigene InvocationID sowie die der Replikationspartner erhalten:

```
Repadmin /showutdvec localhost
  dc=firma,dc=de /nocache
```

Der folgende Prozess sollte nur im absoluten Notfall angewendet werden, im Normalfall sollten Domänencontroller lieber durch Neuinstallation und Replikation der letzten Daten von benachbarten Domänencontrollern der gleichen Domäne hergestellt werden. Wenn aber ein Snapshot zurückgespielt wurde (oder eine Imagebasierte Sicherung) gehen Sie wie folgt vor:

1. Deaktivieren Sie die Netzwerkverbindung unmittelbar vor, während oder nach der Rücksicherung, aber auf alle Fälle bevor der rückgesicherte DC das erste Mal startet.
2. Booten Sie in den Verzeichnisdienstwiederherstellungsmodus (Directory Services Restore Mode, oder DSRM)

3. Wenn Sie den Dateireplikationsdienst NTFRS für Sysvol verwenden (Standardmäßig vor Windows Server 2008 R2), halten Sie den Dienst an. Dann den navigieren Sie in den Registrierungsschlüssel " HKLM \ System \ CurrentControlSet \ Services \ NtFrs \ Parameters \ Backup/Restore \Process names". Dort ändern oder erstellen Sie den Wert "BurFlags" (Format DWORD) und setzen ihn auf "D2" (das ist für die Wiederherstellung der Sysvol-Replikation notwendig).
4. In der Registry setzen Sie nun unter "HKLM \ System \ CurrentControlSet \ Services \ NTDS \ Parameters" den Schlüssel "Database restored from backup" auf "1" (sollte dieser nicht vorhanden sein, dann erstellen Sie ihn als DWORD). Dies sagt dem DC, dass er nach dem nächsten Start eine neue InvocationID erzeugen soll.
5. Wenn an dieser Stelle auch der Schlüssel "DSA Previous Restore Count" existiert, merken Sie sich den Wert. Er sollte sich nach dem Reboot um 1 erhöhen.
6. Hängen Sie jetzt den Server wieder an das Netzwerk und starten Sie ihn (im normalen Modus) neu.
7. Verifizieren Sie anschließend, dass eine neue InvocationID erzeugt wurde und der Registrierungsschlüssel "DSA Previous Restore Count" um 1 erhöht ist. Im der Ereignisanzeige sehen Sie jetzt auch das Event 1109, das anzeigt dass das AD von einer Datensicherung wiederhergestellt wurde.

Durch diesen Prozess erhält der DC eine neue InvocationID und verhält sich wie ein frisch installierter DC, das heißt er versucht alle Daten im Verzeichnis erneut abzugleichen und verlässt sich nicht auf die Daten, die er bereits hat.

Sollten Sie Snapshots oder ein imagebasiertes Backup der virtuellen Festplatten verwenden (müssen), so ist es empfehlenswert, den Registrierungsschlüssel vor der Datensicherung zu setzen und nach der Sicherung wieder zu entfernen. Damit wird sichergestellt, dass eine Rücksicherung niemals zu einem USN-Rollback führt. Den Registrierungsschlüssel immer gesetzt zu lassen, wird nicht empfohlen, da dann die Invocation ID bei jedem Neustart geändert wird, was zu Netzwerkproblemen und langfristigen Problemen im AD führen kann.

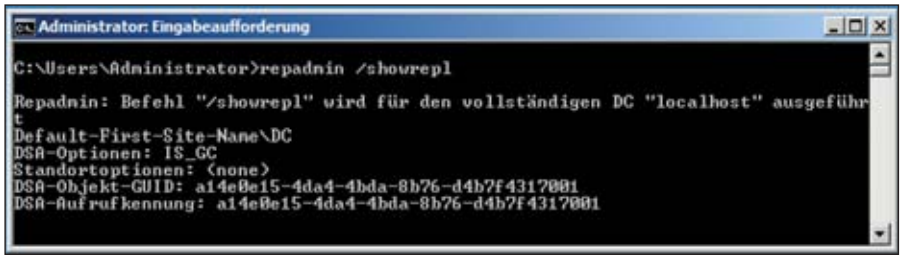


Bild 4: Die InvocationID identifiziert den Domänencontroller eindeutig

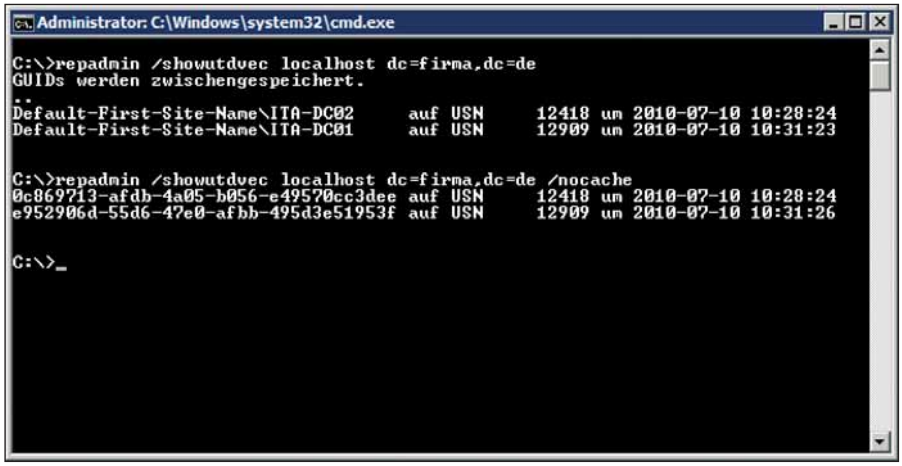


Bild 5: Vor dem Ändern der InvocationID sollte der Administrator diese notieren, was auch von einem Replikationspartner aus erfolgen kann

Einsatzmöglichkeiten virtualisierter DCs

Eingangs nannten wir einige Vorteile der Virtualisierung bei Domänencontrollern. Aber wenn Sie sich tiefergehend mit dem Thema beschäftigen, dann sind virtualisierte DCs auch optimal für die folgenden, beispielhaften Einsatzzwecke:

- Klonen der virtuellen Maschinen durch einfaches Kopieren erlaubt Ihnen, eine produktionsnahe Testumgebung zu realisieren (Achten Sie darauf , dass das Netzwerk abgeschottet ist).
- Für kritische Updates wie Schema-Updates können zusätzliche virtualisierte DCs eingesetzt werden (etwa ein bis zwei DCs pro Domäne), die sich vorübergehend abschotten lassen. Die Schema-Updates können dann dort eingespielt und überprüft werden. Die Replikation mit dem restlichen Netzwerk wird erst wieder erlaubt wenn das Update erfolgreich war.
- Dedizierte Domänencontroller in Außenstellen könnten auf einem virtualisierten Server laufen. Im Allgemeinen, vor allem in größeren Umgebungen, sollten Sie Infrastrukturdienste wie AD, DNS und so weiter von Anwendungs- oder Dateiservern trennen (da diese auch häufig von verschiedenen Personen administriert werden und Sie beim Wiederherstellen von DCs nicht Rücksicht auf "fremde Daten" nehmen müssen). Die Virtualisierung vereinfacht auch dies.

Es gibt unzählige Einsatzzwecke für virtuelle Domänencontroller. Wenn damit verantwortlich umgegangen wird, Single Points of Failure vermieden werden, die USN-Rollback-Problematik bekannt ist und die Zeit-Infrastruktur entsprechend aufgebaut ist, gibt es keinen Grund diese Vorteile nicht zu nutzen. *(jp)*

Die Active Directory-Verwaltungskonsole

Aufgemöbelte Kommandozentrale

Obwohl das Active Directory seit der Einführung mit Windows 2000 mehrere Updates erfahren und sich maßgeblich in einigen Funktionen geändert hat, gibt es andere Optionen und Komponenten des Dienstes, die keinem Wandel unterzogen wurden. Einige Features und Verwaltungswerkzeuge existieren in überwiegend unveränderter Form noch heute – beispielsweise die Verwaltungskonsole "Active Directory-Benutzer und -Computer", kurz ADUC. Doch mit Server 2008 R2 und Windows 7 stehen Änderungen ins Haus.

Löst die in die Jahre gekommene AD-Verwaltungskonsole ab: das AD Administrative Center

Die bisherige Verwaltungskonsole ADUC hat sich, abgesehen von ein paar kosmetischen Änderungen und Updates zur Unterstützung neuer Features, nicht konzeptionell geändert. Doch mit Windows Server 2008 R2 und Windows 7 liefert Microsoft eine komplett überarbeitete Active Directory-Verwaltungskonsole aus: das "Active Directory Administrative Center" (ADAC) oder auch "Active Directory-Verwaltungscenter". Mit dem ADAC will Microsoft seinem Hauptverwaltungswerkzeug für Administratoren neues Leben einhauchen. Die neue Konsole ist übersichtlicher, besser an persönliche Bedürfnisse anzupassen und legt großen Wert auf aufgabenbasiertes Arbeiten. Voraussetzungen für das ADAC sind Windows Server 2008 R2 oder Windows 7. In Windows Server 2008 R2 wird das ADAC beim Heraufstufen des Servers mit den bekannten Tools installiert – in Windows 7 ist das ADAC in RSAT enthalten.

Doch allein mit dem Verwaltungswerkzeug ist es nicht getan: ADAC muss, um eine Verbindung zur Domäne zu erhalten, Kontakt zu einem Domänencontroller (DC) herstellen, der die Active Directory Web Services (ADWS) ausführt. Diese Webdienste sind in Windows Server 2008 R2 bereits enthalten, für Windows Server 2003 SP2 und Windows Server 2008 stellt Microsoft den Download "Active Directory Management Gateway Service" bereit [1]. Mindestens ein ADWS-fähiger DC muss also für das ADAC vorhanden sein, um die Domäne administrieren zu können. Der Grund hierfür sind die Voraussetzungen, die ADAC an die Infrastruktur stellt. Vollständig auf der AD-PowerShell basierend, verbindet sich das Verwaltungsinstrument über die PowerShell mit den AD-Webservices. ADWS kommuniziert alle Anfragen, Suchen und Änderungen mit dem Verzeichnisdienst.

Aufgepeppte Navigation

Das ADAC kommt beim ersten Start optisch aufgepeppter daher: Die Baumansicht der verbundenen Domäne ist aus dem linken Fensterabschnitt verschwunden, im mittleren Teil können Sie gleich nach Start der Konsole bereits erste Verwaltungsaufgaben wie das Zurücksetzen eines Passwortes erledigen. Wird der Domänenname oder ein anderes Objekt des AD angeklickt, blendet sich im rechten Fensterabschnitt die von anderen Konsolen bekannte "Tasks"-Spalte ein. Sie erlaubt es, bekannte Optionen aus dem Kontextmenü mit einem einfachen Klick auszuführen.

Mit einem Klick auf den Domänennamen öffnet sich ein neues Menü mit den "First Level" OUs, die unter dem Domänenobjekt erstellt wurden. Das Menü verhält sich dabei wie andere bekannte Dialogmenüs in Windows: Fahren Sie mit der Maus über eine OU, öffnet sich das nächste OU-Level und zeigt alle Kindsobjekte

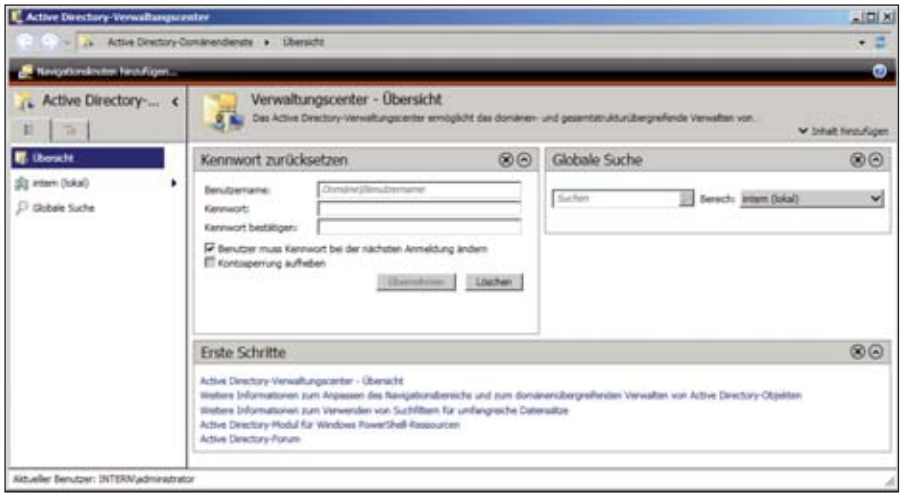


Bild 1: Das ADAC macht auf den ersten Blick einen aufgabenorientierteren Eindruck als sein Vorgänger

der selektierten OU. Kunden mit vielen Organisationseinheiten einer OU-Ebene hat Microsoft mit dem Suchfeld am Kopf des aufgeklappten Menüs einen Gefallen getan. Wer sich mit dem Menü nicht anfreunden mag, kann über die Schaltfläche "Baumansicht" zur altbekannten Baumdarstellung zurückkehren.

Um schnell an immer wiederkehrende Orte im Verzeichnis springen zu können, lässt das ADAC den Benutzer favorisierte Orte zwischenspeichern, die unterhalb des Domänenknotens abgelegt werden. Mit der Schaltfläche "Add Navigation Nodes" über das Navigationsmenü wählen Sie die OUs aus, die Sie anschließend per einfachem Klick öffnen oder als Basis für das Durchsuchen des Verzeichnisses nutzen. Lange Suchen oder das Klicken durch den ganzen Verzeichnisbaum sind nicht mehr notwendig. Die wichtigsten Orte für Administratoren, den Helpdesk oder OU-Admins lassen sich so als Favoriten im ADAC speichern.

Besonders interessant ist dieses Feature, falls Sie mehrere Gesamtstrukturen verwalten müssen. Nicht nur Domänen und OUs des eigenen Forests können Sie so als Favorit hinterlegen, sondern auch Orte im Verzeichnis anderer, vertrauter Forests. Mit einem einzigen, laufenden ADAC administrieren Sie damit mehrere Domänen gleichzeitig. Mit "Active Directory-Benutzer und -Computer" war es bisher notwendig, die Konsole zwischen den Domänen zu verbinden oder mehrere Instanzen der Konsole zu öffnen. ADUC konnte nur eine Domäne fokussieren. Das macht ADAC attraktiv für Mehrdomänen-Forests und Administratoren, die während Migrationen mehrere Domänen administrieren müssen.

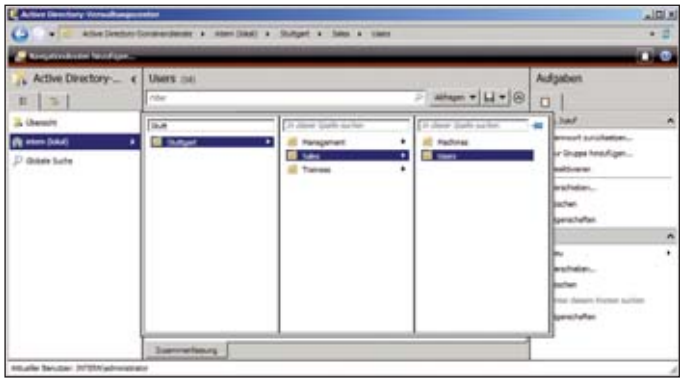


Bild 2: Mit dem ADAC kann das Verzeichnis schneller und effizienter durchforstet werden

Nutzen Sie LDP oder andere LDAP-Browser, werden Sie an der Pfad-Leiste am oberen Rand des ADAC Gefallen finden: Steht eine OU im aktuellen Fokus des ADAC, ändert sich die leicht lesbare Pfadangabe einfach per Klick in die Adresszeile in die LDAP-Schreibweise des Pfades. Pfade können so kopiert und in anderen LDAP-Browsern verwendet werden – oder umgekehrt, so dass ADAC einen kopierten LDAP-Pfad fokussiert und anzeigt.

Gesucht und gefunden

Sind die Abkürzungen zu den wichtigsten Plätzen im Verzeichnis eingerichtet, verdient das Suchen und Finden bestimmter Objekte in OUs eine nähere Betrachtung. Die aus "Active Directory-Benutzer und -Computer" bekannten Abfragen sind im ADAC verbessert und konsequent erweitert worden. Haben Sie eine OU ausgewählt, erscheinen im mittleren Fensterabschnitt alle Objekte dieser OU. Darüber finden Sie ein Filter-Menü, mit dessen Hilfe Sie in der OU und allen untergeordneten OUs anhand vordefinierter Kriterien filtern können.

Neben der Standardsuche nach Namen im "Filter"-Feld, lassen sich benutzerdefinierte Suchen erstellen und für spätere Zwecke speichern. Mit dem Button "Add Criteria" bietet das ADAC eine Reihe vordefinierter Filtermöglichkeiten und viele bekannte Felder aus den Eigenschaften-Reitern von Benutzer- und Computerobjekten aus "Active Directory-Benutzer und -Computer" an. Per Klick erstellen Sie Filter, die alle gesperrten und deaktivierten Benutzer oder jene anzeigen, deren Passwort in wenigen Tagen abläuft. Die vordefinierten Filter spiegeln in der Tat das wieder, was viele Systemverwalter häufig für die Erledigung ihrer Aufgaben suchen: abgelaufene, gesperrte oder deaktivierte Benutzer sowie Standardfelder wie "Name", "Telefonnummer", "Beschreibung" oder die Mitarbeiternummer.

Die Filter lassen sich beliebig kombinieren – jedoch nur per logischem "Und". Filter, die entweder nach der einen oder nach der anderen Eigenschaft selektieren sollen, müssen Sie weiterhin von Hand im LDAP-Filter-Format eingeben. Zurück zu den klassischen LDAP-Suchen gelan-

gen Sie, indem Sie über die "Tasks"-Spalte mit "Search under this node" in die "Global Search" wechseln. Hier stehen "Normale Suche" und "LDAP-Suche" zur Auswahl. Von der normalen Suche können Sie stets in die "LDAP-Suche" wechseln, so dass sich eine Suche erst mit dem "Add Criteria"-Knopf vorbereiten und anschließend mit manuellem LDAP-Code verfeinern lässt.

Die "Global Search" ist auch der richtige Ort für Suchen in unterschiedlichen Orten des Verzeichnisses. Das "Scope"-Auswahlfeld erlaubt die Selektion mehrerer AD-Knoten aus dem Navigationsbereich oder als Alternative eine Suche im Globalen Katalog. Befinden sich Suchergebnisse in mehreren, nicht hierarchisch zusammenhängenden OUs, ist die globale Suche der richtige Ort, um seine Suche zu definieren. Gesichert werden selbsterstellte Suchen über das Diskettensymbol. Gespeicherte Suchen werden auf jeder OU-Ebene über den "Queries"-Knopf aufgerufen und gestartet.

Hervorragende Übersicht hilft bei der Administration

Nach der Suche im Verzeichnis ist es nun an der Zeit, das Verzeichnis mit dem ADAC zu administrieren. In gewohnter Manier wählen Sie hierfür mit einem Rechtsklick den Kontextmenüpunkt "Eigenschaften" eines Benutzer- oder Computerkontos aus, um die Konteneigenschaften zu verwalten. ADAC öffnet daraufhin ein neues Übersichtsfenster. Das Übersichtsfenster der ADAC wirkt geordneter und ist nicht mehr, wie in der ADUC-Konsole, in Tabs aufgeteilt. Stattdessen lassen sich alle Kontenoptionen auf einer Seite bearbeiten.

Die Optionen-Seite ist in Abschnitte aufgeteilt, die Sie am linken Fensterrand per Klick auswählen. ADAC springt beim Klick an die korrekte Stelle innerhalb der Seite. Die Abschnitte sind im Vergleich zu den Kontenoptionen in "Users and Computers" ähnlich gegliedert. Die Kontenreiter im Eigenschaftenfenster sind nun auf einer Seite als Abschnitte angeordnet. Lästiges Suchen nach dem richtigen Reiter entfällt, da alle Informationen auf einer Seite angeordnet sind.

Bild 3: Die aufgabenorientierten Sichten auf Benutzer helfen bei der Administration

Praktisch ist die Option, die Eigenschaftenseite anzupassen. Jeder Abschnitt verfügt über einen "Minimieren"-Pfeil und ein "Schließen"-Kreuz, mit dem sich die Seite auf benötigte Sektionen reduzieren lässt und nicht verwendete Informationen ausgeblendet werden. Wer keine Profilpfade administriert, kann den Abschnitt "Profile" getrost schließen. Sollte der Abschnitt später doch einmal benötigt werden, können Sie diesen über den Punkt "Abschnitt hinzufügen" in der rechten oberen Ecke zurückholen.

Zwingend notwendige Eingaben beim Erstellen neuer Objekte zeigt ADAC mit einem roten Stern an. Das Speichern eines neuen Benutzerkontos wird so lange verweigert, bis alle Angaben korrekt sind. Auch die Prüfung der eingegebenen Werte findet sofort statt. ADUC prüft Passworte beispielsweise nur beim Klick auf "Weiter", um einen neuen Benutzeraccount anzulegen. ADAC färbt bereits beim Editieren des Passwortes das Eingabefeld sowie den Abschnittskopf rot, um auf eine Fehleingabe hinzuweisen.

Eingaben werden umgehend evaluiert. Ein Beispiel hierfür ist die Eigenschaft "Konto läuft ab". Ändern Sie die Eigenschaft von "Never" auf "End of" ab und vergeben ein Ablaufdatum für einen Account, zeigt ADAC fix an, wie lange der Account noch gültig sein wird – in Tagen und Stunden. Liegt das Datum in der Vergangenheit, heißt es "bereits abgelaufen".

Fazit

Als Nachfolger der "Active Directory-Benutzer und -Computer"-Konsole zeigt sich das Active Directory Administrative Center deutlich reifer und zeitgemäßer strukturiert. Ganz auf der PowerShell basierend ist das Administrationszentrum auf das Erledigen von Aufgaben zugeschnitten. Häufig genutzte Suchen und Tätigkeiten der Active Directory-Administration von Benutzern, Computern und Gruppen sind an vielen Stellen bereits vordefiniert und leichter zugänglich. Das Aussehen ist an manchen Stellen einfacher anzupassen und durch kurze Wege schneller zu bedienen. *(dr)*

Links

[1] Active Directory Management Gateway Service
www.microsoft.com/downloads/details.aspx?FamilyID=008940c6-0296-4597-be3e-1d24c1cf0dda&displaylang=en

Dokumentation des Active Directory

Mein Auto, mein Haus, mein AD

Gründe für eine saubere Dokumentation von Diensten und Strukturen gibt es zu Hauf – sei es ein ordentliches Änderungsmanagement, das Vorher-Nachher-Zustände deutlich macht oder aktuelle Ist-Zustände, die im schlimmsten Fall helfen, den letzten Konfigurationsstand wiederherzustellen oder ihn mit einem wiederhergestellten Backup zu vergleichen. Sie alle unterstützen beteiligte Administratoren dabei, Transparenz im Umgang mit dem System zu schaffen. Dieser Beitrag zeigt, wie Sie mit zwei freien Tools Daten und Topologie dokumentieren. Weiterhin werfen wir einen Blick darauf, wie sich Änderungen der Daten im Active Directory dokumentieren lassen.

Eine gute Dokumentation ist natürlich auch für das Active Directory (AD) vonnöten. Als sehr gut skalierender Verzeichnisdienst, der bis in riesige Infrastrukturen wachsen kann, gestaltet sich allerdings die Dokumentation mancherorts schwierig. Das AD hat viele Aspekte und Facetten, die aus unterschiedlichen Richtungen beleuchtet oder dokumentiert werden sollten. Vor dem Einsatz eines Werkzeuges oder Drittanbieterproduktes muss daher der erstrebte Nutzen der geplanten Dokumentation abgesteckt und definiert werden.

Daten- und Topologiedokumentation

Nicht alle erhältlichen Tools zur Beschreibung des Verzeichnisses sind für alle Protokollzwecke geeignet – sie haben jeweils ihre Stärken und Schwächen. Ein Beispiel ist der Active Directory Topology Diagrammer (ADTD) [1], auf den wir später in diesem Artikel zurückkommen. ADTD nutzt eine Schnittstelle zu Microsoft Visio, um ein vollständiges Diagramm der AD-Topologie zu zeichnen. Dabei kann die Detailtreue beliebig tief zwischen Forest- und Domänendiagrammen bis hin zu OUs, Objekten und GPO-Diagrammen variieren. Selbst Standortverknüpfungen und deren Metriken lassen sich abbilden – ganz nach Wunsch des Bedieners. Diese Art von Diagrammen eignet sich hervorragend, um Änderungen am Verzeichnis zu dokumentieren oder interne Mitarbeiterschulungen aufzusetzen, da die Topologie selbst im Vordergrund steht.

Ein anderes Beispiel ist ADExplorer [2] von Sysinternals. ADExplorer ist primär ein weiteres Werkzeug, um das Verzeichnis zu durchstöbern. Es besitzt aber eine interessante Funktionalität, um Momentaufnahmen des AD aufzunehmen und abzuspeichern. Diese Snapshots werden abgelegt und dienen als Beschreibung, etwa für Änderungen, wie das Verzeichnis vor der Änderung und entsprechend, nach der Änderung aussieht. ADExplorer ist ein Beispiel für eine Datendokumentation die, im Gegensatz zur Topologie-Doku, nicht die logische Struktur des Verzeichnisses, sondern des Inhalts, die Daten, fokussiert. Nützlich wird diese Art von Dokumentation, wenn im Fehlerfall ein Backup zurückgespielt werden muss und die Ist-Daten nach dem Restore mit den zuletzt dokumentierten Daten verglichen werden können.

Sie müssen entscheiden, welche Form der Dokumentation Sie bevorzugen – in der Praxis hat sich ein Mix aus Dokumentation der logischen Struktur der Topologie und einem Schnappschuss der Daten eines Zeitpunktes bewährt.

Dokumentation mit José

Ein erstes, freies Tool, das die Struktur des Active Directory grafisch darstellt ist "José". José ist ein HTML-basiertes Werkzeug, das, abhängig von der Auswahl des Bedieners, einen kompletten HTML-Report aller OUs, Objekte und einigen vordefinierten Attributen erzeugt. Der Unterbau von José ist VBscript, das völlig

ohne Benutzerinteraktion im Hintergrund seine Dienste erledigt.

Nach dem Download [3] inklusive Entpacken starten Sie das Tool mit einem Doppelklick auf *Jose.HTA*. Jetzt öffnet sich die HTML-basierte Konfigurationsmaske des Tools. Am oberen Rand des nützlichen Werkzeugs wird die Start-OU in LDAP-Schreibweise angegeben – bleibt sie leer, durchkämmt José alle Objekte bei der Domänenwurzel beginnend bis in die letzten OUs. Das kann gerade in größeren Verzeichnissen einige Zeit in Anspruch nehmen – wollen Sie also nur einen Ausschnitt des AD betrachten, sollten Sie die Start-OU in jedem Fall angeben. Den Grad der Detaillierung des HTML-Reports können Sie beliebig wählen: In "Objekt- und Eigenschaften-Auswahl" bestimmen Administratoren, welche zusätzlichen Informationen im Report auftauchen sollen. Stehen OUs und deren Eigenschaften im Fokus, sind mit Sicherheit Gruppenrichtlinien von Interesse – benötigen Sie Veränderungen des Verzeichnisses im Bericht, sollten Sie die "Änderungsdaten der Objekte" einbeziehen.

Auf Objektebene bietet das Werkzeug die bekanntesten Objektattribute zur Auswahl an. Die Vorgabe wählt nur einige von ihnen aus, weitere Attribute schalten Sie sich per Checkbox zu und ab. Ebenso funktioniert dies mit Objekttypen. Sind Drucker nicht von Interesse oder Kontakte über einen anderen Bericht abgedeckt, werden sie durch Abwahl vom Bericht ausgeschlossen. José konzentriert sich dann ausschließlich auf die restlichen ausgewählten Objekte.

Der untere Abschnitt des Werkzeugs beschäftigt sich mit den Metadaten des Reports. Um eine Legende zu den im Report verwendeten Symbolen anzuzeigen, müssen Sie die entsprechende Checkbox aktivieren. Selbst die aktuelle Auswahl der AD-Objekte und deren Attribute kann José speichern. Mit "Report-Definition speichern" legt das Tool die aktuelle Konfiguration ab. Einmal hinterlegt, kann das Werkzeug per Kommandozeile gestartet werden, um Berichte anhand der gewählten Konfiguration zu erstellen. Sinnvoll wird dies, wenn Berichte zyklisch erstellt werden müssen. Per

```
cscript //nologo JoseExec.vbs
  /d:eigeneDefinition.txt
  /r:EigenerBericht%date%.htm
```

lädt José die als "eigene Definition" gespeicherte Konfiguration, führt sie aus und speichert den HTML-Report als *EigenerBericht{Datum}.htm* im "Reports"-Ordner des Standardverzeichnisses.

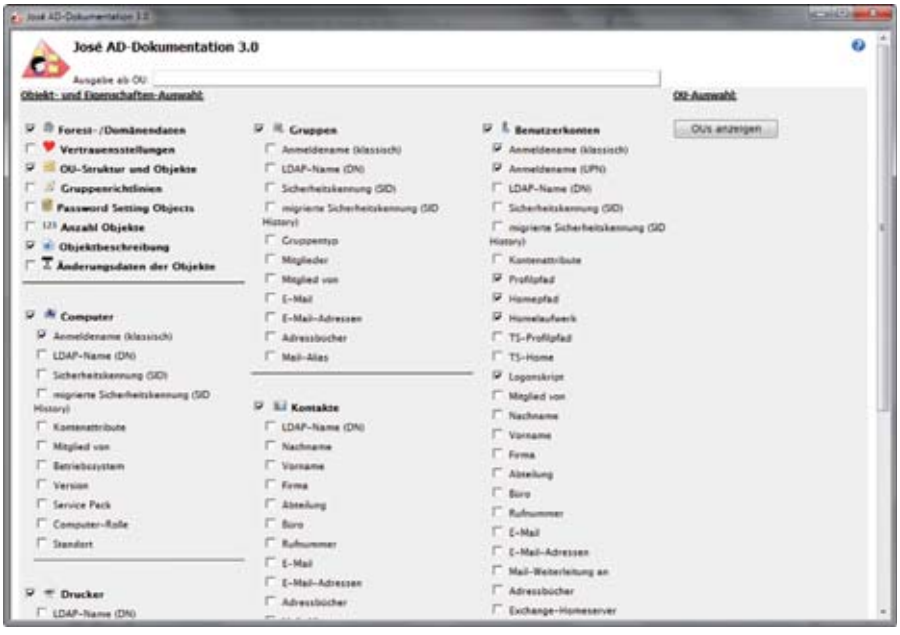


Bild 1: José liefert AD-Objekte und ausgewählte Attribute in einem übersichtlichen HTML-Report

Komplexe Diagramme mit ADTD erstellen

José erzeugt sehr einfach per Knopfdruck die gewünschte Dokumentation in Form von HTML. Ein Bericht im HTML-Format hat allerdings den Nachteil, dass die gefundenen Daten im Bericht nicht einfach verändert werden können, ohne dass der Formatierungscode angepasst wird. Die Platzierung und das Layout des Berichts sind starr.

Um die Option einer möglichen Nachbearbeitung zu wahren, können Sie auf ein anderes Werkzeug setzen: Der schon erwähnte "Active Directory Topology Diagrammer" (ADTD). Das Tool zeichnet AD-Strukturen mit Hilfe von Office Visio und speichert sie im bekannten Visio-Format ab, um spätere Nachbearbeitungen zuzulassen. Das heruntergeladene Paket beinhaltet einen Setupassistenten, der durch die Installation des Diagrammers führt. ADTD ist eine .NET-Applikation und als solche benötigt es das .NET Framework ab Version 2.0 auf dem Client. Die installierte Visio-Version spielt hierbei keine Rolle – ab Visio 2003 bis einschließlich 2010 funktionieren alle Versionen problemlos. Auch das Betriebssystem, ob Server oder Client, spielt keine Rolle. ADTD muss nicht auf einem Domänencontroller installiert werden – es genügt ein beliebiger Client, der mit Visio und dem .NET Framework ausgestattet ist und der Domäne beiwohnt.

Das Sammeln der Daten erledigt ADTD unter Verwendung eines Global Catalogs – das Tool benötigt also eine Verbindung zu einem GC. Da je nach Report einige Daten gesammelt werden, sollte ein GC in Reichweite sein. Der erste Start von ADTD zeigt die Fülle an Informationen, die das Werkzeug dokumentieren kann. Eine komplette AD-Topologie wird in ihre Komponenten geteilt, die per eigener Registerkarte zusätzlich angewählt

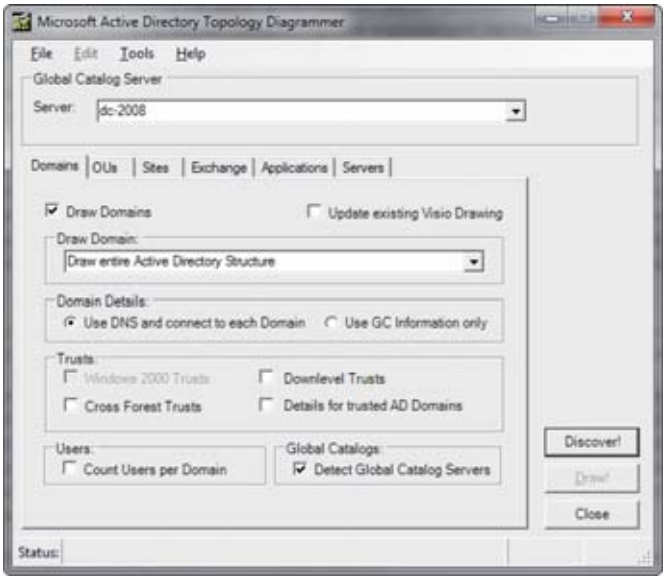


Bild 2: ADTD nutzt Office Visio, um die Active Directory-Struktur und seine Daten darzustellen

und konfiguriert werden können. Die Standardvorgabe wählt im Reiter "Domains" alle verfügbaren Domänen und im Reiter "Servers" die darin befindlichen DCs aus. Nähere Informationen werden dann in den entsprechenden Reitern per Checkbox hinzugeschaltet.

Auch für Exchange ist ein Reiter vorgesehen, der ADTD anweist, Informationen über die Exchange-Organisationen der Gesamtstruktur zu sammeln. Da Exchange ein wichtiger Konsument des Verzeichnisses ist und einen integralen Teil der Infrastruktur darstellt, ist es nur richtig, Exchange in ein Gesamtstrukturdiagramm zu integrieren. ADTD kümmert sich also nicht nur um das Verzeichnis allein, sondern auch explizit um die Konfiguration von Exchange, die im Verzeichnis abgelegt wird.

Der Button "Discover!" sammelt erste Informationen über die Gesamtstruktur, wie etwa die Anzahl der Domänen im Forest, welche Vertrauensstellungen zu anderen Domänen und Forests es gibt und welche Anwendungspartitionen verfügbar sind. Ist dies beendet, sind die gesammelten Informationen in den Dropdown-Auswahlfeldern der einzelnen Reiter verfügbar. In "Domains" können Sie nun beispielsweise zwischen "Draw entire Active Directory Structure" und allen verfügbaren Domänen der Gesamtstruktur wählen. So zeichnet ADTD nur die ausgewählte Domäne und ihre Informationen in Visio. In "Applications" werden nun auch die verfügbaren Anwendungspartitionen zur Einzelauswahl angeboten.

Mit einem Klick auf "Draw!" starten Sie den Sammelvorgang der Diagramminformationen und beginnen gleichzeitig, das Visio-Kunstwerk zu zeichnen. Jede ausgewählte Teilkomponente aus den ADTD-Reitern erzeugt ein eigenes Visio-Diagramm. Die Domänen werden demnach in einem anderen Diagramm als die OUs oder Standorte gezeichnet. Den Abschluss der Dokumentation quittiert ADTD mit der Statusmeldung "Drawing complete!" in der Statuszeile am Fuß des Werkzeuges. Manche Diagramme benötigen noch etwas Feintuning, da ADTD nicht immer alle Verbindungslinien oder Verknüpfungen leserlich nebeneinander legt. Dies lässt sich jedoch in bekannter Drag-and-Drop-Manier korrigieren.

Ist-Zustand sichern

Ein Bild sagt zwar mehr als tausend Worte, wenn aber nicht die Struktur des Verzeichnisses, sondern der Datenbestand zu einem gewissen Zeitpunkt dokumentiert und niedergelegt werden soll, hilft es wenig, Bilder von Unmengen von Objekten abzulegen. Hier sind Abzüge von aktuellen Ist-Daten aus dem Verzeichnis meist sinnvoller. Bereits genannt wurden Vorher-Nachher-Vergleichsmöglichkeiten bei AD-Änderungen oder Neuinstallationen von Diensten und die Kontrolle von Backups nach einer Wiederherstellung. Großen Nutzen bringt der AD-Daten-Dump jedoch nur, wenn die Daten in einem Format vorliegen, das sich einfach und unkompliziert wiederverwenden lässt.

Windows Server ist bereits mit einem Kommandozeilen-Exporteur ausgestattet: "CSVDE". Der sogenannte Directory Exchanger (DE), der Verzeichnisdaten im CSV-Format niederlegt, ist seit Windows 2000 in jeder Server-Version enthalten. CSVDE importiert und exportiert AD-Objekte aus Textdateien, die in Komma-separierten Strukturen abgelegt werden. Jede Zeile der Textdatei entspricht dabei einem Objekt, jede Spalte, durch Kommata getrennt, einem Attribut. CSV-Dateien können Sie für Review-Zwecke sehr einfach mit Excel oder jedem anderen Tabellenkalkulationsprogramm öffnen. Letztlich sind die Daten im CSV-Format in Reintextform formatiert präsent.

Das Kommandozeilenprogramm kennt einige Schalter – darunter den Modusschalter für Imports/Exports, einen Schalter für die Angabe des Basis-DN, an dem der Export stattfinden soll und einen Objektfilter – für das Herausschreiben von Objekten spezieller Natur. Die einfachste Form eines Dumps in das File *output.csv* von Benutzerobjekten der OU "Users" sieht wie folgt aus:

```
csvde -d
  OU=Users,OU=IT,OU=Berlin,DC=
  contoso,DC=com -r
  "&(objectClass=user)
  (objectCategory=person)"
  -f C:\output.csv
```

Der Schalter "-d" gibt den Basis-DN an, "-r" gibt den Filter an, den CSVDE an das Verzeichnis schicken soll. Mit "-f" wird das Output-File angegeben. CSVDE schreibt nachfolgend eine große Auswahl verfügbarer Attribute in die Zieldatei. Sind nur einige, wenige Attribute für den Dump von Interesse, nutzen Sie den Schalter "-l":

Bild 3: Einen Dump aktueller Verzeichnisdaten erstellt CSVDE von der Kommandozeile aus

```
csvde -d OU=Users,OU=IT,OU=HQ-
  Waldshut,DC=intern,DC=frickelsoft,
  DC=net -r "(objectClass=user)"
  -f C:\output-phone.csv
  -l telephoneNumber,mail
```

Administratoren, die mit der Kommandozeile auf Kriegsfuß stehen, werden Carlos [4] mögen. Carlos, vom gleichen Hersteller wie das zuvor vorgestellte José, ist eine kostenfreie Konfigurationsmaske für CSVDE, die per HTML-Oberfläche alle CSVDE-Schalter selbst errechnet und anschließend per Knopfdruck ausführt. Die zu exportierenden Objekte wählt der Administrator per Checkbox aus, gibt im nächsten Schritt die gewünschten Attribute an und wählt anschließend den Startknoten im Verzeichnisdaum in LDAP-Schreibweise. Per Klick auf "Jetzt exportieren" oder per Tastatur ("ALT+E") führt Carlos das CSVDE-Kommando aus. Den zusammengeklickten Befehl gibt das Tool in einer der Statuszeilen aus – für die spätere Verwendung.

Clever vergleichen

Weniger für Dokumentationszwecke bekannt ist "ADExplorer" aus der Sysinternals-Werkzeugkiste. Microsoft beschreibt die Hauptaufgaben von ADExplorer als Navigationshilfe und AD-Browser. Für Dokumentationszwecke weitaus interessantere Features werden erst im zweiten Absatz der Programmbeschreibung erwähnt: die Erstellung von Dumps der AD-Datenbank und eine Vergleichsoption zweier erstellter Dumps.

Beim Start von ADExplorer zeigt das Tool im Fenster "Connect to Active Directory" zwei Optionen an: eine Anmeldung am Verzeichnisdienst per DC-Name, Benutzername und Kennwort oder das Laden eines früher angelegten Snapshots der AD-Datenbank mit dem Tool. Für den ersten Snapshot ist eine normale Anmeldung notwendig, so dass die erste Option mit den entsprechenden Angaben durchgeführt werden muss. Im Anschluss kontaktiert ADExplorer den angegebenen DC und lädt dessen Default-Namenskontexte.

Wie Microsoft anpreist, werden die Namenskontexte in einem Baum angezeigt, so dass Sie durch die Container und OUs navigieren und sich Verzeichnisdaten anzeigen lassen können. Ist eine Stelle im Verzeichnis besonders interessant, speichern Sie sie mit "Favorites" und anschließend "Add to Favorites". Der Favorit wird dann im "Favorites"-Menü angezeigt und kann zur Schnellnavigation ausgewählt werden. Die Snapshot-Funktion versteckt sich hinter dem Diskettensymbol in der Symbolleiste oder im Menü "File / Create Snapshot". Vom Bediener wird erwartet, dass er den Dateinamen und den Zielpfad der Dumpdatei angibt. ADExplorer speichert seine Ergebnisse in eine DAT-Datei ab, die sich nicht mit Texteditoren lesen lassen. Für spätere Analysen des Dumps nutzen Sie also erneut den ADExplorer. Mit einem Klick auf "OK" beginnt ADExplorer mit der Erzeugung des Snapshots.

Hat das Tool seine Arbeit erledigt, sollte die DAT-Datei an einem sicheren Ort aufbewahrt werden. Sie enthält einen Auszug der AD-Livedaten und sollte auf keinen Fall in einem Fileshare oder einem öffentlich zugänglichen Verzeichnis aufbewahrt werden.

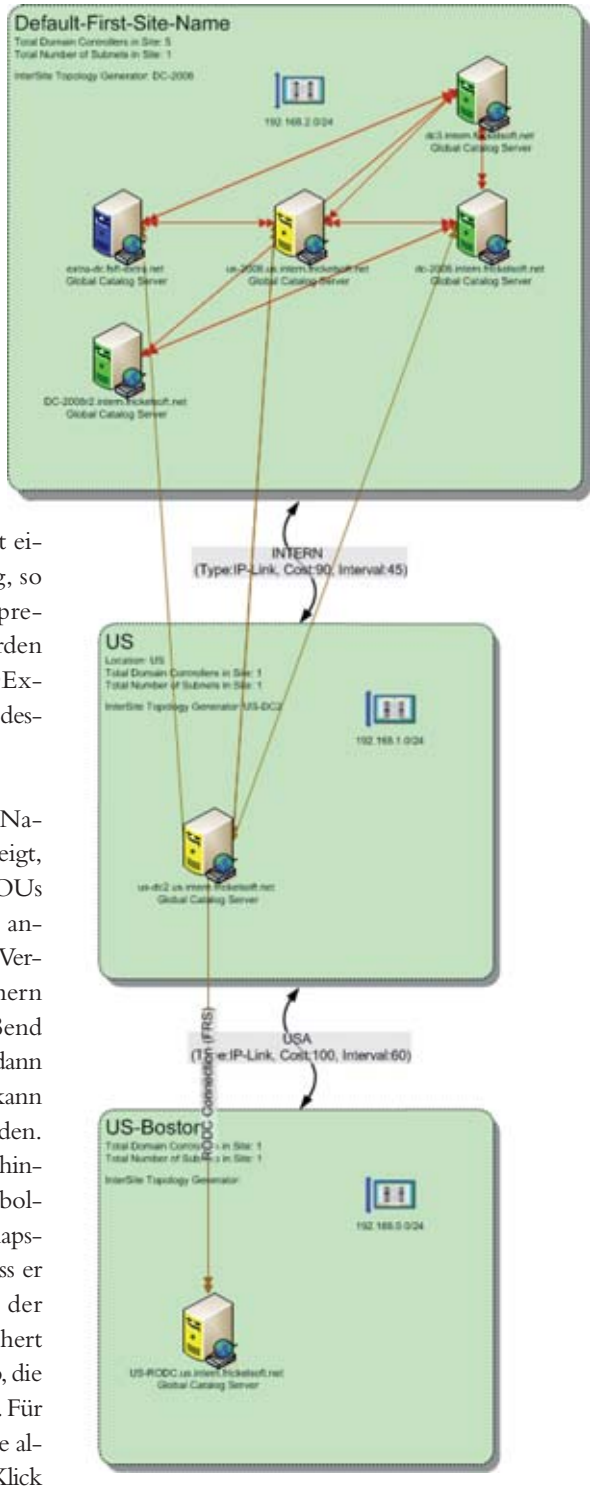


Bild 4: ADTD stellt unterschiedliche Standorte und ihre Verbindungen dar. DCs gleicher Domänen sind farblich gleich markiert.

Ihr Schutz sollte ähnliche Priorität wie der der AD-Datenbank selbst erfahren. Der fertige DAT-Dump kann nun, beim nächsten Start des Tools oder über die "Connect"-Schaltflächen geladen werden.

Vergleiche erstellt ADExplorer stets nur zwischen Snapshots. Das Tool ist nicht in der Lage, die Live-AD-Datenbank mit einem gespeicherten Snapshot zu vergleichen. Die "Compare"-Menüoption und das Lupensymbol mit zwei Textdateien sind nur anwählbar, wenn Sie im Startfenster die Option zum Laden eines Snapshots auswählt haben. Nach Auswahl von "Compare" öffnet "Compare Snapshots" den Vergleich. Hier wählen Sie nicht nur den zweiten Snapshot für den Vergleich, sondern justieren die zu vergleichenden Objekte und deren Attribute. Liegen zwischen den beiden Snapshots einige AD-Veränderungen – interessant sind aber nur ausgewählte Objekte und Attribute – können Sie diese per "Select all", "Clear all" oder per Einzelauswahl aktivieren. Mit dem Klick auf "Compare" erstellt ADExplorer den Bericht. Es stellt dabei gefundene Differenzen textuell heraus und beschreibt Differenzen mit "Attribute differs", "Attribute missing in first" oder "Attribute missing in second".

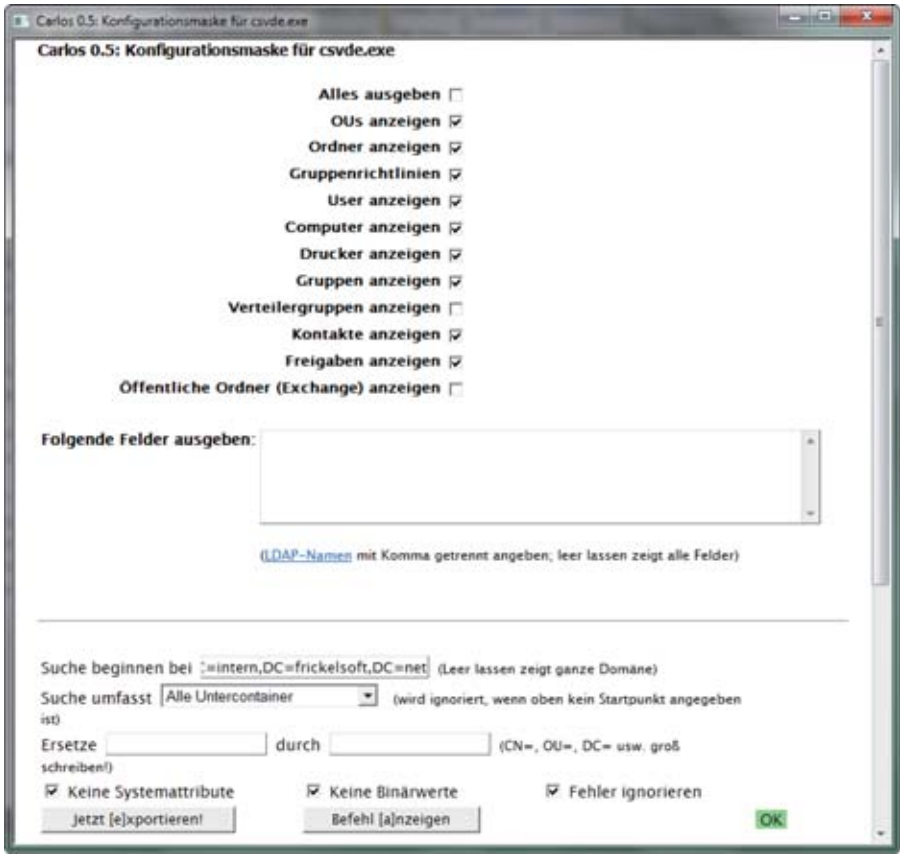


Bild 5: Skriptkenntnisse sind für CSVDE nicht notwendig – die Konfiguration der Kommandozeile übernimmt Carlos

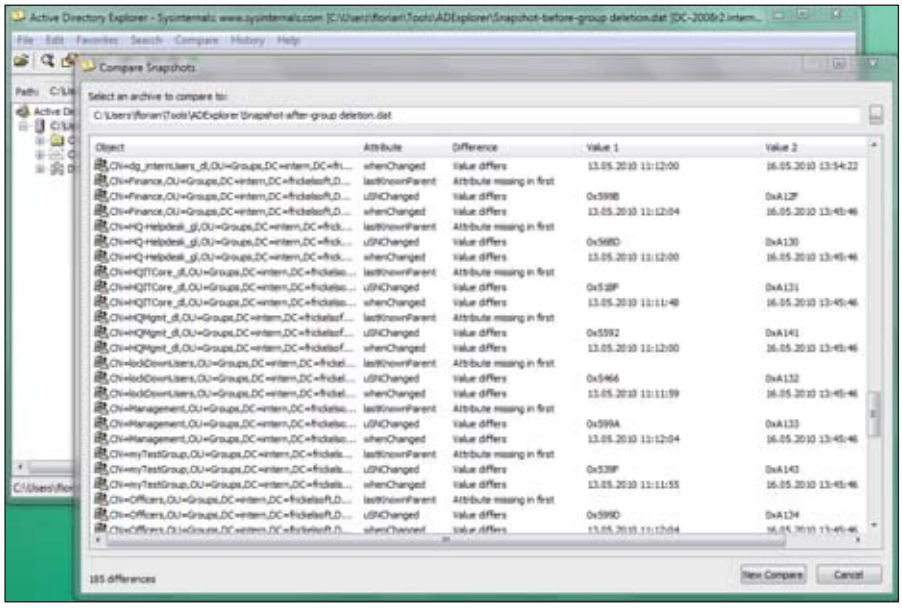


Bild 6: ADExplorer erstellt Snapshots von AD-Zuständen.
Auf Wunsch vergleicht es zwei Schnappschüsse miteinander und stellt Differenzen heraus.

Anpassung an die Anforderungen

Die Reporting- und Berichtsfunktionen für das AD sind vielfältig. Letztlich ist jeder mit ein wenig Programmier- oder Skriptingerfahrung in der Lage, gesuchte Daten zu extrahieren und sie in gewünschter Form auszugeben. Die Zahl der verfügbaren Tools ist kaum zu bändigen. Die wichtigste Frage stellt sich aber stets vor der Evaluation eines geeigneten Tools: Welche Daten sollen exportiert werden und wofür sollen sie genutzt werden? Aus dem gewünschten Nutzen der Daten ergibt sich dann das Einsatzszenarios der Werkzeuge – und letztlich daraus die Wahl der Tools, die für das Sammeln der Daten in Frage kommen. *(jp)*

[1] Active Directory Topology Diagrammer (ADTD)
http://www.microsoft.com/downloads/details.aspx?FamilyID=cb42fc06-50c7-47ed-a65c-862661742764&displaylang=en

[2] ADExplorer von Sysinternals
http://technet.microsoft.com/de-de/sysinternals/bb963907.aspx

[3] José: Active-Directory-Dokumentation
http://www.faq-o-matic.net/2010/05/26/jos-version-3-0-ist-da/

[4] Carlos: Konfigurationsmaske für csvde.exe
www.faq-o-matic.net/2003/07/25/carlos-konfigurationsmaske-fuer-csvde-exe/

Links


Quelle: Pixelio.de

LDAP und Active Directory

Den Wald vor lauter Bäumen sehen

Das Active Directory ist ein LDAP-Verzeichnisdienst. An vielen Stellen lässt sich die tägliche Arbeit als Administrator mit LDAP-Abfragen vereinfachen. Wie Sie die erstellen und damit in Verwaltungsoberflächen oder Skripten hantieren, zeigt dieser Beitrag. Der Workshop erklärt darüber hinaus die LDAP-Struktur und wie Suchvorgänge im Verzeichnisbaum funktionieren.

In den verschiedenen Artikeln dieses Sonderheftes führten wir eine Reihe von Begriffen für das Active Directory (AD) und seine Datenspeicher ein. Neben dem AD, dem Verzeichnis und Verzeichnisdienst, stellten wir auch die *NTDS.DIT*, die flache "Verzeichnisdatenbank" vor. Wie andere Verzeichnisse auch operiert das AD nach dem X.500-Verzeichnisstandard und beinhaltet einen LDAP-Server, über den Lese- und Schreibaktionen an der Datenbank durchgeführt werden. In den Domänencontrollern (DC) sind Interaktionen mit dem AD über diese Schnittstelle implementiert. LDAP (Lightweight Directory Access Protokoll) bestimmt, welcher Struktur Anmeldungen und Modifikationen am Verzeichnis folgen müssen und definiert grundlegende Formen, in denen Objekte erreicht und gefunden werden.

Die LDAP-Struktur

In einem LDAP-Verzeichnis beruht alles auf Objekten und Attributen, die einem definierten Schema folgen. Objekte werden in vielfältigen Relationen zueinander abgespeichert, etwa die hierarchische Struktur von Organisationseinheiten, die Benutzerobjekte enthalten und einem Domänenobjekt unterstellt sind. Somit entsteht eine logische Baumstruktur, aber auch Beziehungen der Objekte untereinander (Benutzer zu Gruppe, Manager zu Mitarbeiter) lassen sich darstellen. Die Baumstruktur innerhalb des LDAP-Verzeichnisses wird dadurch auf den zweiten Blick betrachtet deutlich komplexer als die Darstellung der Objekte in "Active Directory-Benutzer und -Computer". Zudem sind die Objekte ineinander verzahnt, um Datenkonsistenz und Verknüpfungen wie etwa Gruppenmitgliedschaften abzubilden.

Der Baum des Verzeichnisses lokalisiert alle Objekte eindeutig über ihren "DistinguishedName" (DN). Dieser setzt sich aus einer "Typbeschreibung" und "Werten" jedes Knotens im Navigationsbaum über dem gewünschten Objekt zusammen. Die im AD verwendeten "Typbeschreibungen" sind

- cn: für "Common Name", dies ist die gebräuchlichste Beschreibung
- ou: für "Organisatorische Einheiten"
- dc: für "Domain Component" – ein Teilname der Domäne

Ein Beispiel für einen Distinguished Name ist also "cn=Ulf B. Simon-Weidner,ou=Muenchen,ou=Benutzer,dc=firma,dc=de". Wie zu erkennen ist, liegt das Benutzerobjekt in der "OU München", welche unterhalb der "OU Benutzer" in der Domäne "firma.de" angesiedelt ist.

Attribute sind die Eigenschaften, die ein Objekt ausmachen – genau genommen sind Objekte eine Reihe schemadefinierter Attribute. Typische Attributbeispiele für das Benutzerobjekt sind der Vorname, Nachname, der Logonname, der Security-Identifyer, die Adresse und das Benutzerpasswort. Das Schema stellt den Bauplan dar, anhand dessen neue Objekte im Verzeichnis erstellt werden. Im Schema sind alle Attribute und Objekte definiert. Es hält außerdem fest, aus welchen Attributen ein Objekt besteht, welche Attribute unbedingt für die Existenz des Objektes notwendig sind und welche optional mit Werten befüllt werden.

All diese Informationen werden in der Active Directory-Datenbank gespeichert. Eine Datenbank erfüllt ihren Zweck nicht, wenn sie lediglich Daten aufnimmt, sie aber keinerlei Möglichkeit bietet, diese gezielt oder nach geforderten Kriterien gefiltert auszugeben. Die Betonung liegt hierbei auf "gezielt", da eine Ausgabe aller Daten der Datenbank nur in den allerwenigsten Fällen wirklich gewünscht ist. Eine weitere Anfor-

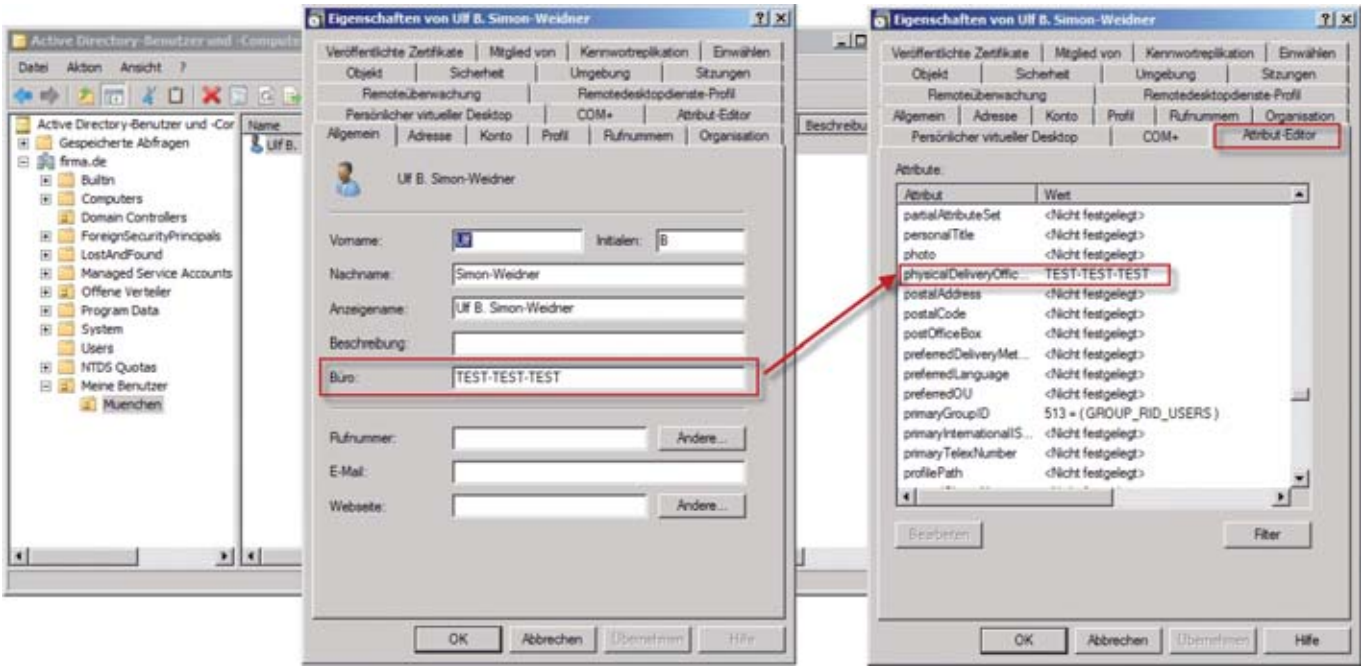


Bild 1: Der Attribut-Editor in "Active Directory-Benutzer und -Computer" hilft, die LDAP-Namen herauszufinden

derung an eine Datenbank ist, nicht nur alle Daten anzuzeigen, sondern auch eine kleine Auswahl der Daten, basierend auf Kennwerten oder Schlagworten. So interessiert sich ein Lagerist in der Inventardatenbank möglicherweise nur für Schrauben der Maximallänge von 5 Zentimetern mit Kreuzschlitz – alle anderen Schraubenarten aus dem Lager möchte er nicht betrachten. In LDAP können Sie derartige Suchfilter erstellen.

Suchen in LDAP

In Verbindung mit dem LDAP-Server und den Suchmöglichkeiten des LDAP-Protokolls können Anwendungen und Benutzer selbst im Active Directory nach Objekten im Verzeichnis suchen – und dabei Attribute als eingrenzende Kriterien angeben, um gezielt Objekte als Suchresultate zu erhalten. Die technische Lösung dahinter ist die LDAP-Suche. Die LDAP-Suche ist das effizienteste Medium, um Active Directory per Skript, Kommandozeile und PowerShell oder in einer Anwendung zu durchsuchen. Die Suche selbst basiert auf drei Basisinformationen, die zwingend für die Suche angegeben werden müssen und einem optionalen Satz an Attributen, die für die gefundenen Objekte als Resultat ausgegeben werden sollen. Die Basisinformationen sind:

- Der Basis-DN/Start-DN: Der Basis-DN teilt dem LDAP-Server mit, von welchem Objekt aus die Suche gestartet werden soll.
- Der Suchbereich ("Scope"): Der Scope der Suche teilt dem LDAP-Server mit, wie weit die Suche ausgehend vom Start-DN gehen soll, um Ergebnisobjekte zu finden. Hier sind drei Werte möglich: "Base", das den LDAP-Server anweist, nur das Startobjekt zu betrachten, "One Level", das das Startobjekt und die direkt darunter liegenden Objekte betrachtet und "Subtree", dass alle Objekte, ausgehend vom Start-DN durchsucht. Suchen Sie nach Benutzern aus der Marketing-OU wählen Sie "One Level", um mögliche weitere Unter-OUs von Marketing, etwa "Praktikanten", auszuschließen. Sind auch Praktikanten für die Suche in Marketing interessant, wählen Sie "Subtree", um auch Sub-OUs und alle folgenden, verschachtelten OUs innerhalb von Marketing zu durchforsten.
- Der Suchfilter: Der Suchfilter, oder LDAP-Filter, schränkt die Suche der Objekte ein. Anhand des Suchfilters wählen Sie aus, welche Eigenschaften der Satz von Ergebnisobjekten filtern soll. Suchfilter sind, in deutscher Sprache formuliert, nach einem einfachen Muster aufgebaut: "Finde alle Benutzerobjekte, deren Gehalt größer als 50.000 ist und die der Abteilung Praktikanten zugeordnet sind.

Arbeiten mit LDAP-Filtern

Bevor Sie die erste LDAP-Suche ausführen, sollten Sie den Suchfilter genauer betrachten. LDAP-Suchfilter sind in der Form "(Attributname <Operator> Vergleichswert)" aufgebaut, wobei die beiden runden Klammern von manchen LDAP-Applikationen zwingend gewünscht, von anderen als nicht wichtig erachtet werden. Die generelle Empfehlung hier lautet, die Klammern so gut es geht mitzuführen. In späteren Beispielen, die deutlich umfangreicher als diese kleinste Filterform sind, dienen uns die Klammern auch als Strukturierung mehrerer Bedingungen.

Der Attributname muss einem Attribut aus dem AD-Schema entsprechen. Für die zuvor genannten Beispiele "Gehalt" und "Abteilung" sind dies die Attribute "sala-

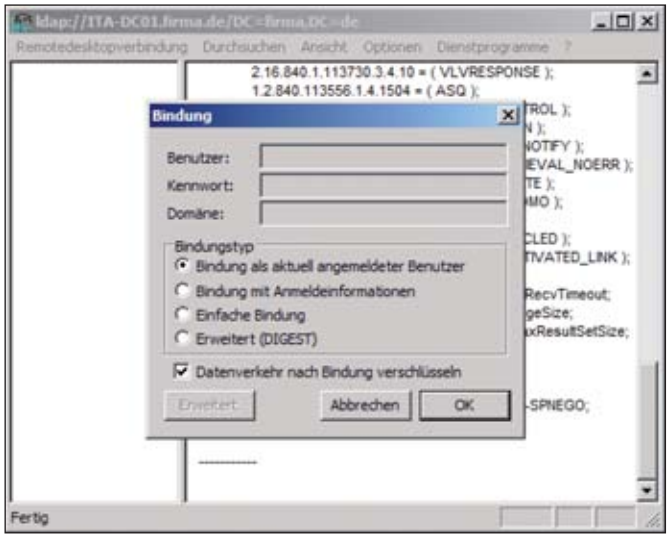


Bild 2: Die LDAP-Suche auf einem Domänencontroller erfordert eine Authentifizierung mittels *LDP.exe*

ryInfo" und "department". Der Vorname ist beispielsweise im Attribut "givenName" gespeichert, der Nachname im Attribut "sn". Um eine Liste der Attribute zu erhalten, sollten Sie entweder in MSDN [1] nach dem richtigen Namen suchen oder ein Referenzobjekt mit dem ADSIEdit-Werkzeug (oder dem Attribut-Editor bei Windows Server 2008 R2) untersuchen. ADSIEdit zeigt die korrekten LDAP-Attributnamen an, in denen Werte gespeichert werden. Ein Referenzobjekt lässt sich so mit Hilfe von "Active Directory-Benutzer und -Computer" mit einem Beispielwert versehen und anschließend mit dem Attribut Editor oder ADSIEdit untersuchen. Der Attribut-Editor in Active Directory-Benutzer und -Computer erscheint in den Eigenschaften jedes Objektes, wenn Sie die Ansicht "Erweiterte Features" einschalten.

In der Suchabfrage dient der Operator dem Vergleich von Werten. Neben dem Istgleich-Zeichen ("=") existieren weitere Operatoren wie "kleiner oder gleich" ("<=") und "größer oder gleich" (">="). Ein reines "Größer" oder "Kleiner" ohne den "oder gleich"-Teil kennt LDAP nicht. Die Größergleich/Kleinergleich-Logik lässt sich sowohl für Text- als auch für Zahlensuchen anwenden. Suchen Sie alle Mitarbeiter, deren Vorname (= givenname) mit M oder später beginnt, formulieren Sie die Suche mit "givenname>=M*".

Der Vergleichswert stellt den eigentlich zu suchenden Zielwert dar. Valide Eingaben für Vergleichswerte sind Zahlen oder Buchstaben, ganze LDAP-Pfade oder der Stern als Joker. Für die einfache Suche nach Gehältern größer 50.000, nutzen Sie den folgenden, einfachen LDAP-Filter: *(salaryInfo >= 50000)*. Suchen Sie nach Objekten, deren Vorname "Martin" lautet, erreichen Sie dies mit *(givenName = Martin)*. Um außer Martin auch Frauen mit dem Vornamen "Martina" einzuschließen, verwenden Sie den Joker *(givenName = Martin*)*. Die Sternvariante ist allerdings mit Vorsicht zu genießen, da außer Martin und Martina auch weitere Mitarbeiter, etwa Martino, von dieser Suche gefunden werden.

LDAP-Filter mit mehreren Bedingungen

Da nur sehr selten nach einem einzigen Kriterium gesucht wird und das Ziel einer Suche die Einschränkung auf möglichst genaue Resultate sein muss, reicht die bisherige Suchlogik nicht aus. Sollen Benutzer nach dem obigen Beispiel eingeschränkt auf das Gehalt und die Abteilung ausgegeben werden, benötigt der LDAP-Filter mehrere Bedingungen, die Sie aneinander knüpfen müssen:

```
(&(salaryInfo>=50000)(department=
  "Praktikanten"))
```

Der LDAP-Filter ist beträchtlich gewachsen. Aus einer Bedingung sind zwei entstanden, die Sie durch ein logisches "Und" ("&") verknüpfen. Die ganze Logik wird erneut durch umfassende Klammern zusammengehalten. Dieser Suchfilter zeigt nur Objekte an, die beide Attributeinschränken erfüllen. Möglich ist auch das Hinzufügen weiterer Einschränkungen:

```
(&(salaryInfo>=50000)(department=
  "Praktikanten")(givenName=Martin))
```

Suchfilter live einsetzen

Mit der bisher gezeigten Logik können Sie die ersten Suchen starten. Um eine Sucheanfrage an das Active Directory abzuschicken, benötigen Sie einen LDAP-Client. Ein sehr bekannter LDAP-Client hierfür ist *LDP.exe*, der in Windows Server 2008 mitgeliefert wird. Für frühere Windows-Versionen muss er mit den Support-Tools installiert werden. Das Werkzeug öffnet zunächst eine Verbindung per "Remotedesktopverbindung / Verbinden". Wenn Sie die Zeile "Server" leer lassen, verwendet das Werkzeug den aktuellen Domänencontroller. Anschließend verlangt der LDAP-Server, dass eine Anmeldung stattfindet – dies geschieht per "Remotedesktopverbindung" und

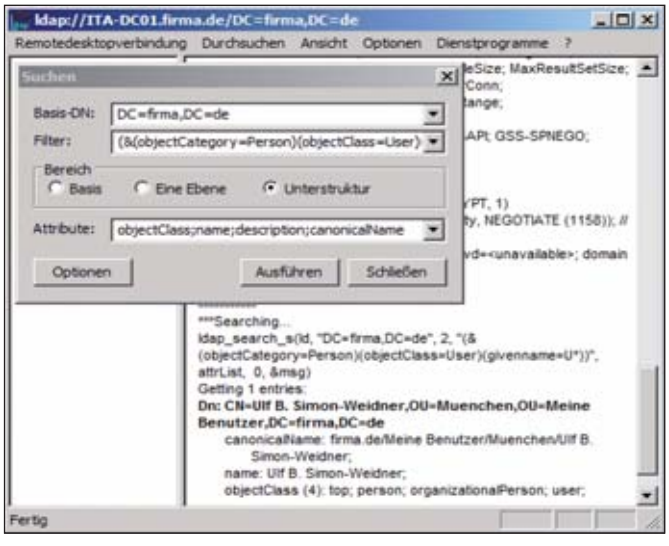


Bild 3: LDP ist ein LDAP-Browser, mit dem Sie LDAP-Suchen absetzen

"Gebunden" (leider ist die Übersetzung des Tools etwas gewöhnungsbedürftig). Den Erfolg meldet LDP in der rechten Spalte im Ergebnisfenster.

Im Menü unter "Durchsuchen / Suchen" befindet sich die Suchmaske für LDAP-Suchen. LDP verlangt die drei zuvor genannten Informationen, Basis-DN, Filter und Suchweite (= Bereich) als Eingaben, bevor die Suche starten kann. Optional legen Sie die Attribute fest, die Sie von den gesuchten Objekten anzeigen möchten. Die Vorauswahl der Suchweite ist "Eine Ebene" (= One Level), Sie sollten diese aber für erste Suchzwecke auf "Unterstruktur" (= Subtree) ändern, damit Sie nützliche Ergebnisse erhalten.

Zum Beispiel können Sie eine Suche nach allen Benutzern im Verzeichnisdienst durchführen, deren Vorname mit "U" beginnt. Hierfür wählen Sie für den Basis-DN die Domäne (zum Beispiel "DC=firma,DC=de") und geben den folgenden Filter ein:

```
(&(objectCategory=Person)(object-
  Class=User)(givenName=U*))
```

Setzen Sie den Bereich auf "Unterstruktur" und stoßen nun die Suche mit "Starten" an, zeigt LDP die Ergebnisse der Suche im rechten Ergebnisfenster an. Im Suchfenster unter "Attribute" geben Sie optional die Attribute an, die LDP für diese Sucherergebnisse auflisten soll. Die Voreinstellung zeigt bereits eine Reihe von Attributen an. Dies wird schnell unübersichtlich, wenn die Suche mehrere Ergebnisse findet. Eine Einschränkung auf wesentliche, interessante Attribute erhöht die Übersichtlichkeit.

Benutzer und Computer unterscheiden

In einem der häufigsten Suchszenarien sucht der Administrator nur bestimmte Objekttypen im Verzeichnis. In seltenen Fällen sind sowohl Benutzer-, Computer- als auch Druckerobjekte innerhalb der gleichen Abfrage gleichermaßen interessant, so dass Sie zwischen den sogenannten "Objektklassen" unterscheiden müssen. Auch dies ist mit einem LDAP-Filter möglich – das korrekte Attribut hierfür ist "objectClass".

Erstaunlich ist allerdings, dass eine Suche nach *(objectClass=user)* nicht nur Benutzerkonten zu Tage fördert, sondern auch Computerkonten. Das Ergebnis der Suche ist jedoch kein Fehler im LDAP-Server von Microsoft, sondern eine Funktion. Denn das Objektmodell von LDAP ist ebenfalls, wie alle Objekte im Verzeichnis, in einer Hierarchie strukturiert. Als Mutter aller Objekte ist das Objekt "top" definiert, aus dem sich weitere Kindsobjekte ableiten. Kindsobjekte von "top" besitzen alle Attribute, die "top" auch besitzt – und können eigene, weitere Attribute definieren, um so besondere Eigenschaften zu entwickeln. Ein Kindsobjekt von "top" namens "person" bringt ein weiteres Kindsobjekt namens "organizationalPerson" hervor, aus dem "user" entsteht – ein "user"-Objekt leitet sich demnach aus den Objekten "top", "person" und "organizationalPerson" ab, und bringt, außer den von den Vaterobjekten definierten Attributen, weitere, eigene mit.

Die Besonderheit am Computerobjekt ist simpel: die LDAP-Objektstruktur definiert Computerobjekte als Kindsobjekte der Objektklasse "user". Somit sind Computerobjekte in AD spezielle "Benutzer"-Objekte mit weiteren, eigenen Attributen. Das macht in der Tat Sinn: Ähnlich wie herkömmliche Benutzer besitzen Computer ein Konto, können sich an der Domäne authentifizieren, wechseln ihr Passwort von Zeit zu Zeit und greifen auf Ressourcen zu. Computer sind für das AD in Wirklichkeit nur sehr spezielle Benutzer. Für die Unterscheidung von Benutzern und Computer müssen Sie also ein weiteres Attribut zu Rate ziehe: "objectCategory". Die Objektkategorie separiert eigentlich ähnliche Objekte und lässt Benutzer von Computern unterscheiden. Nur-Benutzer-Suchen benötigen demnach folgenden Suchfilter:

```
(& (objectClass=user)
  (objectCategory=person) )
```

Suchfilter mit ODER-Verknüpfungen

Neben der UND-Verknüpfung können Sie Attribute auch per ODER-Verknüpfung miteinander verbinden, damit LDAP-Filter flexibel auf Alternativen reagieren. Das zuvor gewählte Beispiel für die Suche nach Martin und Martina als Vornamen von Benutzern sieht mit einer ODER-Verknüpfung anstatt dem Jokerzeichen wie folgt aus:

```
(|(givenName=Martin)(givenName=
  Martina))
```

Einen Haken hat diese Suche weiterhin: Sie zeigt auch Kontaktobjekte aus dem AD an, die Sie sich möglicherweise nicht im Ergebnissatz wünschen. Es soll also zusätzlich nur nach Benutzerobjekten gefiltert werden, was den Filter ein wenig aufbläht:

```
(&(objectClass=user)
  (objectCatego-ry=person)
  (|(givenName=Martin)
  (givenName=Martina)))
```

Einzeln betrachtet ist die Abfrage einleuchtend: Bestehen bleibt die ODER-Abfrage nach Martin oder Martina als Vornamen der Objekte. Was zusätzlich hinzukommt, ist die Abfrage nach Benutzerkonten. Es wird also nach folgendem gesucht: Alle Objekte, deren Objektklasse "user" entspricht UND deren Objektkategorie "person" entspricht UND deren Vorname "Martin" oder "Martina" ist. Die ODER-Verknüpfung von Martin und Martina ist ein weiteres Glied der "UND"-Verknüpfung des ersten Teiles des Filters.

Suche mit Stern

Zusätzlich zu den UND-/ODER-Verknüpfungen haben wir den Stern als Jo-

kerzeichen kennengelernt. Der Stern kann sowohl am Ende, als auch am Anfang und in der Mitte des Suchwortes stehen:

```
(givenName=Martin*) oder
  (givenName=*tin) oder
  (givenName=Mar*n)
```

Eine Besonderheit ist der Stern als Jokerzeichen ohne Buchstaben. Hier wird nach allen Objekten gesucht, die für das angegeben Attribut einen Wert zugewiesen haben. Objekte, die für das betroffene Attribut keinen Wert, somit "NULL" in der Datenbanksprache oder "not set" für AD aufweisen, werden von der Suche ausgeschlossen.

Um die boolsche Logik für LDAP-Suchen fast zu komplettieren, existiert der Nicht-Operator in Form des Ausrufezeichens. Attribute, die nicht einem gewünschten Wert entsprechen sollen, werden mit einem anführenden Ausrufezeichen angegeben: *(!givenName=Martin)*. Objekte, die keinen Attributwert, in diesem Beispiel "Vorname", zugewiesen bekamen und somit "NULL" oder "not set" sind, lassen sich so finden: *(!givenName=*)*.

Suchen mit Jokerzeichen am Anfang oder in der Mitte, sowie Suchen mit einer Negierung, sollten Sie wenn möglich vermeiden. Diese Suchen sind im Allgemeinen nicht sehr performant, beschäftigen also den Domänencontroller recht lange, weil er eine Vielzahl von Objekten untersuchen muss. Wie in Datenbanken gibt es im AD die Möglichkeit der Indizierung, und sollten solche Suchen wirklich häufig der Fall sein, weil eine bestimmte Applikation eingesetzt wird, wäre ein entsprechenden Index, der diese Suchen unterstützt, sinnvoll.

Filtern und suchen mit DSquery

Seit Windows Server 2003 gibt es das DSquery-Kommando. Mit der Syntax

```
dsquery * <base-dn> -Filter
  "(&(..)()..))" -scope subtree
  [-attr givenname sn]
```

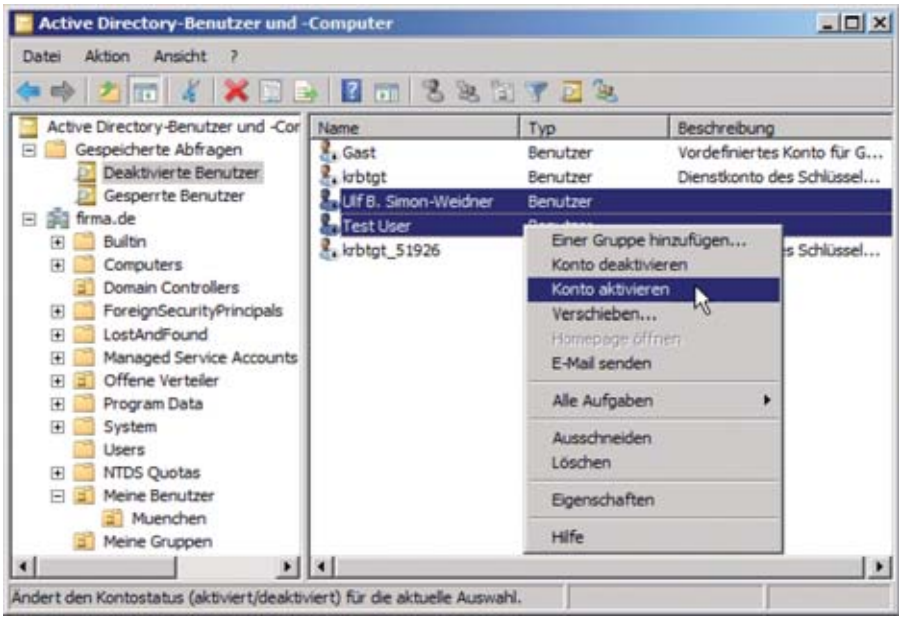


Bild 4: Deaktivierte oder gesperrte Konten – mit gespeicherten Abfragen in "Active Directory-Benutzer und -Computer" finden Sie "Problemkonten"

erstellen Sie beliebige LDAP-Suchen. Den Base-DN können Sie in diesem Kommando auch auf "domainroot" oder "forestroot" setzen, wenn Sie "-scope" nicht setzen. Verwenden Sie "subtree" und "-attr" ist nicht angegeben, erhalten Sie den distinguishedName zurück. Damit setzen Sie das Beispiel von vorhin auf der Kommandozeile wie folgt um:

```
dsquery domainroot -filter
 "(&(objectClass=user)(object
 Category=person)
 (|(givenName=Martin)
 (givenName=Martina)))"
```

Zusätzlich gibt es noch spezielle Filter, um sogenannte Binäre-Suchen zu unterstützen. Der folgende Filter sucht zum Beispiel nach allen Benutzerkonten, bei denen das zweite Bit von userAccountControl gesetzt ist – dieses Bit markiert deaktivierte Benutzerkonten:

```
(&(objectClass=user)
 (objectCategory=person)
 (userAccountControl:1.2.840.
 113556.1.4.803:=2))
```

Durch die spezielle OID in Doppelpunkten zwischen dem Attribut und den gesuchten Wert weiß das AD, dass es seine binäre UND-Verknüpfung durchführen soll, also wenn "userAccountControl AND 2" einen Wert ergibt (also das Bit mit dem Dezimalwert "2" gesetzt ist).

Eine deutlich erweiterte Abfrage kann die Hierarchien und Verschachtelungen im AD aufbrechen. Über die spezielle "LINKED_IN_CHAIN_OID 1.2.840.113556.1.4.1941" stellen Sie zum Beispiel auch verschachtelte Gruppenmitgliedschaften fest. Die folgende Abfrage liefert ein Ergebnis, wenn der Benutzer Ulf rekursiv Mitglied in der Gruppe "Bereich Technologie" ist (tatsächlich ist er Mitglied der Gruppe Consulting, die wiederum Mitglied der Technologie-Gruppe ist):

```
dsquery * "cn=Bereich
 Technologie,ou=Meine
 Gruppen,dc=firma,dc=de" -Filter
 "((member:1.2.840.
 113556.1.4.1941:=cn=Ulf B. Simon-
 Weidner,ou=Muenchen,ou=Meine Be-
 nutzer,dc=firma,dc=de))"
```

Mit folgendem Befehl überprüfen Sie alle Gruppen, in denen unser Benutzer direkt oder auch rekursiv Mitglied ist:

```
dsquery * domainroot -Filter
 "((member:1.2.840.113556.
 1.4.1941:=cn=Ulf B. Simon-Weid-
 ner,ou=Muenchen,ou=Meine Benut-
 zer,dc=firma,dc=de))"
```

Bei mehreren Domänen müssen Sie dieses Kommando allerdings auch gegen einen Domänencontroller jeder Domäne ausführen, um korrekte Ergebnisse zu erhalten (bestimmte Gruppen können nicht domänenübergreifend gefunden werden).

Gespeicherte Abfragen

Besonders nützlich sind LDAP-Filter in der Kombination mit gespeicherten Abfragen. Sie können diese in "Active Directory-Benutzer und -Computer" erstellen, speichern und danach jederzeit wiederverwenden. Die geschickte Erstellung von LDAP-Filtern erspart viel Zeit in der täglichen Administration und außerdem viel Skriptarbeit.

In "Active Directory-Benutzer und -Computer" existiert ein Knoten über dem Domänenobjekt namens "Gespeicherte Suchen". Per Rechtsklick auf den Knoten und Auswahl von "Neu" und "Suche" öffnen Sie den "Neue Suche"-Dialog. Im Namensfeld tragen Sie dann ein entsprechenden, beschreibenden Name ein. Über den Knopf "Suche definieren" hinterlegen Sie die eigentliche, zu speichernde Suche. Per Vorgabe ist hier "Gemeinsame Suchen" ausgewählt. Das Auswahlfeld bietet dabei eine Reihe von Optionen, aus denen Sie die Suchen zusammenstellen. Interessant für LDAP-Experten ist die Auswahl von "Benutzerdefinierte Suche". Entweder über die Auswahl des Attributes in "Feld" und dem Zusammenbauen der Abfrage oder per manueller Eingabe im "Erweitert"-Reiter lässt sich die Abfrage zusammenstellen.

Um eine für den Alltag nützliche Suche zu definieren, soll das System nach ausgesperrten Benutzern suchen. Signifikant für ausgesperrte Benutzer ist das Attribut "lockOutTime", das einen Wert größer 0 annimmt, sobald ein Account gesperrt ist:

```
(&(objectClass=user)(userCatego-
ry=person)(lockOutTime>=1))
```

Wichtig für die Arbeit mit gespeicherten Suchen ist, dass das gesamte Query von Klammern umschlossen wird – sonst verhält sich der Dialog seltsam und versucht, die Suche selbstständig zu komplettieren – meist mit wenig Erfolg. Mit "OK" speichern Sie die Suche. Diese ist dann unter dem Knoten "Gespeicherte Suchen" verfügbar.

ANR für Sammelsuchen verwenden

Das Active Directory kennt eine ganz spezielle Suchart, die vor allem AD-Konsumenten wie Outlook oder Exchange verwenden. Die Rede ist von der sogenannten "Ambiguous Name Resolution"-Suche. Die Idee dahinter ist clever: Alle Attribute, die relevant sein können für eine generische Suche, werden unter Verwendung eines Pseudo-Attributes angestoßen. Nützlich ist das, wenn bei der Suche nach Objekten ein Schlagwort bekannt ist, das betreffende Attribut, in dem sich das Schlagwort befinden könnte, jedoch nicht. Die Suche nach "Johann" könnte einen Vornamen meinen, einen Benutzeraccount für den Benutzer "Joachim Hann" oder eine Adresse wie "Johann-Krüger-Allee".

Das Pseudo-Attribut heißt treffend "anr" und wird wie folgt verwendet: *(anr=Johann)*. Bei einer Windows Server 2008-Installation ist dies gleichbedeutend mit der folgenden Suche:

```
(|
(displayName={suchbegriff}*)
(givenName={suchbegriff}*)
(legacyExchangeDN={suchbegriff}*)
(msDS-AdditionalSamaccountName=
  {suchbegriff}*)
(msDS-PhoneticCompanyName=
  {suchbegriff}*)
(msDS-PhoneticDepartment=
  {suchbegriff}*)
(msDS-PhoneticFirstName=
  {suchbegriff}*)
(msDS-PhoneticLastName=
  {suchbegriff}*)
(physicalDeliveryOfficeName=
  {suchbegriff}*)
(proxyAddresses={suchbegriff}*)
(name={suchbegriff}*)
(sAMAccountName={suchbegriff}*)
(sn={suchbegriff}*)
)
```

Welche Attribute für den ANR hinzugezogen werden, definiert sich über eine entsprechende Schemaeinstellung. Aus diesem Grund kann der ANR, falls Exchange oder andere Schema-Erweiterungen installiert wurden, größer oder geringer ausfallen. *(jp)*

Die LDAP-Schreibweise verstehen

Die LDAP-Pfadschreibweise ist für die Suche über LDAP-Server essentiell und wichtig zu verstehen. Grundsätzlich orientiert sich die Schreibweise am Baum des Verzeichnisdienstes in umgekehrter Reihenfolge. Das Domänenobjekt, das im Baum an oberster Stelle steht, wird im Pfad am Ende angegeben. Getrennt werden die einzelnen Pfadkomponenten mit Kürzeln, die den Objekttyp angeben sollen. "DC" steht für "Domain Component" und gibt die Domäne an, "OU" steht für "Organizationalunit", "CN" prinzipiell für Container, wobei Benutzer und Computer hier wie Container behandelt werden.

Getrennt werden die einzelnen Komponenten mit dem Komma als Separator. Die Domäne "contoso.com" wird in" LDAP-Schreibweise als "DC=contoso,DC=com" angegeben. Der Benutzer "Tom Bauer" in der OU "Produktion" direkt unter dem Domänenobjekt erhält den LDAP-Pfad "CN=Tom Bauer,OU=Produktion,DC=contoso,DC=com". Ein weiter verschachteltes Benutzerobjekt von "Tina Kruse", die in der Projekt-OU "TV" der "Werbung"-OU im Marketing zu finden ist, wird mit "CN=Tina Kruse,OU=TV,OU=Werbung,OU=Marketing,DC=contoso,DC=com" angegeben.

Für Verwirrung sorgt in den meisten Fällen die Angabe der Komponenten in umgekehrter Reihenfolge. Der Verzeichnisbaum wird sozusagen vom anzugebenden Objekt den Ästen entlang bis zum Domänen-Wurzelobjekt aufgerollt und im Pfad angegeben.

Active Directory und DNS

Eine Hand wäscht die andere

DNS ist eine grundlegende Infrastrukturkomponente in einem Active Directory-basierenden Netzwerk. Active Directory benötigt DNS, um seine Dienste zu finden und zu veröffentlichen. Windows-integriertes DNS nutzt zudem das AD, um die Daten abzulegen. Im diesem Workshop gehen wir zum einen auf die Grundlagen von DNS ein, so dass Sie in der Lage sind, das DNS-Design und dessen Komponenten zu verstehen. Zum anderen betrachten wir die Integration des Active Directory in die DNS-Infrastruktur.

Der Domain Name Service (DNS) ist seit Windows 2000 mit der Einführung des Active Directory die Komponente für die Namensauflösung innerhalb von Windows-Netzwerken. Nicht nur die Namen von Clients und Servern, sondern vor allem auch Services innerhalb des Active Directory werden über die DNS-Namensauflösung gefunden.

Der DNS-Namensraum

An der Spitze des DNS-Namensraums steht eine fiktive "Internet Root" mit dem Namen "." (Punkt). Die sogenannten Top-Level-Domänen (TLD) wie ".com", ".net.", ".de" und so weiter sind fest definiert. Jedes Unternehmen, das einen öffentlichen DNS-Namen benötigt, kann sich seine Namen (soweit verfügbar) registrieren lassen. Dabei setzt sich der Name immer von unten nach oben in der Hierarchie zusammen. Ein kompletter DNS-Name, der alle Elemente bis zur Internet Root "." enthält, heißt "Vollqualifizierter Domänenname" (Full Qualified Domain Name, FQDN). Dabei ist zu beachten, dass der FQDN theoretisch immer mit dem "." der Internet Root abgeschlossen wird, also "www.it-administrator.de.". In der Praxis wird dieser häufig weggelassen (was je nach dem Auflösungsverhalten des DNS-Client zu zusätzlichen Anfragen führen kann).

Der erste Teil eines FQDN ist üblicherweise ein Hostname, also der Name eines Clients oder Servers. Welche Server für die Top-Level-Domänen zuständig sind, ist definiert und bekannt. Jeder Server, der für einen Namensraum verantwortlich (autoritativ) ist, verwaltet diesen Namensraum. Das heißt, dass er auch die Namen unter seinen Fittichen hat, die in der Hierarchie unterhalb der Wurzel seines Namensraums liegen.

Domänen und Zonen

Zwei Begriffe, die im Zusammenhang mit DNS immer wieder gebraucht werden, sind "Domänen" und "Zonen". Dabei ist es wichtig, den Unterschied zu verstehen: DNS-Domänen sind Strukturelemente – eine DNS-Domäne ist jeder Teil eines FQDN zwischen zwei Punkten (also jeder Teil, der nicht der Hostname ist). Sie dient daher nur der Unterteilung des Namensraums. Anders dagegen die DNS-Zone, die einen "administrativen Bereich" darstellt. Eine Zone kann separat von anderen Zonen verwaltet sowie auf verschiedene Server übertragen werden, und der Administra-

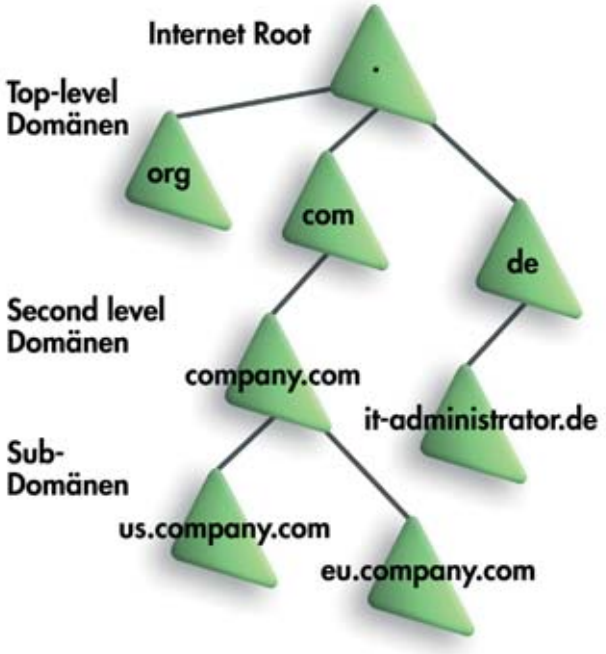


Bild 1: Ein Beispiel für die DNS-Namensräume

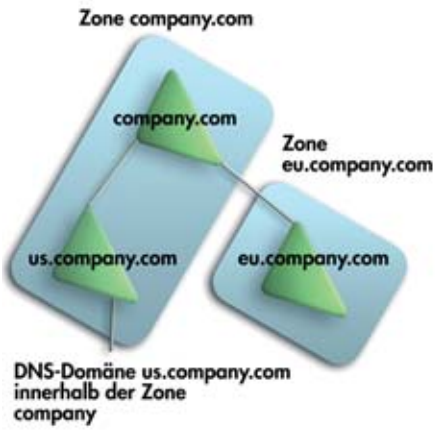


Bild 2: Zonen sind administrative Einheiten, die untergeordnete Domänen enthalten oder untergeordnete Namensräume an andere Zonen delegieren können

tor kann jeder Zone unterschiedliche Eigenschaften zuweisen. Dabei kann eine Zone auch weitere DNS-Domänen (unterhalb ihres Namensraums) beinhalten.

Um einen Namensraum zu erstellen, der einer Zone untergeordnet ist, lässt sich dieser aber auch von der Zone zu einer anderen Zone delegieren. Schließlich ist auch der Top-Level-Domänenname ".de." nur eine Zone. Ließe sich der Namensraum nicht an weitere Zonen delegieren, so müssten die Server für ".de." alle Namen verwalten, die unterhalb dieses Namensraums existieren. Auf die Delegation gehen wir später noch ein.

Innerhalb einer Zone liegen DNS-Einträge. Die folgenden Typen von Einträgen werden am häufigsten verwendet:

- Host-Einträge (A) beschreiben, welcher Rechner welche IP-Adresse hat, also "ITADC01 hat die IP-Adresse 192.168.100.1".
- Start-of-Authority-Einträge (SOA) beschreiben, welcher Server schreibend auf die Zone zugreifen darf und wie die Eigenschaften der Zone sind (wer ist administrativ für diese zuständig, wie lange sollen Einträge per Default in einem Zwischenspeicher/Cache gehalten werden).
- Nameserver-Einträge (NS) geben an, welche DNS-Server den Inhalt der Zone kennen. Im Gegensatz zu SOA können dies auch Server sein, die nur Auskünfte erteilen, aber nicht schreiben dürfen.
- Alias-Einträge (CNAME) legen alternative Namen fest, das heißt in der Zone *company.com.* könnte ein CNAME für WWW auf *INETSERVER1.firma.de.* stehen. Ein Client der *www.company.com.* anfragen würde, bekäme dann die Antwort, dass er stattdessen *INETSERVER1.firma.de* suchen soll.
- Service-Einträge (SRV) beschreiben, welcher Dienst auf welchem Server gefunden wird und enthalten weitere Informationen wie den verwendeten Port des Dienstes. Die Rollen im Active Directory wie Domänencontroller, Globaler Katalogserver et cetera können über SRV-Einträge gefunden werden.
- Pointer-Einträge (PTR) lassen sich als das Gegenteil von Host-Einträgen beschreiben. Ein PTR-Eintrag beschreibt, hinter welcher IP-Adresse welcher Hostname (als FQDN) steht.

Des Weiteren gibt es zahlreiche zusätzliche DNS-Einträge (wie der MX-Eintrag für Mailserver), aber für die DNS- und Active Directory-Struktur genügen die erwähnten Einträge.

Die Auflösung von Netzwerknamen zu IP-Adressen wird auch als "Forward-Lookup" bezeichnet. Allerdings gibt es auch Anwendungen, die eine IP-Adresse in den Netzwerknamen auflösen möchten. Hierzu gibt es den "Reverse-Lookup".

Reverse Lookup

Wenn wir uns an einen "normalen" FQDN im DNS erinnern, steht das "kleinste Element", der Hostname, ganz links am Anfang des Namens (etwa *Server1.company.com.* oder *www.it-administrator.de.*). Sehen wir uns IP-Adressen an, so steht das kleinste Element, das dem einzelnen Rechner zugeordnet ist, auf der rechten Seite (zum Beispiel, wenn Server01 die IP-Adresse 192.168.100.1 hat, entspricht die rechte 1 der Adresse des Server01 innerhalb des Netzwerks 192.168.100.x).

Um eine Auflösung von IP-Adressen zu Netzwerknamen über DNS zu ermöglichen, gibt es einen Trick. Es wurde eine fiktive Domäne "in-addr.arpa" eingeführt, und unter dieser können die IP-Adressen in umgekehrter Reihenfolge eingerichtet werden. Das Netzwerk 192.168.100.x hätte also die DNS-Zone 100.168.192.in-addr.arpa und innerhalb dieser Domäne werden dann die einzelnen IP-Adressen gepflegt.

Reverse-Lookup kann innerhalb eines Unternehmens von einigen Applikationen gefordert sein. Zum Beispiel ist es denkbar, dass diese überprüfen wollen, ob sie wirklich mit einem bestimmten Server kommunizieren. Unternehmensübergreifend ist Reverse-Lookup noch selten im Einsatz. Manchmal wird das Verfahren verwendet um, die Authentität von E-Mailservern zu überprüfen. So könnte ein Mailserver, der eine E-Mail von *it-administrator.de* erhält, überprüfen, ob die IP-Adresse des sendenden Mailservers tatsächlich dieser Domäne zugeordnet ist. Erst dann leitet er die E-Mail weiter. Sowohl für den Forward- wie auch für den Reverse-Lookup werden die Namensräume in Zonen verwaltet.

Zonentypen und Eigenschaften

Es gibt unterschiedliche Typen von Zonen mit verschiedenen Eigenschaften: **Primäre Zonen** dürfen Informationen in die Zone schreiben. Wenn Sie einen geänderten oder einen neuen Eintrag schreiben möchten, erfolgt dies in der Primären Zone. Im Allgemeinen darf es nur einen Server geben, der die Primäre Zone für einen Namensraum hält.

Sekundäre Zonen halten eine Kopie der Zone, die nur gelesen werden darf. Sekundäre Zonen erhalten Änderungen immer von einem anderen Server. Es kann beliebig viele Server geben, die eine Sekundäre Zone von einer Primären Zone halten. Damit eine Sekundäre Zone eine Kopie der Primären Zone erhalten kann, muss der Server definiert sein, der die Primäre Zone hält. Außerdem muss der Server, auf dem die Primäre Zone liegt, den Zonentransfer

auf die Server erlauben, die die Sekundäre Zone erhalten sollen. Dies können Sie in den Eigenschaften der Zone überprüfen.

Stub-Zonen gibt es im Microsoft DNS seit Windows Server 2003. Während eine Sekundäre Zone den gesamten Inhalt einer Zone kopiert, speichert die Stub-Zone nur die Einträge einer Zone, die definieren, welche Server für die Namensauflösung der Zone zuständig sind (also die NS- und zugehörigen A-Einträge). Die Vorteile hierbei liegen auf der Hand: Zum einem muss dafür kein Zonentransfer erlaubt werden (die Stub-Zone kann die Einträge einfach wie ein DNS-Client anfragen und speichert diese dann). Zum anderen müssen nicht so viele Daten gespeichert und übertragen werden. Zusätzlich bietet die Stub-Zone mehr Flexibilität, da Anfragen immer an einen der Server gemacht werden – wenn neue hinzukommen, können auch diese gefragt werden. Allerdings bieten die Stub-Zonen damit auch keine Entlastung für die anderen DNS-Server, da sie keine Host-Einträge außer denen der Namensserver für die Zone kennen. Dies ist aber häufig nicht so relevant, da DNS-Server ja sowieso die Ergebnisse von Anfragen zwischenspeichern.

Der Zonentransfer zwischen Primären und Sekundären Zonen kann mit DNS-Servern ab Windows 2000 auch inkrementell erfolgen. Davor wurden immer alle Inhalte der Zone bei einem Transfer übertragen. Jetzt ist es möglich, nur die Unterschiede seit dem letzten Transfer auszutauschen.

Wenn der DNS-Server Dienst auf einem Active Directory-Domänenkontroller (DC) läuft, können Sie Active Directory-integrierte Primäre Zonen erstellen oder auch existierende Zonen umstellen. Das hat die folgenden Vorteile:

- Die Replikation der Zonendaten läuft über das Active Directory.
- Alle DNS-Server, die auf DCs laufen, können auf die Zone schreibend zugreifen (Multi-Master).
- "Sichere Dynamische Updates" können benutzt werden.

Windows-Domänenmitglieder seit Windows 2000 können außerdem die Daten in den DNS-Zonen über Dynamische Updates aktualisieren. Ohne dynamische Updates müsste der Administrator jede Änderung bei der Zuordnung von Netzwerknamen zu IP-Adressen händisch anpassen (und bei Active Directory-Domänenkontrollern noch dessen Services-Einträge). Über die dynamischen Updates informieren DNS-Clients und DHCP-Server die DNS-Server über Änderungen von IP-Adressen. Standardmäßig aktualisiert der Client die Zuordnung Hostname zu IP-Adresse in der Forward-Lookup-Zone – der Hostname ändert sich normalerweise nicht für den Client. Der DHCP-Server aktualisiert die umgekehrte Zuordnung der IP-Adresse zum Hostnamen (der Client bekommt immer wieder eine andere IP-Adresse, der DHCP-Server bleibt aber für die von ihm verwalteten IP-Adressen zuständig). Wenn Sie in einem Active Directory integrierten DNS (nur sichere) dynamische Updates auf der Zone ermöglichen, gewährleistet der Mechanismus für die Aktualisierung, dass der gleiche Computer immer die gleichen Einträge erneuert. Damit können Sie anderen Computern Änderungen an fremden Einträgen verbieten und so für mehr Sicherheit sorgen.

Bezüglich der dynamischen Updates ist noch zu erwähnen, dass die Dienste Netlogon und DHCP-Client auf dem DNS-Client für die Aktualisierungen der Einträge im DNS verantwortlich sind. Machen Sie daher nicht den Fehler, den DHCP-Client auf einem Mitgliedsserver zu deaktivieren (viele Administratoren sind der Ansicht, dass dieser Dienst nicht gebraucht wird, wenn die TCP/IP-Eigenschaften manuell vorgegeben sind). Ansonsten sind keine dynamischen Updates mehr möglich.

GlobalNames – der langsame Abschied von WINS

Seit Windows 2000 versucht Microsoft, die Kurznamensauflösung WINS durch DNS zu ersetzen. Gab es bei Windows 2000 noch zahlreiche Produkte, die eine Kurznamensauflösung benötigten (wie Cluster oder Exchange 2000), sind es über die Zeit immer weniger geworden. Während einige Unternehmen trotz mehrerer Domänen keine Kurznamensauflösung nutzen, sondern die Applikationen ausschließlich vollqualifizierte Namen verwenden, beharren andere Unternehmen für bestimmte Dienste oder Intranets auf diesen Kurznamen.

Betrachten wir das Thema genau, brauchen die Produkte kein WINS, sondern nur eine Auflösung von "Kurznamen", also SRV01 statt *srv01.example.com*. Aber wenn wir uns ansehen, wie ein System Namen auflöst, so wird schnell klar, dass WINS für eine Kurznamensauflösung nicht unbedingt notwendig ist. Befinden sich zum Beispiel der Client und der Server in der gleichen DNS-Zone, wird der Client immer in der

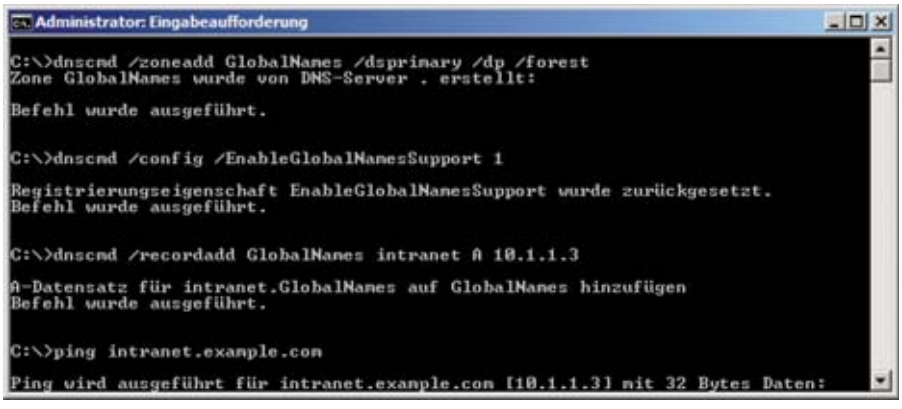


Bild 3: Um auf den Eintrag aus den unterschiedlichsten Zonen zuzugreifen, legen Sie zunächst die Zone "GlobalNames" an, dann schalten Sie den GlobalNamesSupport ein und richten schließlich den Eintrag ein

Lage sein, den Server aufzulösen, da er seinen "Domänensuffix" an die Anfrage hinten anhängt. Genau das gleiche gilt, wenn sich Clients und Server im gleichen Subnetz befinden, da der Client den Server dann per Broadcast auflösen wird.

Beim DNS von Windows Server 2008 hat sich Microsoft eine neue Variante einfallen lassen, um dem Thema zu begegnen: die GlobalNames-Zone. Dies ist eine Zone, die Sie auf einem DNS-Server einrichten können. Diese muss "GlobalNames" heißen und auf einem Windows Server 2008 liegen. Zusätzlich muss die Unterstützung des Features eingeschaltet werden. Dies erreichen Sie über

```
dnscmd /config
  /EnableGlobalNames-Support 1
```

Diesen Befehl müssen Sie für die Server ausführen, die die GlobalNames-Zone enthalten. Danach können Sie in der Zone "GlobalNames" beliebige Alias-Einträge (CNAME-Records) anlegen. Diese werden dann – unabhängig vom angefragten Domänenanteil – für alle Zonen zurückgegeben, die dieser DNS-Server verwaltet. Zum Beispiel würde der DNS-Server die IP-Adresse des Eintrages "intranet.globalnames" zurückgeben wenn er nach *intranet.firma.de* oder *intranet.example.com* gefragt wird, solange er auch für die Zonen "firma.de" und "example.com" zuständig ist.

Natürlich unterstützt DNS unter Windows Server 2008, wie alle Komponenten von Windows Server 2008 und Windows Vista, die IP-Adressierung mittels IPv6.

DNS-Clients und -Server

Ein DNS-Client ist prinzipiell jede Maschine im Netzwerk (auch Mitgliedsserver, Domänencontroller oder DNS-Server), die auf einen DNS-Server zugreift. Der DNS-Client kümmert sich darum, dass die Applikationen auf dem Computer in der Lage sind, DNS-Namen zu IP-Adressen aufzulösen. Hierfür leitet er die Anfragen an einen DNS-Server weiter. Welchen DNS-Server der DNS-Client verwendet, lässt sich im Dialogfeld "Eigenschaften von Internet Protocol (TCP/IP)" angeben. Clients, die ihre IP-Adressen über DHCP bekommen, können auch über DHCP TCP/IP-Eigenschaften wie die DNS-Server erhalten.

Des Weiteren ist es wichtig, dass der Client seinen vollständigen Netzwerknamen (FQDN) kennt. Dies geschieht normalerweise beim Beitritt in eine Active Directory-Domäne automatisch. Wenn Sie eine Domäne erst noch aufbauen oder etwas verkonfiguriert haben, müssen Sie den Namen gegebenenfalls anpassen. Dies geschieht in den "Systemeigenschaften / Computername" über die Schaltflächen "Ändern" und "Weitere". Passen Sie hier den "Primären Domänensuffix" an, etwa bei "client1.firma.de" auf "firma.de". Beachten Sie noch, dass das Auswahlfeld "Primäres DNS-Suffix bei Domänenmitgliedschaftsänderung ändern" gesetzt ist, dann wird der "Primäre DNS-Suffix" bei einer neuen Änderung der Domäne automatisch angepasst.

Der DNS-Client speichert auch die Anfragen, die er getätigt hat, und deren Antworten zwischen. Hierbei werden auch Anfragen, die nicht aufgelöst werden konnten, zwischengespeichert. Mit

```
ipconfig /displaydns
```

lassen Sie sich den Inhalt des Auflösungscaches anzeigen, während Sie mit

```
ipconfig /flushdns
```

den Auflösungscache leeren. Wenn Sie Zonen für Ihren internen Namensraum erstellt haben, und die DNS-Clients richtig eingestellt sind, funktioniert jetzt die Namensauflösung dieser Zone.

DNS-Delegationen

Eingangs erwähnten wir, dass ein Server, der eine Zone hält, für deren Namensraum verantwortlich ist. Dies würde auch alle Namen unterhalb dieses Namensraums beinhalten. Damit ein Server, der zum Beispiel die Zone "company.com." hält, nicht auch alle Einträge für die untergeordnete DNS-Domäne "eu.company.com." managen muss, lässt sich die Verwaltung von DNS-Domänen in neue DNS-Zonen delegieren. Bei einer Delegation wird in die Zone "company.com." geschrieben, dass für den Namensraum "eu.company.com." ein oder mehrere andere Server verantwortlich sind. Würde ein Client (oder ein anderer DNS-Server) jetzt einen der DNS-Server von "company.com." nach einem Namen in der DNS-Zone "eu.company.com." fragen, so würde der Server nur antworten, welche Server für diesen Bereich zuständig sind (technisch korrekt ist dies abhängig von der Art der Anfrage, ob der Server selber auf die Suche gehen soll oder nur mit Referenzen auf weitere Server antwortet).

Sowohl Stub-Zonen als auch Delegationen enthalten die Einträge für Nameserver (NS-Einträge) der jeweiligen Zonen. Damit die IP-Adressen der Server auch gefunden werden, enthalten Delegationen und Stub-Zonen zusätzlich die Host-Einträge (A-Einträge) der Nameserver.

Delegationen sind immer sehr zielorientiert: Wird ein DNS-Server nach einer untergeordneten Domäne gefragt, lautet die Antwort immer, wer für diese zuständig ist (oder zumindest, wer mehr weiß – das kann bei mehreren Hierarchien vorkommen). Merken können Sie sich das ganz einfach: So bedeutet eine Delegation, einen Teil der Verantwortung (über den gesamten Namensraum) an jemand anderen abzugeben. Es ist dabei aber genau definiert, an wen diese Übertragung der Verantwortung erfolgt. Wenn derjenige einen weiteren Teilbereich delegiert, muss er mitteilen, an wen er diesen delegiert hat. Genau so verhält es sich auch beim DNS.

DNS-Weiterleitungen

Innerhalb eines Namensraums lässt sich die Delegation von oben nach unten in der Hierarchie nutzen. Wenn jetzt aber jemand den DNS-Server für *eu.company.com.* nach einer Adresse in *company.com.* oder *it-administrator.de.* fragt, kommen die Wei-

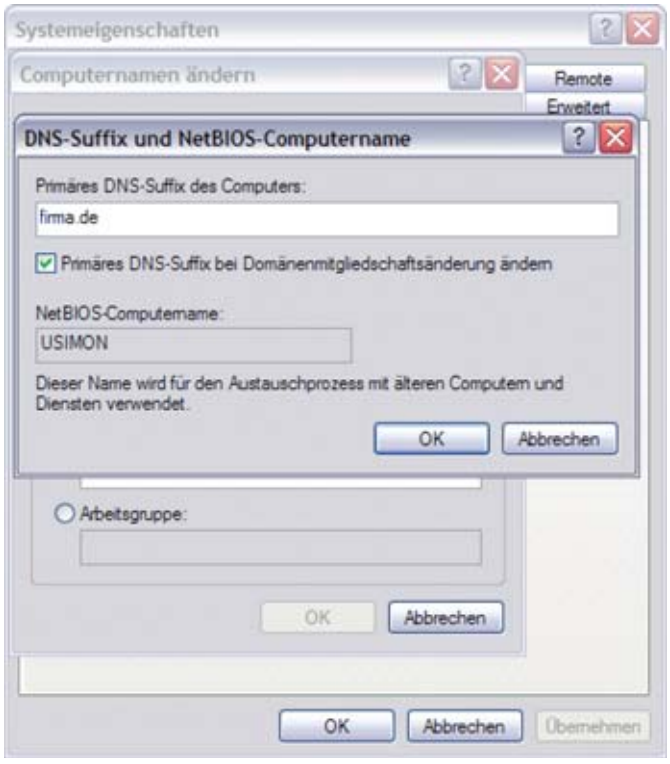


Bild 4: Es ist wichtig, dass der DNS-Client den richtigen DNS-Suffix hat. Nur so kann er seinen Netzwerknamen und seine IP-Adresse dem DNS-Server mitteilen.

terleitungen (Forwarder) ins Spiel, die in den Eigenschaften des DNS-Servers eingerichtet werden. Eine Weiterleitung bedeutet immer soviel wie "ich weiß nicht weiter, aber dieser übergeordnete Server sollte mehr wissen". Ein DNS-Server wird immer zuerst seine eigenen Zonen betrachten, nur wenn er für den angefragten Namensraum (oder einen übergeordneten Namensraum) nicht zuständig ist, wird er den ersten verfügbaren Server fragen, der in der Weiterleitung eingestellt ist.

Typische Einstellungen für den Weiterleitungsserver sind:

- Innerhalb eines Namensraums verweist der Weiterleitungsserver häufig auf einen DNS-Server, der in der Hierarchie weiter oben liegt. Zum Beispiel würde der Forwarder für die DNS-Server der "eu.company.com." DNS-Domäne auf die DNS-Server der company.com-Domäne zeigen.
- Bei DNS-Servern, die in der Hierarchie des Namensraums ganz oben liegen (etwa die DNS-Server für "company.com."), zeigt der Weiterleitungsserver häufig auf den DNS-Server des Internet Service Providers. Dieser ist in der Lage, alle im Internet bekannten DNS-Namen aufzulösen. Alternativ kann der Weiterleitungsserver auch auf einen DNS-Server des Unternehmens (zum Beispiel in der DMZ) zeigen, der in der Lage ist, die Namen im Internet aufzulösen.

Natürlich gibt es auch die Möglichkeit, dass keine Weiterleitungen verwendet werden. Dies ist entweder der Fall, wenn keine Namensauflösung von externen DNS-Namen erwünscht ist (der gesamte Verkehr in das Internet läuft über E-Mail- oder Proxyserver, nur diese sind in der Lage, externe Namen aufzulösen) oder die Server im Unternehmen, die externen Namen über die Stammserver (die für die Internet Root "." zuständig sind) auflösen.

Bedingte Weiterleitungen

Um auch komplexere DNS-Umgebungen zu ermöglichen, gibt es seit Windows Server 2003 die Option der bedingten Weiterleitung (Conditional Forwarding). Hier können Sie abhängig vom angefragten Namensraum unterschiedliche Server als Weiterleitungsserver einstellen. Das kann zum Beispiel in den folgenden Szenarien interessant sein:

- Die Windows DNS-Infrastruktur eines Unternehmens hat einen anderen Namensraum als alle anderen Systeme des Unternehmens. Trotzdem sollen externe Anfragen an den ISP gestellt werden. Hier lässt sich eine bedingte Weiterleitung für den anderen Namensraum im Unternehmen einrichten, und die normale Weiterleitung auf die DNS-Server des Internet Service Providers (ISP) stellen.
- Ein Unternehmen mit mehreren Standorten hat einen durchgängigen Namensraum. Um aber die WAN-Leitungen zu entlasten, nutzt jeder Standort eine direkte Anbindung an das Internet. Hier kann der interne Namensraum des Unternehmens auf die DNS-Server beispielsweise des zentralen Standorts eingestellt werden. Alle anderen Anfragen beantwortet der DNS-Server des ISP.
- Ein Unternehmen greift auf Systeme eines anderen Unternehmens zurück (zum Beispiel ein Tochterunternehmen oder übergeordneter Konzern). Auf der Firewall zwischen den Unternehmen ist die Kommunikation zwischen bestimmten DNS-Servern erlaubt. Hier kann der Namensraum des anderen Unternehmens an die DNS-Server auf der anderen Seite der Firewall weitergeleitet werden. Alle anderen Anfragen gehen wieder an den ISP.
- Bei einer Migration wird die neue DNS-Infrastruktur erstellt, trotzdem sollen noch für einen begrenzten Zeitraum die Namen in der alten Infrastruktur aufgelöst werden können. Auch hier kann eine bedingte Weiterleitung erstellt werden, die später wieder gelöscht werden kann.

Es gibt noch einige andere Fälle für den Einsatz der bedingten Weiterleitung, aber dies sind die gebräuchlichsten.

Steht keine Firewall zwischen den DNS-Servern, sollten Sie immer überprüfen, ob sich nicht auch Stub-Zonen anstelle von bedingten Weiterleitungen oder Delegationen verwenden lassen. Stub-Zonen haben hier den Vorteil, dass diese dynamisch sind. Das bedeutet, fügen Sie neue DNS-Server für die andere Zone hinzu, werden diese auch in die Stub-Zone übernommen. Bei der Delegation oder der bedingten Weiterleitung müssen Sie die Server, die angefragt werden sollen, manuell einrichten. Allerdings lässt sich bei der Stub-Zone nicht einstellen, welcher DNS-Server angefragt werden soll

(was zum Beispiel bei der Kommunikation über eine Firewall notwendig ist).

Überprüfen der DNS-Namensauflösung

Die DNS-Namensauflösung können Sie mit dem Befehl *nslookup* überprüfen. Geben Sie das Kommando einfach in der Eingabeaufforderung ein. Jetzt stehen Ihnen eine Vielzahl weiterer Parameter zur Verfügung – tippen Sie einfach "?" um alle Optionen zu sehen. Mit diesem Befehl können Sie DNS-Abfragen erstellen und überprüfen, ob die Antworten Ihren Erwartungen entsprechen. Hier sind die gebräuchlichsten Befehle:

```
server {IP-Adresse oder Servername}
```

stellt den DNS-Server ein, der für zukünftige Abfragen verwendet werden soll. Standardmäßig wird der Server verwendet, der in den "Eigenschaften von Internetprotocol (TCP/IP)" angegeben ist.

```
set type={Abfragetyp}
```

legt fest, welche Typen von Einträgen Sie abfragen wollen. Welche Abfragetypen Sie einstellen sollen und welche Antworten Sie hierbei erhalten sollten, finden Sie weiter unten. Mit

```
Set debug Set d2
```

können Sie den Debug-Level erhöhen. Das bedeutet, Sie können auch sehen, welche Anfragen und Antworten zum Auflösen Ihrer Anfrage verwendet werden.

Nachdem wir die gebräuchlichsten Befehle erklärt haben, sehen wir uns einmal an, wie eine Überprüfung der DNS-Infrastruktur aussieht. Nehmen wir an, Sie erhalten nach der Eingabe von *nslookup* eine Antwort wie die folgende:

```
*** Der Servername für die Adresse
  192.168.100.1 konnte nicht gefun-
  den werden: Timed out
Standardserver:  UnKnown
Address: 192.168.100.1
```

Dies ist kein Grund zur Besorgnis. Entweder haben Sie keine Reverse-Lookup-Zone eingerichtet oder der DNS-Server hat sich in dieser noch nicht registriert. Wenn die Zone existiert, der DNS-Client des Servers richtig eingerichtet ist und die Zone auf dynamische Updates einstellt ist, starten Sie den DHCP-Client-Dienst auf dem DNS-Server neu. Überprüfen Sie jetzt, dass der Server seine IP-Adresse in der Reverse-Lookup-Zone eingetragen hat (als PTR-Eintrag).

Bild 5: Die Weiterleitungen und bedingten Weiterleitungen lassen sich bis Windows Server 2003 R2 in den Eigenschaften des DNS-Servers konfigurieren

Tippen Sie nun den Befehl *set type=SOA* ein. Ab jetzt wird nach den Start-Of-Authority-Einträgen gesucht. Diese sollten für jede Zone existieren und jeweils einen der Server anzeigen, die eine Primäre Kopie der Zone halten. Geben Sie jetzt den Namen der DNS-Zone ein (etwa "company.com."), sollten Sie den Server und dessen Eigenschaften erhalten.

```
> set type=SOA
> company.com
Server:  UnKnown
Address: 192.168.100.1

company.com
        primary name server =
itadc01.company.com
        responsible mail addr =
  hostmaster
        serial  = 40
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
itadc01.company.com
  internet address = 192.168.100.1
```

Erhalten Sie bei einer Anfrage die Antwort "Nicht autorisierte Antwort" oder "Non-Authoritative Answer", bedeutet das nur, dass Sie die Antwort von einem Server bekommen haben, der nicht schreibend auf die angefragte DNS-Zone zugreifen kann. Dies soll Ihnen einen Hinweis darauf geben, dass der Eintrag auf dem primären Server eventuell aktueller sein kann als die Antwort, die an Sie geliefert wurde.

Zur weiteren Überprüfung geben Sie nun jede andere DNS-Domäne in Ihrem Unternehmen ein. Sie sollten für jede Domäne eine Antwort erhalten. Ist dies aber bei einer Domäne nicht der Fall, überprüfen Sie, warum dies so ist. Funktionieren die Weiterleitungen nach oben in der Hierarchie und die Delegationen nach unten? Wenn ja, sollte auch die Antwort stimmen. Als nächstes tippen Sie den Befehl *set type=NS* ein. Geben Sie jetzt den Namen

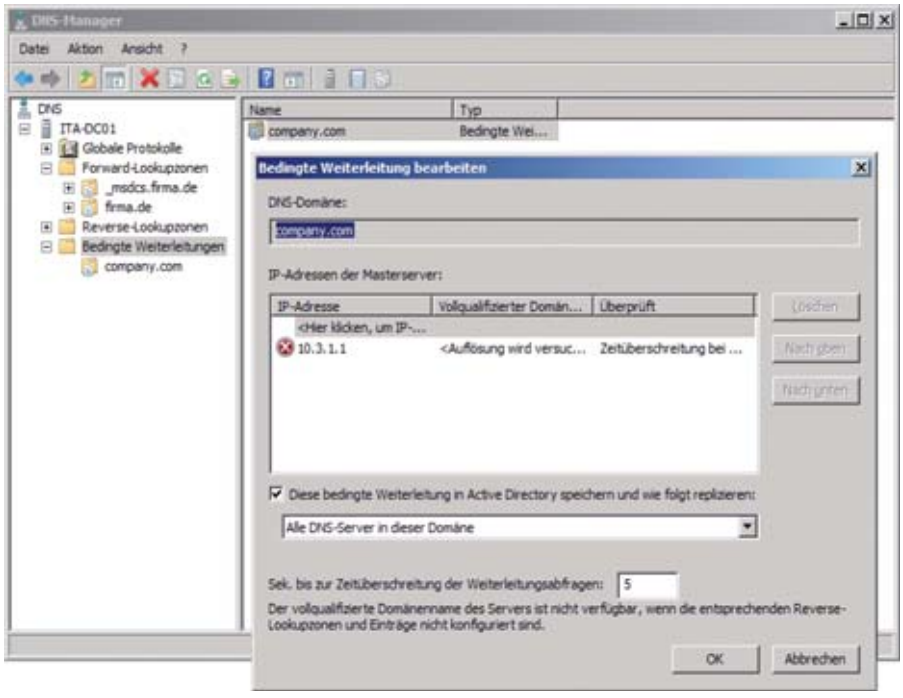


Bild 6: Unter Windows Server 2008 (R2) lassen sich die bedingten Weiterleitungen direkt in der DNS-Verwaltung pflegen. Hier wird auch eingestellt, ob die Weiterleitungen auf andere DNS-Server über das Active Directory repliziert werden sollen.

einer DNS-Zone ein, sollten Sie die Namen aller Server erhalten, die für diese Zone antworten können (also Server, die entweder eine Primäre oder eine Sekundäre Kopie der Zone halten). Das Ergebnis sollte wie folgt aussehen:

```
> set type=NS
> company.com
Server:  UnKnown
Address: 192.168.100.1

company.com
  nameserver = itadc01.company.com
company.com
  nameserver = itadc02. company.com
itadc01.company.com
  internet address = 192.168.100.1
itadc02.company.com
  internet address = 192.168.101.1
```

Überprüfen Sie auch hier wieder jede andere Zone im Unternehmen. Haben Sie beim vorigen Test Antworten erhalten, sollte auch das Aufzählen der Namensserver funktionieren. Allerdings ist es möglich, dass Sie nicht alle Namensserver für eine Zone erhalten, die Sie eingerichtet haben. Hier haben Sie vielleicht vergessen, einen dazugehörigen NS-Eintrag in den Eigenschaften der Zone zu erstellen (welche Nameserver für eine Zone zuständig sind, müssen Sie manuell einrichten).

Wie bereits erwähnt, werden in einer Delegation und einer Stub-Zone die NS- und die dazugehörigen A-Einträge gespeichert. Das heißt, erhalten Sie eine Antwort auf eine Anfrage, kann diese Antwort auch von einem Server stammen, der eine Delegation oder Stub-Zone auf die angefragte Zone hält. Um daher sicher zu gehen, dass die Delegation oder Stub-Zone funktioniert, müssen Sie einen Server oder Client anfragen, der in der Zone liegt, aber kein DNS-Server ist. Hierzu können Sie mit *set type=A* nach Hostnamen suchen. Geben Sie einfach einen Server oder Client in jeder Zone ein und das Ergebnis sollte so aussehen:

```
> set type=A
> client01.company.com
Server:  itadc01.company.com
Address:  192.168.100.1
Name:    client01.company.com
Address:  192.168.100.54
```

Nach Abschluss dieser Tests können Sie mit dem Befehl *server* gefolgt von der IP-Adresse oder dem Namen des Servers die Suche auf einem anderen Server fortsetzen. Wiederholen Sie hier alle Tests. Um sicher zu gehen, dass die DNS-Infrastruktur funktioniert, sollten Sie mindestens einen DNS-Server pro Zone nach allen anderen Zonen abfragen. Am besten ist es natürlich, wenn Sie jeden DNS-Server überprüfen.

Ein wichtiger Punkt ist noch, dass *NSLookup* nicht den DNS-Client verwendet, um Anfragen durchzuführen. Stattdessen löst es die Namen selbstständig über DNS-Server auf. Wenn Sie also auf einzelnen Systemen Probleme haben, DNS-Namen aufzulösen (zum Beispiel über das PING-Kommando), aber die Namen über *NSLookup* auflösbar sind, dann reicht es häufig aus, den DNS-Client-Dienst neu zu starten.

Um zu überprüfen, ob ein Name vom DNS-Client-Dienst aufgelöst werden kann, führen Sie einfach einen Ping auf den Namen durch. Ob sie eine Antwort erhalten, ist hier irrelevant; interessant ist, ob in der ersten Zeile der Servernamen in eine IP-Adresse aufgelöst werden kann.

DNS-Einträge für das Active Directory

Der Domain Name Service (DNS) dient in einem Active Directory-Netzwerk nicht nur dem Auffinden der Namen von Clients und Servern, sondern vor allem auch dazu, um die Active Directory Dienste von Domänencontrollern zu finden. Damit die Dienste der Domänencontroller in einem Active Directory von den Mitgliedern der Domäne ausfindig gemacht werden können, werden diese von den DCs in die entsprechende DNS-Zone eingetragen.

Für die domänenspezifischen Dienste kommen hierbei DNS-Subdomänen zum Einsatz. Wird zum Beispiel für eine Firma der Namensraum "firma.de" verwendet, werden in der Zone "firma.de" die DNS-Subdomänen "_msdcs.firma.de", "_sites.fir-

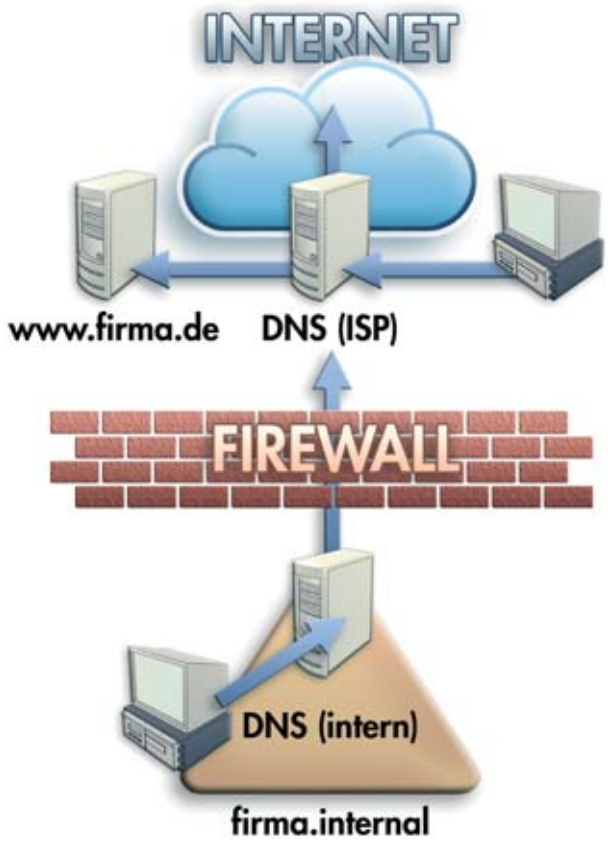


Bild 7: Verschiedene Namensräume (zum Beispiel intern ein privater) kann der Administrator leichter verwalten

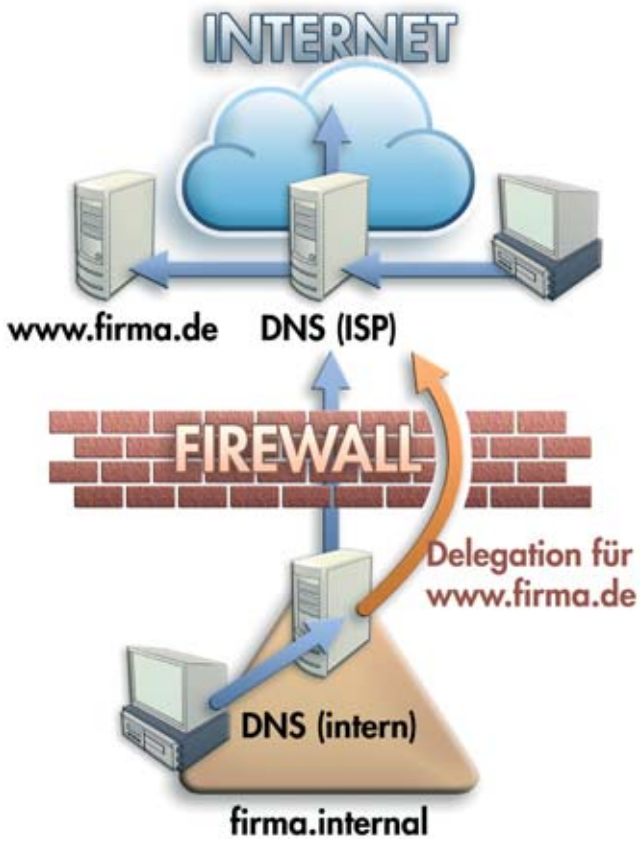


Bild 8: Wird intern und extern der gleiche Namensraum verwendet, muss der Administrator sicherstellen, dass die externen Server auch intern aufgelöst werden können

ma.de", "_tcp.firma.de" und "_udp.firma.de" eingerichtet. Seit Windows Server 2003 gibt es noch zusätzlich die DNS-Subdomänen "domainDnsZones" und "forestDnsZones". In diesen DNS-Subdomänen finden sich alle Informationen über die Anmeldeserver und die Globalen Katalogserver (GC) der Umgebung, sowie welche Server die Rolle des PDC-Emulators halten. Über die Struktur unterhalb dieser DNS-Subdomänen können zum Beispiel die Domänenmitglieder auch einen bestimmten Dienst in einem ausgewählten Standort suchen.

Sowohl für die Anmeldung der Clients an der Active Directory-Domäne als auch für die Replikation zwischen den Domänenkontrollern ist es wichtig, dass die Einträge der Domänenkontroller und Dienste im DNS gefunden werden. Besondere Aufmerksamkeit verdienen hier die Einträge, die unterhalb der "_msdcs-DNS"-Domäne der ersten Domäne in einer Gesamtstruktur (auch Rootdomäne) liegen: Unterhalb dieser DNS-Domäne werden von allen Domänenmitgliedern die Einträge der Globalen Katalogserver gesucht – auch während des Anmeldevorgangs. Haben Sie mehrere Active Directory-Domänen über mehrere Standorte verteilt und die erste Domäne der Gesamtstruktur existiert nicht in allen Standorten, sollten Sie überlegen, wie Sie diese DNS-Subdomäne auch auf den DNS-Servern der weiteren Standorte zur Verfügung stellen. Seit Windows Server 2003 wird dies standardmäßig berücksichtigt: Lassen Sie den DNS-Service beim Einrichten der Active Directory-Domäne automatisch konfigurieren, legt der Assistent eine separate Zone für die _msdcs-DNS-Domäne an und erstellt eine Delegation der übergeordneten Domäne. Das hat den Hintergrund, dass eine Zone unabhängig von anderen Zonen auf dem Server repliziert werden kann. Beim Einrichten des Active Directory konfiguriert der Server diese Zone so, dass sie über das Active Directory auf alle DNS-Server der Gesamtstruktur, die auch DCs sind, repliziert wird.

Auch bei einem Windows 2000 Active Directory wird aus dem gleichen Grund empfohlen, die _msdcs-DNS-Domäne der Rootdomäne als eigene Zone anzulegen. Damit ist der Administrator dann in der Lage, diese Zone als Sekundäre Zone auf die DNS-Server in anderen Standorten zu übertragen – auch diejenigen, in denen kein DNS-Server der Rootdomäne steht.

In Umgebungen, die seit Windows 2000 migriert wurden, ist dies häufig noch nicht berücksichtigt beziehungsweise korrigiert worden. Obwohl dies erst relevant ist, wenn es mehr als eine Domäne in der Gesamtstruktur gibt, spricht nichts dagegen, die Infrastruktur nach heutigen Best Practices zu konfigurieren, um Problemen bei zukünftigen Erweiterungen vorzubeugen.

Bild 9: Ein paralleler Namensraum lässt sich seit Windows Server 2003 auch mit "Bedingten Weiterleitungen" realisieren

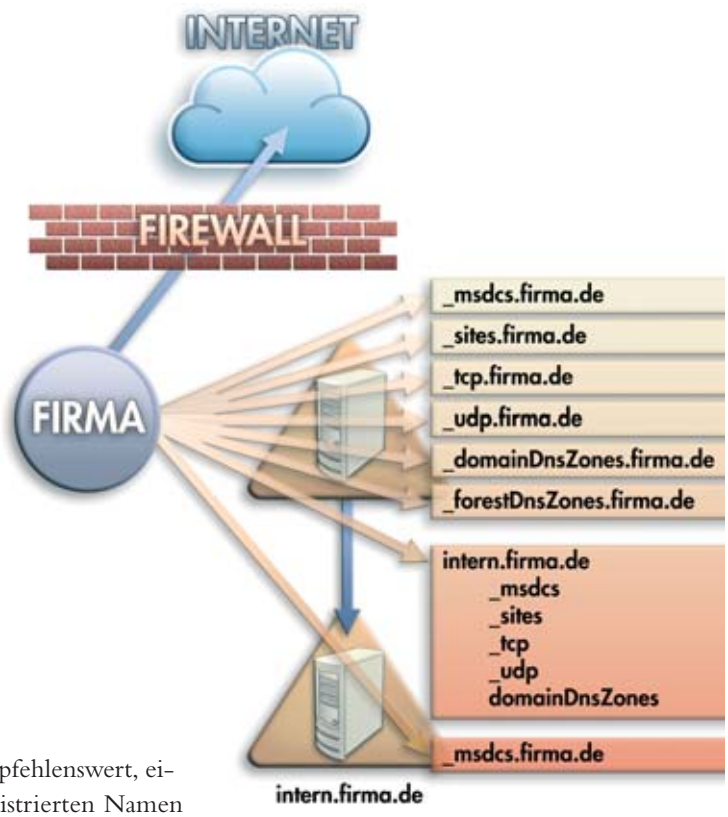


Bild 10: Muss der gleiche Namensraum für die Active Directory-Rootdomäne verwendet werden, empfiehlt es sich, durch Delegationen die Subdomänen auf Windows DNS-Servern zu halten

Namensraum für das AD

Der Namensraum stellt die oberste in der DNS-Hierarchie verwendete DNS-Domäne dar, zum Beispiel fallen in den Namensraum "company.com" auch alle DNS-Namen unterhalb dieser Domäne, etwa "eu.company.com". Für ein Active Directory muss mindestens ein Namensraum verwendet werden. Bei der Wahl des Namensraums sollten Sie beachten, dass der Name nicht von anderen Unternehmen registriert ist, da dies zu rechtlichen Problemen führen könnte. Also sollten Sie entweder einen Namen verwenden, der für Sie registriert ist, oder einen der nicht registrierbar ist.

Intern einen privaten Namensraum verwenden

Häufig wird für den internen Namensraum ein Name wie "firma.local" verwendet, da ".local" derzeit kein offizieller Top-Level-Domänenname ist. Bei einem solchen privaten Namen besteht jedoch immer das Risiko, dass der Name in Zukunft als Top-Level-Domänenname zugelassen wird. Zum Beispiel wird der Name ".local" derzeit in einem Internet Draft für Multicast DNS-Namen [1] vorgeschlagen.

Daher ist es empfehlenswert, einen offiziell registrierten Namen zu verwenden. Dies kann der Name sein, der für den offiziellen Internet-Auftritt Ihres Unternehmens im Internet verwendet wird, oder auch ein weiterer registrierter Name, der nicht verwendet wird. Ansonsten haben Sie mit einem privaten Namen aber den Vorteil, dass Sie den Namen nicht offiziell registrieren müssen und dass Sie keine Konflikte zwischen dem internen und externen Namensraum lösen müssen.

Dabei werden die DNS-Namen nach folgendem Muster aufgelöst:

- Interne Clients lösen interne Namen über den internen DNS-Server auf.
- Interne Clients lösen externe Namen über den internen DNS-Server auf (dieser hat den DNS-Server des Internet Service Providers als Weiterleitung eingetragen und fragt bei diesem nach).
- Interne Clients lösen den eigenen Webserver genau so auf wie alle anderen externen Namen.
- Externe Clients können interne Namen nicht auflösen.
- Externe Clients können den eigenen Webserver auflösen (über den DNS-Server des ISP).
- Der Webserver kann extern und intern meistens über "http://firma.de" (ohne "www") aufgelöst werden.

Intern und extern den gleichen Namensraum verwenden

Wenn Sie intern und extern den gleichen Namen verwenden (zum Beispiel "firma.de"), müssen Sie berücksichtigen, dass zumindest Ihre externen Webserver, VPN-Gateways und so weiter für die Anwender erreichbar bleiben müssen. Sie müssen sich daher darum kümmern, dass die internen DNS-Server in der Lage sind, die externen Namen (wie *www.firma.de*) aufzulösen. Dies bedeutet einen zusätzlichen Verwaltungsaufwand. Hierbei gibt es zwei Möglichkeiten:

1. Sie richten Host-Einträge (A-Records) im internen DNS-Server für die externen Server ein. Ändert der ISP die IP-Adressen, müssen Sie dies auch im internen DNS verwalten.

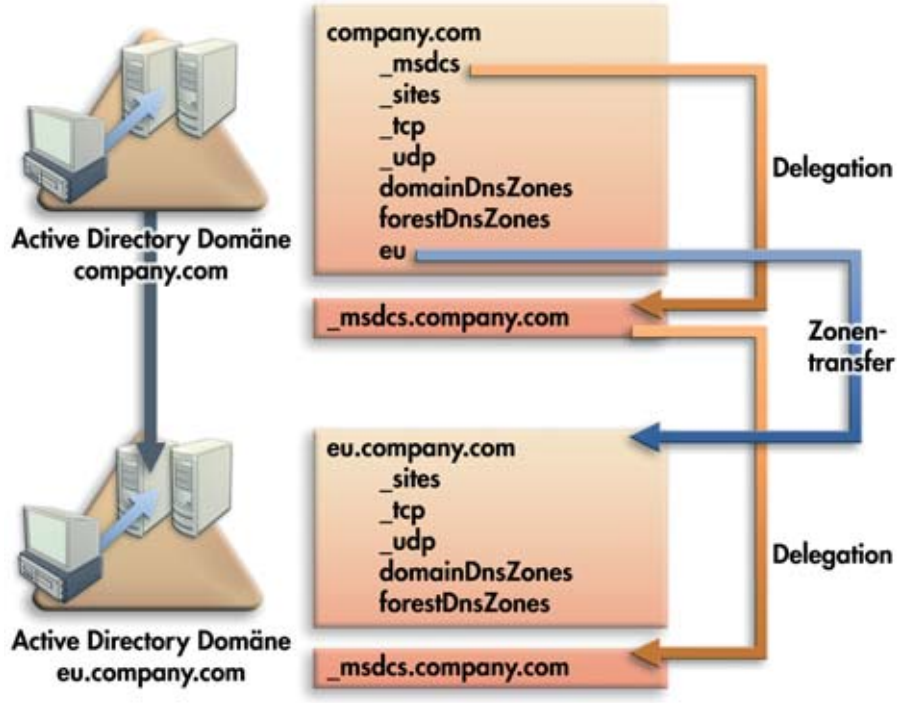


Bild 11: Die DNS-Subdomäne "_msdcs" der Rootdomäne sollte zu anderen Domänen übertragen werden können. Hierzu muss sie als Zone eingerichtet werden.

2. Sie richten eine Delegation für den Namen Ihrer Webserver auf den internen DNS-Servern ein, diese werden auf die DNS-Server des ISP delegiert (zum Beispiel wird eine Delegation für www in der Zone "firma.de" erstellt, die auf die IP-Adresse des ISP zeigt). Wenn Ihr ISP jetzt die IP-Adressen der Webserver ändert, müssen Sie keine Änderungen in den internen DNS-Einträgen machen.

Außerdem müssen Sie bei diesem Szenario berücksichtigen, dass der FQDN der Domäne (zum Beispiel "firma.de") von den Domänenkontrollern und Clients benötigt wird. Im Internet mag Ihr Webauftritt auch unter "http://firma.de" erreichbar sein, intern wird und darf dies nicht der Fall sein. Bei Anfragen von Clients nach "firma.de" werden stets die IP-Adressen der Domänenkontroller dieser Domäne zurückgeben.

In diesem Szenario werden die DNS-Namen wie folgt aufgelöst:

- Interne Clients lösen interne Namen über den internen DNS-Server auf.
- Interne Clients lösen externe Namen über den internen DNS-Server auf (dieser hat den DNS-Server des Internet Service Providers als Weiterleitung eingetragen, und fragt bei diesem nach).
- Interne Clients lösen den eigenen Webserver über den internen DNS-Server auf, der Administrator hat auf diesem den Eintrag entweder über einen Host-Eintrag oder über eine Delegation auf den DNS-Server des ISP eingerichtet.
- Externe Clients können interne Namen nicht auflösen.
- Externe Clients können den eigenen Webserver auflösen (über den DNS-Server des ISP).
- Der Webserver kann nur extern meistens über "http://firma.de" (ohne "www") aufgelöst werden. Intern können die Clients den Webserver über diesen Namen nicht auflösen.

Vorteile der Windows DNS-Server

Es wird insbesondere bei Migrationen immer wieder diskutiert, ob Unternehmen den DNS-Service von Microsoft oder von Drittherstellern nutzen sollen. Dies ist besonders bei Unternehmen, die derzeit bereits eine Nicht-Microsoft DNS-Infrastruktur einsetzen, der Fall.

Die Vorteile des Microsoft DNS unter Windows 2000 und höher sind vor allem diese:

- Multi-Master DNS-Zonen: Normalerweise darf immer nur ein DNS-Server, der die Primäre Zone hält, auf diese schreibend zugreifen. Ist die DNS-Zone Active Directory integriert, können alle DCs, die eine Kopie der Zone halten, diese auch beschreiben. Die intelligente Replikation des Active Directory löst die Konflikte.
- Replikation: Ist die Zone in das Active Directory integriert, wird dessen Replikation verwendet. Die AD-Replikation ist darauf optimiert, sowohl innerhalb von Standorten als auch über schwache WAN-Leitungen zuverlässig zu replizieren.
- Sichere Dynamische DNS-Aktualisierungen: Ein AD-basiertes DNS kann auch die Sicherheit des Active Directory nutzen. Kommt ein Drittherstellerprodukt für DNS zum Einsatz, können häufig keine sicheren Dynamischen Updates verwendet werden. Seit Windows Server 2008 werden auch sichere dynamische Updates über DNSSec anstatt Kerberos

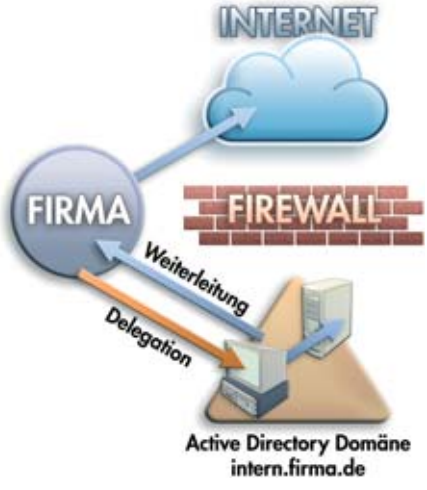


Bild 12: Wird die Windows DNS-Domäne auf Windows-Servern als Subdomäne des Namensraums eingerichtet, ist eine Delegation und eine Weiterleitung erforderlich

unterstützt, dies ist allerdings optional und muss eingerichtet werden.

- Support aus einer Hand: Tritt ein Problem in der Infrastruktur auf, das den Support des Herstellers erfordert, fangen die Anbieter häufig an, sich die Schuld gegenseitig zuzuweisen. Wenn Sie ein Problem mit dem Active Directory oder dem Microsoft DNS haben, erhalten Sie Hilfe aus einer Hand, was bei derartigen Problemen durchaus wünschenswert ist.

Active Directory als Subdomäne einer DNS-Umgebung einrichten

Besitzt das Unternehmen bereits eine DNS-Infrastruktur und ist diese von der Microsoft-Infrastruktur unabhängig und sehr heterogen, ist es manchmal wünschenswert, die Windows-Domäne als Subdomäne in die bestehende DNS-Umgebung zu integrieren. Der größte Vorteil hierbei ist, dass sich der Windows DNS-Service für die Windows-Domänen nutzen lässt.

Hierbei müssen Sie eine Delegation von dem bestehenden Namensraum für die neue Subdomäne einrichten. Die Subdomäne liegt auf den Active Directory-basierten DNS-Servern. Auf den Windows DNS-Servern wird eine Weiterleitung auf die darüber liegenden DNS-Server eingerichtet.

Das Active Directory in einem parallelen Namensraum einrichten

Manchmal wünschen die Unternehmen auch, für die Windows-Welt einen neuen Namensraum zu verwenden. Dies sieht dann genau so aus wie bei dem eben beschriebenen Szenario. Alternativ dazu können Sie aber seit Windows Server 2003 auch eine "Bedingte Weiterleitung" verwenden.

Hierbei kann der Windows Server den DNS-Server des ISP als Weiterleitung verwenden und fragt den bisherigen DNS-Server nur für dessen Namensraum an. Die "Bedingte Weiterleitung" konfigurieren Sie in den Eigenschaften des DNS-Servers. Manchmal ist es auch gewünscht, die Active Directory-Domäne in einen bereits bestehenden Namensraum zu integrieren. Hierfür gibt es zwei Varianten.

AD-Domäne in DNS-Umgebung integrieren und Subdomänen delegieren

Soll die Active Directory-Domäne in den bestehenden Namensraum integriert werden, können Sie die Microsoft-spezifischen DNS-Subdomänen und die Active Directory-Subdomänen auf einen Windows DNS-Server delegieren.

Mit diesem Szenario kann das Unternehmen die Vorteile des Windows-DNS mit einem gemeinsamen DNS-Namen verbinden. Dynamische Aktualisierungen sind in allen Microsoft-spezifischen Subdomänen möglich und die Domänencontroller können ihre Einträge automatisch schreiben. Allerdings müssen Sie alle Zonen manuell einrichten und konfigurieren. Dann müssen Sie Delegationen für alle Zonen auf dem Nicht-Windows DNS-Server setzen. Außerdem sind die Host-Einträge für die Clients und Server der Rootdomäne im Nicht-Windows DNS manuell zu pflegen. Daher sollten Sie darauf achten, dass die Clients und Server alle Mitglieder in der Active Directroy-Subdomäne sind.

```
arrComp = Array("itadc01.firma.de",
   "itadc02.firma.de")

For each sComp in arrComp
  WScript.Echo "Der Cache auf " & sComp & " wird
   gelöscht"

  On Error Resume Next

  Set objWMIService = GetObject("winmgmts:" _
   & "{impersonationLevel=impersonate}!\\" &
   sComp & _
       "\root\MicrosoftDNS")

  If Err.Number  0 then
    WScript.Echo "Fehler " & Err.Number & ": " &
   Err.Description
    Err.Clear
  Else
    Set cItm = objWMIService.ExecQuery("Select *
   From MicrosoftDNS_Cache")

    For Each oItm in cItm
      oItm.ClearCache()
      If Err.Number  0 Then
        WScript.Echo "Fehler " & Err.Number & ": "
   & Err.Description
        Err.Clear
      End If
    Next
  End If
Next
```

Listing: Löschen der DNS-Caches von mehreren Servern

Die Active Directory-Domänen in eine bestehende DNS-Domäne integrieren

Können Sie auf die Vorteile der Active Directory-integrierten DNS-Zonen und dynamische Aktualisierungen verzichten und haben bereits eine Nicht-Windows DNS-Infrastruktur im Einsatz, lässt sich die Active Directory-Domäne auch in das bestehende DNS integrieren. Dafür ist es notwendig, dass Sie jede Änderung der Standortstruktur, der Betriebsmaster, der

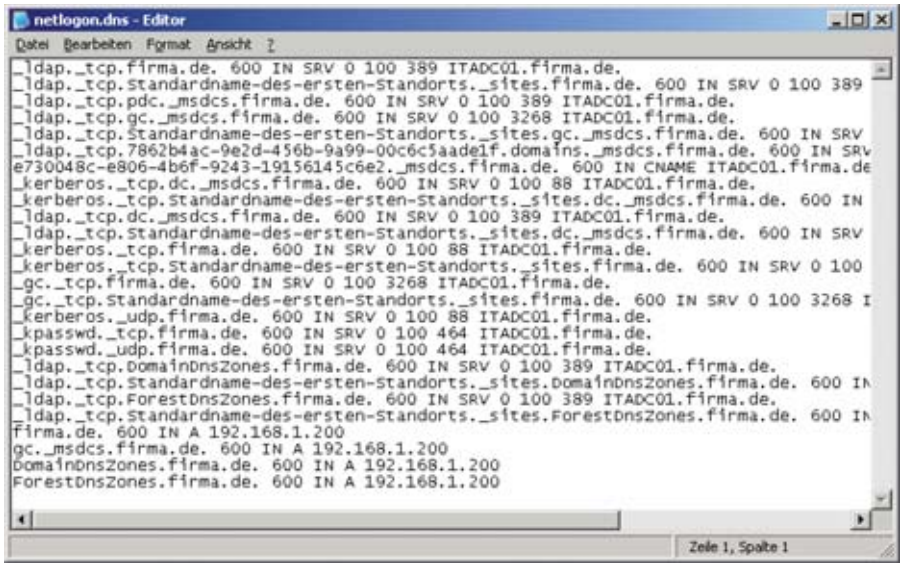


Bild 13: Die Datei *Netlogon.dns* enthält alle DNS-Einträge, die der Administrator für einen Domänenkontroller anlegen muss

Domänenkontroller oder der Globalen Katalogserver im DNS pflegen (normalerweise würden die DCs dies automatisch über die dynamischen Aktualisierungen machen).

Hierzu verwenden Sie die Datei *%windir%\system32\config\netlogon.dns* auf jedem Domänenkontroller als Vorlage. In dieser Datei speichert der DC, welche DNS-Einträge auf dem DNS-Server für ihn geschrieben werden müssen. Dann müssen Sie dem DC noch abgewöhnen, dass er die dynamischen Einträge schreiben will. Das erledigen Sie im folgenden Registrierungsschlüssel:

```
HKLM\SYSTEM\CurrentControlSet\
  Services\Netlogon\Parameters
RegisterDnsARecords = 0 (reg_DWord)
```

Einrichten und Konfigurieren von DNS über die Befehlszeile

Wenn Sie DNS einrichten oder verwalten, können Sie eine Menge Aufgaben mit Kommandozeilentools vereinfachen. In vielen Unternehmen werden Routinen zur automatischen Installation von standardisierten Servern verwendet. Wenn Sie die Installation des DNS-Server-Dienstes per Kommandozeile automatisieren möchten, verwenden Sie ab Windows Server 2008 hierfür *ServerManagerCMD.exe* wie folgt:

```
ServerManagerCMD.exe -install DNS
```

In der PowerShell erledigen Sie dies über die folgenden Befehle:

```
import-module ServerManager
Add-WindowsFeature DNS
```

Damit ist der DNS-Server Service schon installiert. Wenn Sie dies in einem Batch-Script steuern, können Sie das Kommando auch mit "start /wait" aufrufen und in den folgenden Schritten den neuen DNS-Service gleich einrichten. Zum Einrichten des DNS-Server-Service dient das Befehlszeilenkommando *DNSCMD* (bis Windows Server 2003 in den Support-Tools, auf der Windows Server-CD im Verzeichnis "Support" zu finden – bei Windows Server 2008 und neuer direkt im Betriebssystem).

Machen Sie sich nun mit den Möglichkeiten von *DNSCMD* vertraut. Wie gewohnt erhalten Sie mit dem Befehl *dnscmd /?* eine Liste, welche Parameter unterstützt werden. Das Einrichten der Server für die Weiterleitung erfolgt mit

```
dnscmd /resetforwarders 192.168.1.1
  192.168.1.2
```

Bei Windows Server 2003 lassen sich "Bedingten Weiterleitungen", die Sie mit dem AD auf allen DNS-Servern der Domäne / der Gesamtstruktur einrichten wollen, ausschließlich über das dnscmd-Kommando setzen. Bei der grafischen Benutzeroberfläche ist dies erst seit Windows Server 2008 möglich, bei Server 2003 müssten Sie die "Bedingte Weiterleitung" auf jedem DNS-Server einzeln eintragen. Die AD-integrierte "Bedingte Weiterleitung" erstellen Sie über

```
dnscmd /ZoneAdd zielzone.com
  /DsForwarder 10.0.1.1 10.0.1.2
```

Natürlich können Sie über *DNSCMD* auch neue Zonen generieren. Der folgende Befehl legt eine AD-integrierte Zone an und repliziert diese auf alle Domänenkontroller im Forest, die auch DNS-Server sind:

```
dnscmd /ZoneAdd firma.de /DsPrimary
  /dp /forest
```

Als nächsten logischen Schritt stellen Sie diese Zone so ein, dass "Nur Sichere Dynamische Aktualisierungen" erlaubt sind:

```
dnscmd /Config firma.de
  /AllowUpdate 2
```

Wenn Sie jetzt noch Einträge in der neuen Zone hinzufügen möchten, erstellen Sie diese mit dem folgenden Kommando:

```
dnscmd /RecordAdd firma.de dc01 A
  192.168.1.1
```

Dieser Befehl legt einen Host-Eintrag (A-Record) in der Zone "firma.de" für den Server dc01.firma.de. mit der IP-Adresse 192.168.1.1 an.

Natürlich können Sie sich auch mit VB-Script viele Aufgaben am DNS-Server vereinfachen. Das Listing zeigt ein Beispiel, mit dem Sie den Cache mehrerer DNS-Server löschen (zum Beispiel wenn Sie Änderungen an Einträgen übergeordneter DNS-Server vornehmen). Weitere Beispiele, wie Sie mit VB-Script DNS-Server und -Einträge verwalten, finden Sie im Microsoft TechNet Scriptcenter [2] unter der Kategorie "Networking / DNS".

Fazit

Es gibt viele verschiedene Varianten, wie Sie ein Active Directory in eine bestehende DNS-Infrastruktur implementieren können. Welche Sie wählen, hängt meistens von den konkreten Anforderungen des Unternehmens ab. Häufig werden auch Mischformen der hier gezeigten Szenarien eingesetzt. Der DNS-Server-Service unter Windows Server bietet viele Vorteile, die Sie zumindest in der Windows-Welt in Ihrem Unternehmen nutzen sollten.

Auch gibt es mittlerweile diverse Möglichkeiten, wie Sie das Einrichten und Verwalten eines DNS-Servers über Stapelverarbeitungsdateien (Batch oder CMD) automatisieren. Wenn Sie sich dann noch mit den Möglichkeiten von VB-Script auseinandersetzen, lässt sich nahezu jede Anforderung auch automatisieren. *(jp)*

[1] **Internet-Draft für Multicast DNS-Namen**
http://files.multicastdns.org/draft-cheshire-dnsext-multicastdns.txt

[2] **Microsoft TechNet Scriptcenter / Kategory "Networking / DNS".**
http://gallery.technet.microsoft.com/ScriptCenter/en-us/

Links

DNS im Active Directory

Hausputz im Netz

Seit eh und je sind Active Directory und DNS eng miteinander verwoben. Nahezu die gesamte Namensauflösung sowie die Logik des Auffindens von Diensten und Hosts im Verzeichnis basiert auf dem engen Zusammenspiel zwischen AD und DNS. Wie DNS im Windows-Netz funktioniert und warum dort gelegentlich aufgeräumt werden muss, zeigt dieser Workshop.

Active Directory-Domänen werden in DNS mit Zonen verwaltet. Eine Active Directory-Domäne entspricht einer DNS-Zone (Details hierzu siehe Artikel "Active Directory und DNS" auf Seite 48), die nicht nur die Namenseinträge für alle Mitgliedscomputer verwaltet, sondern auch die Standort- und Dienstspezifischen Einträge von Domänencontrollern (DC) speichert. Clients können Diensteinträge (Service- oder SRV-Records) anfragen, um einen Server mit einem bestimmten Dienst abzurufen. Ein Beispiel für eine Anwendung dieses Prinzips ist der DC-Locator-Process: Clients sollen in der Lage sein, DNS-Server nach DCs in bestimmten Standorten zu fragen, um möglichst kurze Pfade bei der Authentifizierung zurücklegen zu müssen.

Einträge in DNS können sowohl statischer als auch dynamischer Natur sein. Neben den manuell festgelegten, statischen Einträgen zur Namens-Adress-Auflösung beherrschen Computer heute die Aktualisierung von DNS-Einträgen auf automatisierter Basis per dynamischem DNS (DDNS) [1]. DNS-Administratoren verwalten deshalb keine statischen Namenslisten mehr, sondern lassen Clients selbstständig die Erstellung und Aktualisierung ihrer Namenseinträge in der Zone durchführen.

Auch Domänencontroller registrieren sich und ihre Dienste in DNS. Dies sind neben den üblichen A- und PTR-Einträgen auch SRV-Records für ihren Verzeichnisserver (LDAP) und die Authentifizierungdienste (Kerberos), damit sie von Clients gefunden werden können.

Den Registrierungsvorgang für DDNS stoßen die Netlogon- und DHCP-Client-Dienste an. Beim Start des Dienstes und zyklisch im laufenden Betrieb findet die Registrierung der notwendigen A- und bei Bedarf SRV- und CNAME-Einträge in DNS über den Netlogon-Dienst statt. Der DHCP-Client-Dienst kümmert sich um die PTR-Einträge. DNS-Clients finden so bei Vorwärts-, Rückwärts- und Dienstsuchen verfügbare Einträge und können alle in der Zone verfügbaren Namen in IP-Adressen – und umgekehrt – auflösen. Wird einer der Einträge aus der Zone entfernt, registriert Netlogon ihn nach spätestens 24 Stunden per Update erneut – vorausgesetzt der Client und der Dienst laufen.

DHCP und DNS

Die Zuständigkeit der Aktualisierung der Einträge für die Namensauflösung wechselt, wenn DHCP-Server in die Umgebung eingeführt werden und Clients IP-Adressen über diese Server-Dienste beziehen. DHCP-Server können Sie mit einer eigenen Option dazu konfigurieren, einen Teil oder sogar alle DNS-Einträge für ihre "IP-Abonnenten" zu aktualisieren. Der DHCP-Server unterscheidet hierbei zwischen drei Modi: keine Registrierung, das Registrieren von PTR-Records oder das Registrieren von

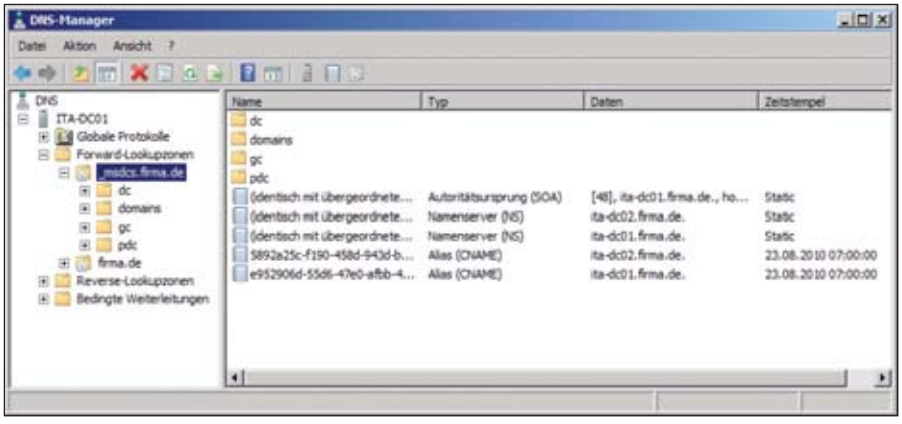


Bild 1: Die Active Directory-Namensauflösung beruht auf DNS

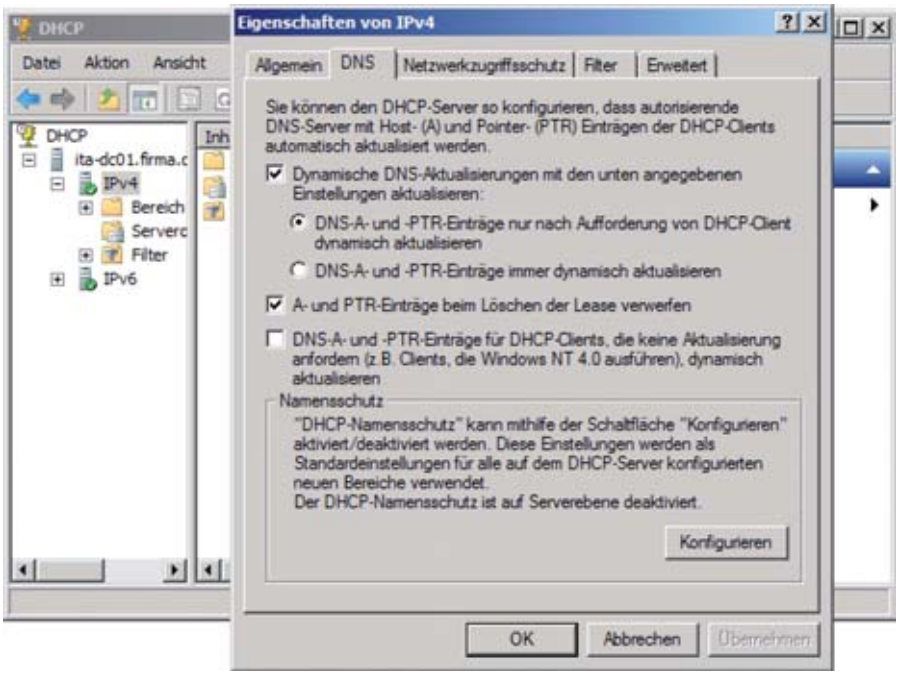


Bild 2: Wünschen es Clientcomputer, kann ein DHCP-Server automatisch Einträge in DNS für sie registrieren

allen notwendigen Records für ihre Clients. Das Standardverhalten für DHCP-Server und -Clients auf Windows-Basis sieht vor, dass der DHCP-Server den PTR-DNS-Eintrag des Clients aktualisiert und der Client sich selbst um seinen A-Record und dessen Wartung kümmert. So sind Vorwärts- und Rückwärtssuche in DNS gewährleistet. Prä-Windows 2000-Maschinen können von diesem Standardvorgehen nicht profitieren, da sie keine Aktualisierungen per DDNS vornehmen. Für sie muss der DHCP-Server beide Records registrieren.

Ein Nachteil dieses Verhaltens macht sich beim Einsatz mehrerer DHCP-Server bemerkbar – etwa dann, wenn DHCP-Server überlappende Bereiche aufweisen oder eine Cluster-Lösung existiert. Denn per Vorgabe wird der Ersteller eines "nur sicheren" DNS-Eintrages automatisch zu seinem Besitzer – und erhält exklusive Aktualisierungsrechte. Erstellt ein Knoten im Cluster einen neuen DNS-Record, wird sein Computeraccount zum Besitzer des Objektes, so dass nur dieser Knoten eine spätere Aktualisierung durchführen kann. Versucht ein anderer Knoten desselben Clusters, den Record zu erneuern, scheitert der Versuch. Selbst in kleineren Umgebungen mit einem einzigen DHCP-Server wird genau dies zu einem Problem: Nämlich dann, wenn der DHCP-Server ausfällt und durch einen neuen ersetzt werden soll. Besoonders schlimm ist dies bei Migrationen, wo IT-Verantwortliche diesen Effekt leicht einmal vergessen.

Arbeiten mit der DHCPUpdate-Proxy-Sicherheitsgruppe

Für diese Szenarien stellt Microsoft eine eigene Lösung (ab Windows 2000 SP2) zur Verfügung: die Sicherheitsgruppe "DHCPUpdateProxy". Sind DHCP-Server Mitglied dieser Gruppe, erstellen sie neue DNS-Objekte nicht mehr mit exklusiven Zugriffsrechten, sondern lassen den Zugriff auf die erstellen Objekte offen – so offen, dass alle in der Domäne angemeldeten Benutzer im der Zugriffsliste des DNS-Objektes "Schreiben"-Berechtigungen erhalten. "Authentifizierte Benutzer" können auf diese Weise DNS-Einträge manipulieren und die DNS-Auflösung der Domäne beeinflussen, ebenso als würden Sie "unsichere dynamische DNS-Updates" erlauben. In Punkto Sicherheit stellt sich dieses Szenario sehr kritisch dar, wenn der DHCP-Server auf einem Domänencontroller läuft und somit auch dessen Einträge ungesichert sind.

Ein unschöner Nebeneffekt, den Sie durch einen cleveren Trick vermeiden: Anstatt die DHCPUpdateProxy-Gruppe zu nutzen, lassen Sie (ab Windows 2000 SP2) den Service unter einen eigenen Konto laufen, und mit Windows Server 2003 sind Sie in der Lage, ein dedizierten DHCP-Benutzer zu

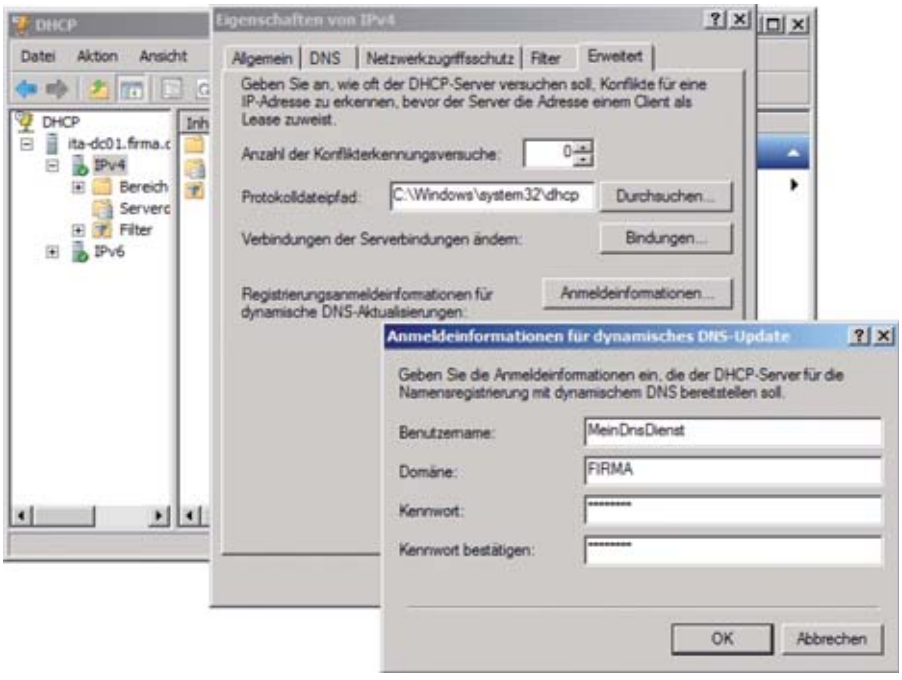


Bild 3: Für das Registrieren von DNS-Einträgen sollten Administratoren einen dedizierten AD-Benutzeraccount verwenden

konfigurieren, der die Registrierung im DNS vornimmt. Erstellen Sie ein dediziertes Benutzerkonto in Active Directory und konfigurieren Sie diesen Benutzer auf allen DHCP-Servern der Domäne, ist das Problem gelöst: Die Server sind, da sie alle im Kontext desselben Benutzers agieren, stets Besitzer der von ihnen erstellten DNS-Objekte und können damit auch Einträge aktualisieren, die von anderen Knoten erstellt wurden. Dennoch gilt die Verwendung der DHCPUpdateProxy-Gruppe als Gefährdung der DNS- und damit auch der AD-Infrastruktur.

DNS aufräumen (lassen)

Mit dem Erstellen und der Aktualisierung füllen Clients und DHCP-Server eigenständig die Zone mit validen Daten. Nur selten ist ein Eingreifen von administrativer Seite notwendig. Was jedoch im Lebenszyklus eines DNS-Eintrages fehlt, ist ein Aufräumvorgang. Fällt der Blick nochmals auf den Registrierungsprozess, so stellen wir fest, dass DHCP-Server nur bei der Erteilung und Erneuerung einer Lease aktiv werden. Nach Ablauf der Lease findet kein Update statt, das den registrierten PTR-Eintrag als "veraltet" markiert. Clientcomputer sind noch weniger in der Lage, ihre veralteten Records zu löschen, sollten sie sie eines Tages nicht mehr benötigen. Ist ein Clientcomputer für längere Zeit offline, ausgeschalten oder einfach nicht am Netzwerk, kann er seine DNS-Daten nicht aktualisieren oder löschen. Es stellt sich also die Frage, wer die veralteten Daten löscht.

Wenn es nicht gerade DNS-Administratoren sein sollen, muss der DNS-Dienst selbst tätig werden. Diese Tätigkeit führen DNS-Server jedoch nicht freiwillig aus – Sie müssen die Server dafür konfigurieren. Die fragliche Funktion nennt sich "Aging and Scavenging" (oder Aufräumvorgang) und beschreibt die Bereinigung veralteter Zonendaten. Dahinter steckt ein Dienst, der DNS-Einträge anhand ihres Aktualisierungsdatums für "zu alt" befindet und anschließend aus der Zone entfernt. Was "zu alt" bedeutet, ist fallspezifisch zu entscheiden und hängt von der Frequenz ab, mit der sich Clients durchschnittlich bei DNS an- und ummelden und wie lange die Leasedauer von IP-Adressen auf dem DHCP-Server ist.

Aufräumvorgang aktivieren

Den Aufräumvorgang müssen Sie an zwei Stellen aktivieren, damit alte Daten bereinigt werden: an der DNS-Zone und am DNS-Server. In den Einstellungen in der Zone definieren Sie, wann ein Eintrag aktualisiert wird und wie lange. Am DNS-Server richten Sie ein, wie häufig der Aufräumvorgang ablaufen soll. Fehlt die Konfiguration an einer dieser Stellen, wird der Aufräumprozess seinen Dienst nicht verrichten – zumindest nicht wie gewünscht.

Für statische oder per Hand eingerichtete DNS-Einträge können Sie den Vorgang auch manuell aktivieren. Standardmäßig werden statisch eingerichtete Einträge nicht aufgeräumt, da sie auch keinen Aktualisierungszeitstempel haben. Seit Windows Server 2008 finden Sie die Aktualisierungszeitstempel auch in der DNS-Verwaltungskonsole in der Übersicht der Einträge, was sehr beim Troubleshooting hilft.

Um die entsprechende Zone für die Bereinigung zu konfigurieren, nutzen Sie in den Eigenschaften der Zone im Reiter "Allgemein" die Schaltfläche "Alte-

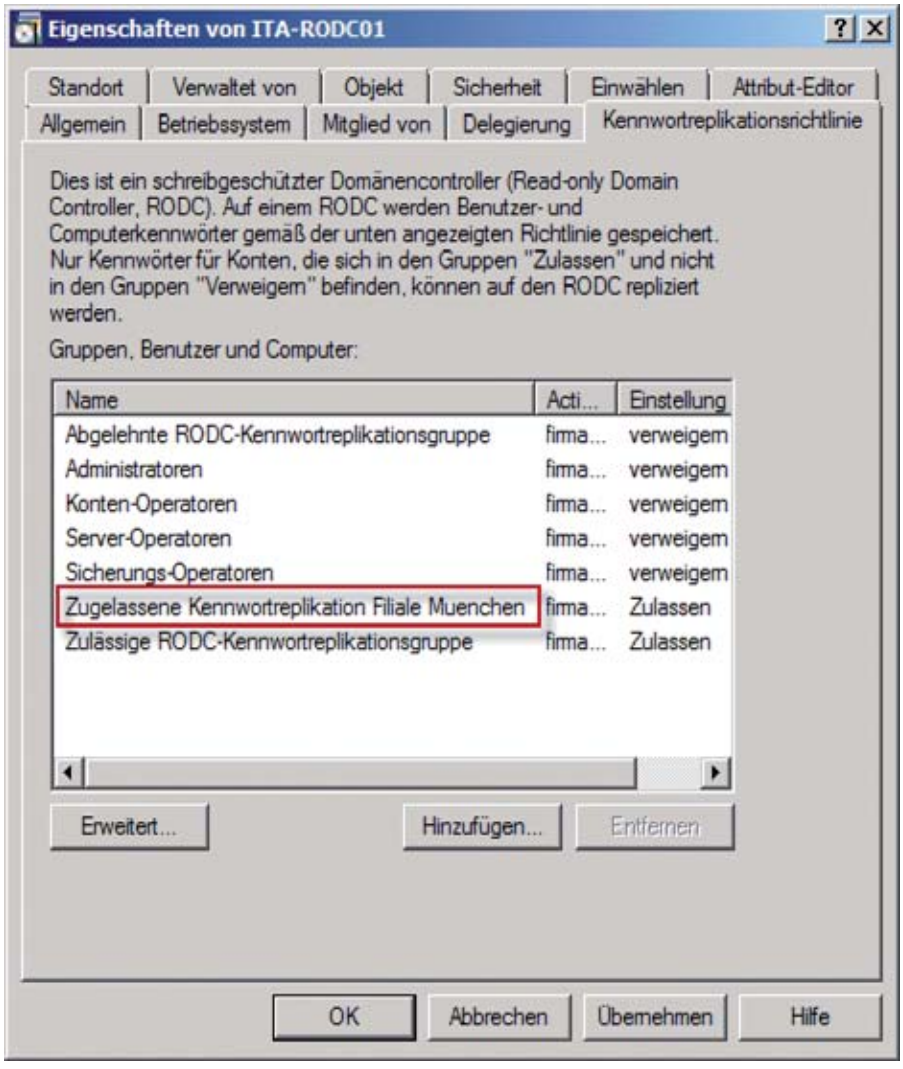


Bild 4: Für die Zone müssen Nichtaktualisierungs- und Aktualisierungsintervall festgelegt werden, nach denen alte Einträge gelöscht werden dürfen

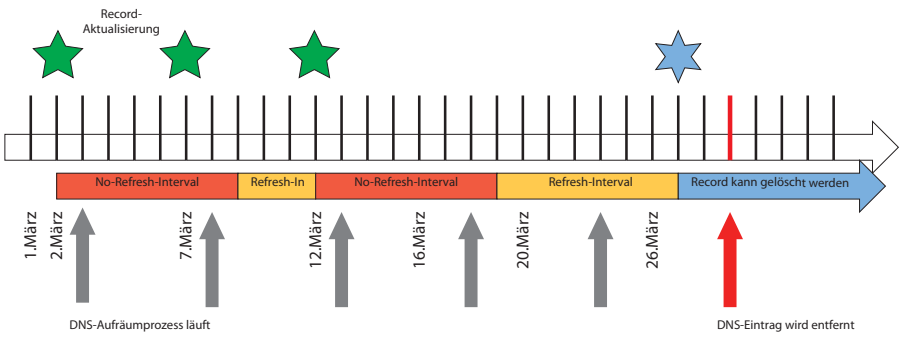


Bild 5: Es ist nicht immer einfach vorhersehbar, wann der Aufräumprozess DNS-Einträge löscht

rung". Im folgenden Dialog aktivieren Sie das "Veraltern" von alten Einträgen. Dabei müssen Sie zwei Zeiten angebe: das Nichtaktualisierungs- und das Aktualisierungsinterval.

Aktualisierungsintervall festlegen

DNS-Server entscheiden anhand des "Nichtaktualisierungsintervalls", ob sie einen Eintrag in der Zonendatenbank erneuern oder die Aktualisierung ignorieren. Dies geschieht, um einen Replikationssturm zu vermeiden, den viele Clients bei der Aktualisierung ihrer Einträge verursachen könnten. Steht das "Nichtaktualisierungsintervall" auf beispielsweise sieben Tage, werden sieben Tage nach der letzten erfolgreichen Aktualisierung des DNS-Eintrags keine Neuerungen entgegengenommen. Erst nach Ablauf dieser Zeit kann der Client wieder erfolgreich seinen Record aktualisieren.

Der Wert des "Aktualisierungsintervalls" räumt Mitgliedsrechnern Zeit ein, ihre DNS-Records zu aktualisieren. Das "Aktualisierungsintervall" beginnt direkt nach dem "Nichtaktualisierungsintervall". In dieser Zeitspanne müssen Clients einen Aktualisierungsversuch unternehmen, um ihre DNS-Einträge vor der Löschung zu bewahren – denn nach Ablauf beider Intervalle, sollte kein Update erfolgt sein, darf der Aufräumprozess des DNS-Servers den Eintrag löschen.

Maßgebend ist ein Zeitstempel, der allen DNS-Records beiliegt. Mit jeder erfolgreichen Aktualisierung wird der Zeitstempel überschrieben und auf die aktuelle Zeit gesetzt. So erkennen DNS-Server, ob sich ein Eintrag gerade im "Nichtaktualisierungs-", im "Aktualisierungs-Intervall" oder in der Aufräumphase befindet.

Aufräumvorgang starten

Abschließend aktivieren Sie den Aufräumvorgang auf Serverebene. In den Eigenschaften des DNS-Servers in der DNS-Konsole wird auf der Registerkarte "Erweitert" die Einstellung "Aufräumvorgang bei veralteten Einträgen automatisch aktivieren" angezeigt. Bei Aktivierung der Einstellung geben Sie ein Zeitintervall für den Aufräumvorgang ein, in dem der DNS-Server nach veralteten DNS-Einträgen suchen soll. Die Einstellung "7 Tage" startet den Aufräumdienst des DNS-Servers einmal wöchentlich. Alle zu diesem Zeitpunkt veralteten Einträge werden aus dem DNS entfernt.

Der Aufräumvorgang und das automatische Update eines DNS-Eintrages werden anhand eines kleinen Beispiels deutlich: An einer DNS-Zone ist für sowohl das "Nichtaktualisierungsintervall" wie auch das "Aktualisierungsintervall" ein Wert von "7 Tage" definiert. Der Aufräumprozess des Servers soll im Fünf-Tages-Rhythmus starten. Nehmen Sie nun einen neuen Clientcomputer am 2. März in das Netzwerk auf, erhält er per DHCP eine IP-Adresse und registriert daraufhin seinen A-Record in DNS. Die DHCP-Leasedauer beträgt zehn Tage und nach Ablauf der Hälfte der Leasedauer versuchen Clients, ihre IP zu erneuern. Daher erfolgt das erste Update des Records am 7. März. Zu diesem Zeitpunkt befindet sich der Client noch im "Nichtaktualisierungsintervall", in dem Aktualisierungen am Eintrag nicht gestattet sind. Der Client versucht es fünf Tage später am 12. März noch einmal und hat Erfolg, da er sich nun im "Aktualisierungsintervall" befindet. Während der Aktualisierung wird der Zeitstempel des Eintrags auf das aktuelle Datum und die aktuelle Zeit gesetzt. Das "Nichtaktualisierungsintervall" beginnt erneut. Am 16. März fährt der Besitzer des Clients in den Urlaub. Der Client ist aus und wird nicht mehr gestartet. Gerade noch im Nichtaktualisierungsintervall vergehen weitere Tage, bis schließlich am 27. März sowohl das Nichtaktualisierungs- als auch das Aktualisierungsintervall verstreichen. Der DNS-Eintrag des Clients ist damit frei für eine Bereinigung. Er wird jedoch nicht zwingend sofort aus der Datenbank entfernt, da der Aufräumprozess im konfigurierten Abstand von fünf Tagen läuft. Schließlich, am 29. März, startet der Prozess, der den Eintrag daraufhin löscht.

Die zu wählenden Einstellungen für die Aktualisierungsintervalle und den Aufräumvorgang sind frei wählbar, Sie sollten sie allerdings mit der DHCP-Leasedauer abstimmen, um ein unnötiges Verschwinden von Einträgen zu vermeiden. Domänenmitglieder, die über statische IP-Adressen verfügen, kümmern sich selber und unabhängig von der Leasedauer um die Aktualisierung. Eine Empfehlung unsererseits ist, dass die Summe aus Nichtaktualisierungsintervall und Aktualisierungsintervall etwas länger ist als die DHCP-Leasedauer, wobei der Nichtaktualisierungsintervall ruhig etwas kürzer als die Hälfte der Leasedauer sein darf. Wie häufig der Aufräumprozess läuft ist fast egal, hier reichen auch wenige Tage. *(jp)*

[1] Konfigurieren von dynamischen DNS-Updates in Windows Server 2003
http://support.microsoft.com/?id=816592

Links


Quelle: Pixel - Fotolia.com

Active Directory für ein neues Windows vorbereiten

Generationenwandel

Die Einführung einer neuen Version von Windows bedeutet Veränderungen in der IT-Infrastruktur. Clientcomputer müssen vorbereitet, verwaltete Installationen angepasst und Helpdesk sowie Mitarbeiter geschult werden. Serversysteme sind ebenfalls einem Wandel unterworfen: Neue Windows Server-Versionen bringen zusätzliche Features, neue Verwaltungsmöglichkeiten oder sind schlicht Voraussetzung für den Betrieb einer Server-Anwendung, die zur Verfügung gestellt werden soll. In diesem Workshop erfahren Sie, wie Sie das Active Directory auf einen solchen Generationenwandel vorbereiten.

Wie bereits im Beitrag über die Active Directory-Versionen auf Seite 8 beschrieben, verfügt jede Windows Server-Version über eine eigene, neue AD-Version. Da das Produkt stetig weiterentwickelt und vorangetrieben wird, wartet jede Iteration mit neuen AD-Funktionen und Verbesserungen auf, die ein Identitäts- und Infrastrukturmanagement einfacher und besser gestalten sollen.

Gründe für den Wechsel

Wer beim Überblicken der Neuigkeiten im Active Directory (AD) keine interessanten Features für sich entdeckt, wird zögerlich mit einem Update der Infrastruktur umgehen. Nur in seltenen Fällen ist die Veröffentlichung eines AD-Features alleiniger Grund für die Aktualisierung aller Domänencontroller (DC) und damit der Domäne oder des gesamten Forests. Ausnahmen wie die Fine-Grained Password Policies oder der AD-Recycle Bin stehen in den neuesten AD-Versionen als Beispiel voran. Vielmehr jedoch spielen häufig andere Faktoren eine entscheidendere Rolle. Der Austausch von Hardware, der meist gleichzeitig ein neues Betriebssystem bedeutet, bietet Gelegenheit, eine neue Windows-Version einzuführen und den ersten DC einer neuen Betriebssystemgeneration in die Domäne und den Forest einzuführen. Andernorts finden Aktualisierungen statt, weil Windows NT und neuerlich Windows 2000 vom Microsoft-Support nicht mehr unterstützt werden. Wer keinen exklusiven Support-Vertrag mit Microsoft abschließen will, muss seine Infrastruktur und seine DCs aktuell halten, was auch aus Sicherheits- und Verwaltungsaspekten über kurz oder lang die einzige Option bleibt.

Unabhängig davon, ob aktuell genutzte Hardware weiterverwendet oder neue Hardware beschafft oder gar virtuell zur Verfügung gestellt wird, bei der Einführung neuer Windows-Versionen, die als Domänencontroller fungieren sollen, muss das AD auf die DC-Promotion vorbereitet werden. Dies umfasst stets die Aktualisierung des AD-Schemas sowie in AD-Updates neuer Windows-Versionen das Nachführen von Sicherheitseinstellungen auf AD-Objekten oder die Erstellung von zusätzlichen Domänengruppen. Ein Schema-Update fügt neue Attribute und Objekte hinzu, die für neue Windows-Features verwendet werden. Auf diese Weise wird für die Unterstützung von Read-Only Domänencontroller (RODC) beim Schema-Update für Windows Server 2008 ein neues Verzeichnisdienstobjekt namens "ntds-dsa-ro" für RODCs angelegt. Für ebengleiches Feature werden weitere Sicherheitsprinzipale in der Zieldomäne eingefügt. Die durchzuführenden Aktionen sind meist in "forestweite" und "domänenweite" Änderungen zu trennen.

Aktualisierung des AD mit ADPrep

Die eigentliche Aktualisierung des Verzeichnisses findet mit "ADPrep" statt, einem auf jedem Windows-Medium mitgelieferten Kommandozeilenprogramm. ADPrep übernimmt sämtliche Aktualisierungsvorgänge selbstständig, muss jedoch mit den korrekten Parametern aufgerufen werden. Da eine AD-Aktualisierung immer aus mehreren Änderungen besteht und entweder forest- oder nur domänenweiten Einfluss hat, führen Sie diesen in getrennten, aufeinanderfolgenden Schritten mit ADPrep aus. Nicht alle Domänen müssen Sie zugleich aktualisieren – es ist möglich, einzelne Domänen, getrennt von allen anderen auf den neuesten Stand zu bringen.

Der Befehl *ADPrep /forestprep* ist in der Regel das erste Kommando, das Administratoren für die Aktualisierung ihres ADs nutzen. Forestprep kümmert sich um das Update der Gesamtstruktur. Darunter fallen Änderungen am Schema und an Objekten gesamtstrukturübergreifender Namenskontexte wie dem Config-NC. In der

Regel werden neue Objekte und Attribute zum Schema hinzugefügt und bestehende Objekte im Konfigurations-NC angepasst und durch weitere Sicherheitseinstellungen ergänzt. Details zu den Änderungen können Sie in den LDF-Dateien auf dem Windows-Datenträger im Ordner "SOURCES \ ADPREP" einsehen. Sie beschreiben alle am Verzeichnis vorgenommenen Modifikationen. Forestprep müssen Sie in der Gesamtstruktur nur einmal ausführen, um das Verzeichnis für eine neue AD-Version oder Domänencontroller neuer Windows-Versionen vorzubereiten. Sie müssen Forestprep auf dem Schema-Master-DC ausführen.

Nachdem Forestprep einige Zeit lang seiner Arbeit nachgegangen ist und die Kommandozeile freigibt, können Sie damit beginnen, ADPrep mit dem Schalter "/domainprep" aufzurufen. Sobald alle Schema-Änderungen von Forestprep durch das Verzeichnis propagiert wurden, nutzen Sie *adprep /domainprep* auf dem DC mit der Infrastruktur-Master-FSMO-Rolle einer Domäne. Domainprep stellt sicher, dass Pro-Domänen-Änderungen wie neue Domänengruppen oder ACL-Änderungen in der Domänenpartition erstellt werden. Im Gegensatz zu Forestprep schließt DomainPrep die Aktualisierung des Domänen-NCs recht zügig ab. Domainprep müssen Sie in jeder Domäne ausführen, die neue Domänencontroller bekommen soll.

Um Unterstützung für Read-Only-DCs zu bieten, müssen Sie das Active Directory gesondert für deren Einsatz vorbereiten. Hierzu bietet ADPrep seit Windows Server 2008 einen eigenen Schalter namens "/RODCPrep". Diese Option versucht die ACLs aller Anwendungspartitionen im Verzeichnis für die RODC-Replikation vorzubereiten. In Einzelfällen bricht RODCPrep mit der folgenden Fehlermeldung ab:

```
"Adprep could not contact a replica
  for partition DC=xx,DC=domain,
  DC=com. Adprep failed the
  operation on partition
  DC=xx,DC=domain,DC=com. Skipping
  to next partition".
```

Diese Fehlermeldung ist Folge einer von zwei möglichen Ursachen:

1. Es gibt eine Referenz auf eine Anwendungspartition, die von keinem DC in der Gesamtstruktur mehr repliziert oder gepflegt wird. Es gibt also eine Anwendungspartition, die auf keinem DC verfügbar ist.
2. Der Infrastrukturmaster der Anwendungspartition konnte nicht kontaktiert werden.

Zur Lösung des Problems Nummer eins ist es ausreichend, wenn Sie die verwaiste Anwendungspartition mit NTDSUtil entfernen – natürlich nur dann, wenn diese nicht mehr benötigt werden sollte. Hierzu verwenden Sie das Kommando

```
delete nc "DC=xx,DC=domain,DC=com"
```

im entsprechenden NTDSUtil-Untermenü. Sollte der Infrastrukturmaster der Anwendungspartition nicht mehr gefunden werden können, wählen Sie einen neuen Rolleninhaber für die Anwendungspartition. Der schnellste Weg zum Ziel führt über ADSIEdit. Mit ADSIEdit bauen Sie eine Verbindung zur Anwendungspartition auf, in der das Attribut "fSMORoleOwner" angepasst werden muss. In der Regel verweist das Attribut auf einen Domänencontroller, der zwischenzeitlich nicht mehr existiert und bereits heruntergestuft wurde.

In der MS Knowledge Base befindet sich zu diesem Problem von RODC ein Artikel unter [1]. Mehr zu Infrastruktur-Mastern auf Anwendungspartitionen liefert der Blog-Artikel [2]. Beide Probleme entstehen, weil keines der verfügbaren Verwaltungswerkzeuge in der Lage ist, die Vitalität der Infrastrukturmaster oder der replizierten Anwendungspartitionen zu prüfen.

Vorsicht bei Schema-Updates

Bei allem Eifer und aller Freude auf eine aktualisierte Infrastruktur ist Vorsicht geboten: Änderungen am AD-Schema sind irreversibel – Sie können sie nicht mehr rückgängig machen, sind sie erst einmal in der Gesamtstruktur repliziert. Während Sie Sicherheitseinstellungen und Domänengruppen nach einem AD-Update rückgängig machen oder löschen könnten, lassen sich neu erstellte AD-Objektdefinitionen im Schema nur deaktivieren – Löschen ist nicht möglich. Um ein Schema-Update rückgängig zu machen, müssten Sie im Ernstfall ein Forest-Recovery durchführen, das mit Zeit- und Datenverlust verbunden ist und ein Zerstören aller bis auf einen Domänencontroller pro Domäne nach sich zieht.

AD-Updates sollten Sie also äußerst vorsichtig handhaben und vorab gut planen. Haben Sie bisher nur Schemaaktualisierungen aus dem Hause Microsoft eingespielt, dürfen Sie sich auf der sicheren Seite fühlen. Die Schemen aus Redmond werden mehrfach geprüft und besitzen jeweils eindeutige Namens- und ID-Konventionen, die Attributdopplungen und Inkonsistenzen nahezu ausschließen.

Bei einem AD mit Drittanbietererweiterungen sieht das anders aus – hier können Probleme auftreten, sollten Drittanbieter nicht auf eindeutige Attribut- und Objektnamen und eindeutige ObjektIDs geachtet haben. Aus diesem Grund sollten Administratoren, die für die Unterstützung von Drittanbietersoftware oder eigenen Anpassungen andere Schemaänderungen durchführen mussten, besondere Vorkehrungen treffen. Welche, zeigt Ihnen der Artikel "Schemaerweiterungen für neue Anwendungen" auf Seite 67.

Schritt für Schritt zum AD-Update

In jedem Fall gilt: Ein AD-Update oder eine Schema-Aktualisierung sollte vorher in einer produktivnahen Testumgebung geprüft werden.

Phase 1: Ist-Zustand sicherstellen

Bevor Sie sich an Änderungen im Verzeichnis trauen, sollten Sie eine kurze Gesundheitsprüfung des gesamten AD durchführen. Dies hilft, Probleme nach einem Update besser einzugrenzen, da Sie sich zuvor vergewissern, dass das Verzeichnis vor der Änderung fehlerfrei funktionierte. Gute Anlaufpunkte sind DCDiag oder die Ereignisanzeige auf den Domänencontrollern. Läuft mit den DCs etwas schief, finden Sie Auffälligkeiten in jedem Fall dort.

Mit Repadmin sollte Sie die Replikationstopologie überprüfen. Tauchen hier Fehler auf oder sind einige Knoten nicht erreichbar, kann das zu einer Verzögerung des Schema-Updates führen. Domainprep kann nur korrekt ausgeführt werden, wenn der Schalter Forestprep zuvor korrekt ausgeführt und die Updates an alle Domänencontroller repliziert wurden.

Phase 2: Update durchführen

Nun ist es an der Zeit, die Updates durchführen. ADPrep befindet sich auf dem Windows-Medium im Ordner "SOURCES \ ADPREP". Je nach Architektur müssen Sie die richtige Windows-CD/DVD einlegen, damit 32 Bit Windows-Versionen die 32 Bit-Version von ADPrep ausführen können und 64 Bit-Versionen von Windows die entsprechende. Da seit Windows Server 2008 R2 nur noch ein 64 Bit-Medium existiert, befinden sich im ADPREP-Ordner der DVD zwei Versionen von ADPREP: *adprep32.exe* und ADprep für 64 Bit.

Für das Update sollten Sie ein Zeitfenster mit wenig Last auf dem Schema-Master wählen. Trotz der deaktivierten Outbound-Replikation muss der DC weiterhin Verbindungen von Clients, etwa Authentifizierungs- oder DNS-Anfragen beantworten.

Phase 3: Update überprüfen

Ist der Aktualisierungsvorgang beendet, verifizieren Sie das Update. Hierzu sollten Sie die Bildschirmausgabe von ADPrep überprüfen und das ADPrep-Logfile im Ordner "%Systemroot%\system32\debug\adprep\logs" durchsehen. Sind die Ausgaben des Kommandozeilenprogramms zufriedenstellend und der Eventlog des Schema-Masters frei von Fehlermeldungen, können Sie die Replikation wieder starten.

Phase 4: Administrative Gruppen zurückkonfigurieren

Sind alle Aktualisierungsarbeiten abgeschlossen, sollten Sie das Benutzerkonto wieder aus der Gruppe der Enterprise-Admins, zumindest aber aus der Gruppe der Schema-Admins entfernen. Die Berechtigungen werden nicht mehr benötigt. Somit sollte Ihr Update erfolgreich abgeschlossen sein. *(jp)*

Links

[1] Error message when you run the "Adprep/rodcprep" command in Windows Server 2008: "Adprep could not contact a replica for partition DC=DomainDnsZones,DC=Contoso,DC=com", http://support.microsoft.com/kb/949257/

[2] How many Infrastructure Masters do you have? http://msmvps.com/blogs/ulfbsimonweidner/archive/2008/07/31/how-many-infrastructure-masters-do-you-have.aspx

Schemaerweiterungen für neue Anwendungen

Richtig in die Einbahnstraße


Quelle: Pixelio.de

Das Schema ist ein kritischer Teil des Active Directory, denn ist das Schema beschädigt oder nicht korrekt, werden falsche und nicht funktionierende Objektinstanzen mit unzureichenden Attributen daraus erstellt. Im schlimmsten Fall müssen Sie Ihren kompletten AD-Forest und alle Domänencontroller wiederherstellen, wenn beim Schema-Update etwas schief läuft. Dieser Workshop zeigt Methoden, die Ihnen helfen, Schemaerweiterungen sicher durchzuführen.

Das Schema des Active Directory (AD) ist immer wieder Änderungen unterworfen. Gerade beim AD-Updateprozess oder bei der Installation von AD-nutzenden Drittanbieteranwendungen werden neue Attribut- und Objektdefinitionen für neue Objekte oder Active Directory-Funktionalitäten in das Schema eingespielt. Der Beitrag "Generationenwandel" auf Seite 64 in diesem Sonderheft zeigt, wie der AD-Updateprozess mit Hilfe von ADPrep und seinen zahlreichen Schaltern durchlaufen wird. ADPrep selbst führt seinerseits eine Schemaaktualisierung durch und bringt das Verzeichnis auf den aktuellsten Stand, bevor der erste Domänencontroller (DC) einer neuen Betriebssystemgeneration installiert und zum DC promotet wird. Dieser Prozess bereitet neueste AD-Funktionen vor, damit diese bei der Aktualisierung weiterer DCs eingesetzt werden können.

Schemaaktualisierungen sind dabei nicht ganz ohne, denn der gesamte Forest, nicht nur einzelne Domänen, basiert auf dem Schema. Dabei lassen sich Aktualisierungen an Objekten und Attributen der Schema-Partition maximal deaktivieren, aber niemals rückgängig machen. Daher gilt besondere Vorsicht beim Einspielen der Updates. Vor und während des Updateprozesses gibt es jedoch einige Vorkehrungen, die Sie treffen können, um im schlimmsten Fall nicht im Regen zu stehen und das Schema retten können – ohne ein aufwändiges Forest-Recovery. Das Forest-Recovery besteht dabei aus dem Restore aller DCs der Gesamtstruktur, die die Schemaänderung bereits repliziert haben. Das kann im Worst Case bedeuten, dass Sie alle DCs der Gesamtstruktur per Wiederherstellung zurückholen müssen.

Testen, prüfen, sichern

Bevor Sie mit der Aktualisierung des Schemas beginnen, sollten Sie das Update proben und in einer möglichst lebensnahen Testumgebung durchspielen. Probleme können nicht nur mit dem Active Directory selbst, sondern auch mit anderen Applikationen auftreten, die mit den durchgeführten Aktualisierungen nicht zurechtkommen. Die einzelnen Schritte zur Schemaaktualisierung sollten Sie also in einer Testumgebung nachvollziehen, um Probleme und unerwartete Zwischenfälle zu vermeiden. Bereits virtualisierte Domänencontroller bieten sich für diese Zwecke sehr gut an: Sie können diese klonen und in einem separaten Testnetzwerk wiederherstellen, um das Schemaupdate abgeschottet zu prüfen. Bei der Auswahl der Testdomänencontroller sollten Sie dabei nicht nur die Forest-Root-Domäne berücksichtigen, sondern jeweils möglichst ein Exemplar aller verfügbaren Domänen der Gesamtstruktur. Vor dem Klonen der virtuellen DCs sollten Sie diese, falls möglich, zu Globalen Katalogen (GC) machen. Ändert sich mit dem Schemaupdate die Indexierung des GCs, können Sie die Funktionalität nur auf Globalen Katalogen prüfen – was die Notwendigkeit eines GCs im Testnetzwerk nachdrücklich belegt.

In einem separaten Netzwerk lassen sich GCs jedoch nur mit Mühe erstellen, da Domänencontroller erst mit der Eigenwerbung als GC beginnen, wenn sie von jeder Domänenpartition in der Gesamtstruktur einen Nur-Lese-Speicher aufbauen konnten. Sind die DCs aber im Testnetz abgeschottet und erreichen manche Domänen nicht, werden sie niemals den fertigen GC-Status erlangen und sich selbst als "kompletten" GC betrachten. Virtuelle DCs sollten also nach Möglichkeit bereits vor dem Klonen GCs sein.

Vor der eigentlichen Aktualisierung müssen Sie sich um einige AD-Funktionen kümmern, um die einwandfreie Propagierung der Änderungen sicherzustellen. Eine der wichtigsten Komponenten ist dabei die AD-Replikation zusammen mit der SYSVOL-Replikation, die letztlich alle Änderungen an alle DCs der Gesamtstruktur verteilt. Die Überprüfung der AD-Replikation erfolgt dabei jeweils mit *repadmin* und seinen Parametern. Gibt es Probleme bei der Replikation, sollten Sie diese auf alle Fälle vor der Schemaerweiterung bereinigen, damit alle DCs Änderungen übernehmen können. Ist die SYSVOL-Replikation nicht intakt, werden Berechtigungsanpassungen an Gruppenrichtlinien unter Umständen nicht durchgeführt. In jedem Fall sollten Sie auch die SYSVOL-Replikation auf ihre einwandfreie Funktion und prüfen. In den Artikeln zur AD-Replikation (Seite 138) und der FRS nach DFS-R-Migration (Seite158) beschreiben wir Überprüfungsmöglichkeiten und das Monitoring der Replikation im Detail.

Die Schemaerweiterung ist auch ein guter Zeitpunkt, um die Dokumentation aller Domänencontroller, der installierten DNS-Servern und der FSMO-Rolleninhaber aufzufrischen. Die Überprüfung stellt sicher, dass Ihnen alle Rolleninhaber, alle DCs und die DNS-Server bekannt sind und diese funktionieren, so dass Sie ihre Funktion nach dem Schemaupdate überprüfen können.

Vor dem Einspielen der Erweiterungen sollten Sie eine Liste von AD-abhängigen Anwendungen erstellen. Diese Anwendungen müssen Sie nach dem Update – im besten Fall bereits als eigene Instanz im Testnetzwerk – überprüfen, um frühzeitig Probleme oder Fehler zu entdecken. Ein notwendiges Forest-Recovery auf Grund einer nicht kompatiblen Anwendung gilt es zu vermeiden – aus diesem Grund schadet eine Checkliste aller verfügbaren AD-Anwendungen, seien es Microsoft-Produkte oder Drittanbietersoftware, nicht. Die Liste sollte auch aufzeigen, welche Domänencontroller die Anwendungen nutzen, falls eine festkodierte Auswahl eines DCs innerhalb der Anwendung stattfindet.

Als letzten Schritt vor dem Update führen Sie eine Systemstatussicherung aller Domänencontroller durch. Sollte etwas schief gehen und ein Forest-Recovery notwendig werden, der eine Wiederherstellung aller DCs nach sich zieht, erledigen Sie diese Notfallwiederherstellung durch umfangreiche und aktuelle Backups einfacher und schneller. Sollen nicht alle DCs gesichert oder wiederhergestellt werden, sichern Sie zumindest so viele DCs pro Domäne, dass ein störungsfreier Betrieb für jede Domäne möglich ist. Dies involviert mindestens zwei gesicherte DCs pro Domäne, je nach Last und Anzahl der Benutzer und Applikationen, die die DCs bedienen müssen, deutlich mehr.

Domänencontroller separieren

Obwohl die Schemaupdates eine Einbahnstraße darstellen, gibt es die ein oder andere Möglichkeit, wie Sie sich vor einem kompletten Forest-Recovery im Fehlerfall schützen und den schlimmsten Fall abwenden. Eine Möglichkeit ist das Separieren von Domänencontrollern während der Schemaaktualisierung, ähnlich wie das Abschotten der DCs im Testnetzwerk. So können Sie ausgewählte DCs zuerst mit dem Schemaupdate bestücken und auf Richtigkeit testen, bevor dann alle DCs damit in Berührung kommen.

Hierzu bieten sich die Funktionen der standortübergreifenden Replikation des Active Directory an, die nicht, wie die standortinterne Replikation, sofort erfolgt, sondern sich über einen Zeitplan steuern lässt. Für die ausgewählten DCs erstellen Sie dazu einen oder mehrere neue Standorte auf Basis möglichst kleiner IP-Subnetze, etwa der IPs der jeweiligen DCs, mit einer entsprechend kleinen Subnetzmaske (etwa "/29" für wenige Hosts). Sogar eine Subnetzmaske von 32-Bit (255.255.255.255) ist möglich, um nur einen bestimmten DC anhand seiner IP-Adresse einem Standort zuzuordnen. Sollte ein DC in mehrere Standorte passen, zum Beispiel weil es die Subnetze 10.11.12.0 mit 255.255.255.0 und 10.11.12.13 mit 255.255.255.255 gibt, die unterschiedlichen Standorten zugeordnet sind, wählen Sie denjenigen mit dem kleineren Bereich (also in unserem Beispiel den zweiten). Sind die DCs in einem einzigen Standort gruppiert, müssen Sie entweder die Vorgabe-Standortverknüpfung anpassen oder eine neue erstellen, um die Replikation zwischen dem Hauptstandort mit allen

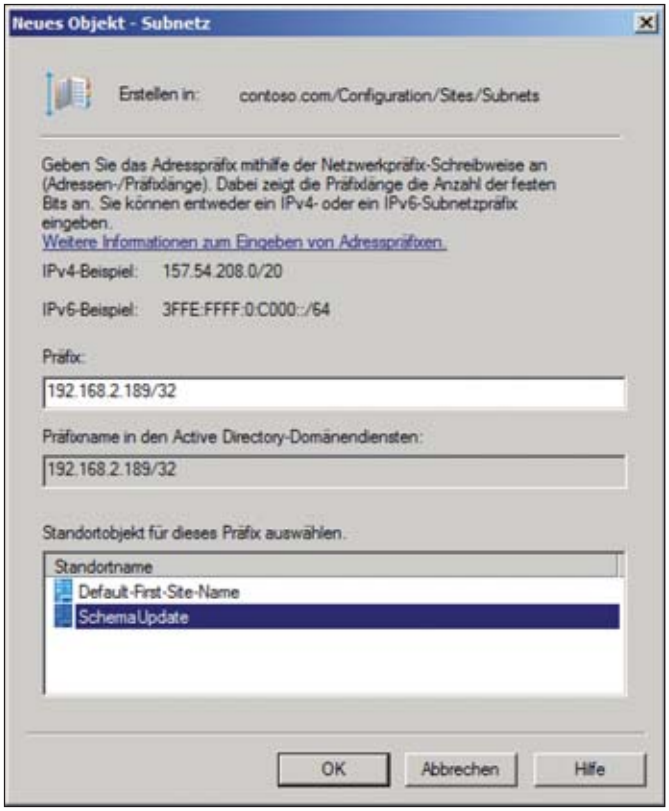


Bild 1: Die Separierung der Domänencontroller für das Schemaupdate kann über die Standortdefinitionen und die Abschottung der Replikation erfolgen

DCs und dem Update-Standort zu kontrollieren. Im "Allgemein"-Reiter konfigurieren Sie über den Button "Zeitplan ändern" den Replikationszeitplan. Da es nicht gewünscht ist, dass sich die Schemaänderungen während des Updates zu allen anderen DCs replizieren, wählen Sie hier einen fiktiven Wert für den Zeitplan. Findet das Schemaupdate beispielsweise am Wochenende statt, erlauben Sie die Replikation zwischen den Standorten Donnerstagnacht – also zu einer Zeit, die die Updatearbeiten sicher nicht behindert.

Kandidaten für die Insellösung im eigenen Standort sind der Schemamaster-DC, auf dem das Schemaupdate ausgeführt werden muss und mindestens ein weiterer DC der gleichen Domäne. Idealerweise ergänzen Sie diese Auswahl um jeweils einen DC einer anderen Domäne. Hierbei müssen Sie auch die Anforderungen des jeweiligen Updates überprüfen. Beim Vorbereiten des Forests und der Domänen auf eine neue Windows-Version mit ADPrep wird zum Beispiel für Forestprep der Schemamaster benötigt, für Domainprep aber der Infrastrukturmaster. Führen Sie in diesem Fall beide Rollen auf den Insel-DCs aus. Für die Überprüfung der Indexierung sollten die Insel-DCs vor ihrer Verschiebung ebenfalls Globale Kataloge sein.

Zusätzlich zur Separierung ist es von Vorteil, einen Domänencontroller pro Domäne offline zu schalten. Fehler und Probleme, die Sie erst nach dem Testlauf in einem eigenen Subnetz feststellen, nachdem alle DCs die Änderungen über die Replikation erhalten haben, führen zum Rückspielen einer Sicherung. Schalten Sie einen DC für die Update- und die anschließende Verifizierungsphase offline, kann er ausgeschaltet oder vom Netz getrennt das "alte" Schema weiterhin beibehalten. Bei Problemen, wenn Sie alle anderen DCs herunterfahren und restaurieren, nehmen Sie diesen Offline-DC online, so dass er die die notwendigen Domänenfunktionalitäten in der Domäne aufrechterhält. In der Praxis hat es sich bewährt, einen speziellen Offline-DC zu verwenden, den Sie hierfür – gegebenenfalls auf einer Virtualisierungsplattform – neu installieren. Dies empfehlen wir, weil Sie nicht immer genau wissen, welche DCs statisch in irgendwelchen Anwendungen konfiguriert wurden. Ist der Offline-Domänencontroller dann längere Zeit nicht verfügbar, verursachen die Applikationen Probleme, wenn sie nicht richtig konfiguriert wurden.

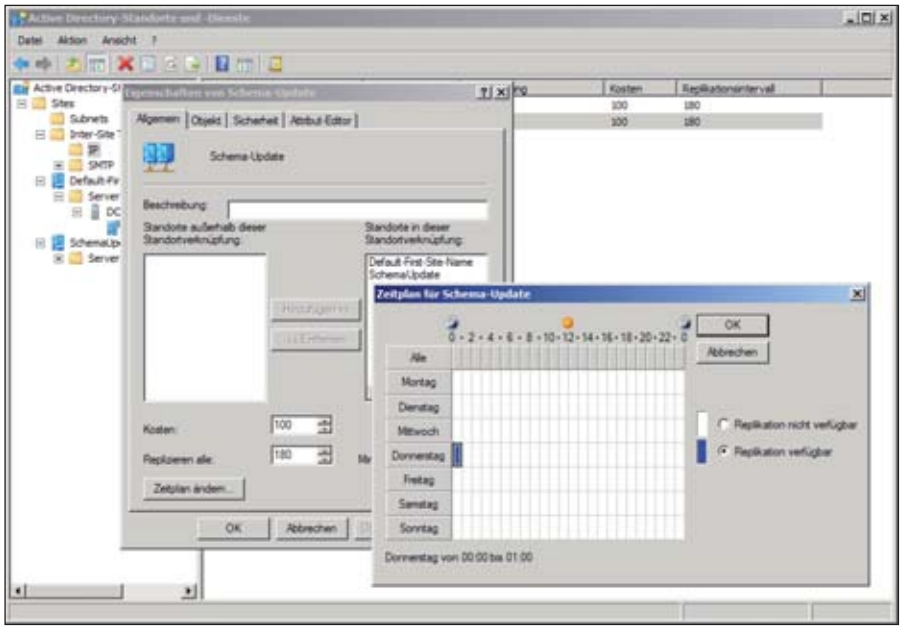


Bild 2: Schemaupdate-DCs in einer eigenen Site lassen sich über den Zeitplan für die Standortreplikation zu einer "Insel" konfigurieren

Replikation minimieren oder stoppen

Mit der Trennung in einen separierten Standort vermindern Sie das Risiko eines generellen Schemaupdate-Problems. Sollte etwas mit dem Schemaupdate grundsätzlich nicht stimmen, sind maximal die Insel-DCs verloren und müssen restauriert, und idealerweise das AD entfernt und die Server neu zu DCs promoted werden. Problematisch sind jedoch weiterhin Anwendungen, die möglicherweise nicht mit dem Schemaupdate operieren können.

Diese müssen Sie kontrolliert testen, ohne die Gesamtstruktur nach dem Inseltest zu aktualisieren. Die Lösung dieses Problems liegt in der Deaktivierung der Replikation auf allen DCs. Das Befehlszeilentool Repadmin erlaubt es, DCs die eingehende und ausgehende Replikation von Änderungen zu verbieten. Wird allen DCs im Hauptstandort das Replikationsrecht genommen, verbreiten sich eventuelle Änderungen des Schemas nicht. Umgekehrt kontrollieren Sie auf diese Weise, welche DCs die Schema-Änderungen wohin replizieren, indem Sie kontrolliert die Replikationssperre aufheben und ausgewählten DCs erlauben, eingehende und ausgehende Replikation durchzuführen.

Der Befehl zur kompletten Deaktivierung der Replikation lautet

```
Repadmin /options {dc-name}
  +DISABLE_INBOUND_REPL
  +DISABLE_OUTBOUND_REPL
  +DISABLE_NTDSCONN_XLATE
```

Anwendungen, die ganz besondere DCs für ihre Zwecke nutzen, testen Sie so mit dem Schemaupdate. Funktioniert die Applikation nach dem Schemaupdate auf dem Ziel-DC, kann das Update, zumindest bezüglich dieser Anwendung, auf alle DCs ausgerollt werden. Funktioniert die Anwendung nicht mit den Schemaänderungen auf dem Ziel-DC, muss ein Notfallplan greifen und unter Umstän-

Bild 3: Die deaktivierte Replikation weist Repadmin nach der Ausführung aus

den das Schemaupdate mittels Restore auf den bereits aktualisierten DCs durchgeführt werden.

Um die eingehende Replikation für einen DC aufzuheben, genügt es, anstelle des Pluszeichens vor dem *DISABLE_INBOUND_REPL*-Befehl ein Minuszeichen zu setzen:

```
repadmin /options {dc-name}
  -DISABLE_INBOUND_REPL
```

Natürlich muss die ausgehende Replikation an einem direkten Replikationspartner bereits erlaubt worden sein – ansonsten werden keine Aktualisierungen ausgetauscht.

Zum Abschluss des Schemaupdates, wenn die Schemaanpassungen verifiziert wurden und alle Überprüfungen positiv verlaufen sind, aktivieren Sie die Replikation:

```
Repadmin /options {dc-name}
  -DISABLE_INBOUND_REPL
  -DISABLE_OUTBOUND_REPL
  -DISABLE_NTDSCONN_XLATE
```

Die Umgebung wird einige Zeit benötigen, die entsprechenden Änderungen in alle Winkel des Verzeichnisdienstes zu replizieren. Erst wenn alle DCs das Schemaupdate erhalten haben und keine Fehler aufgetreten sind, ist die Arbeit beendet. Um den Stand der Replikation zu überprüfen, nutzen Sie Repadmin mit dem Schalter "/replsum":

```
repadmin /replsum /bysrc /bydest
  /sort:DELTA
```

Zeigen die DCs auch nach einiger Zeit keine Fehler oder größere Deltas an, hat die Schemaerweiterung alle DCs erreicht.

Domänen- und Forestupdates prüfen

Domänen- und Forestupdates, die zur Einführung neuer Domänencontroller mit neuen Windows Server-Versionen dienen, können mit einfachen Mitteln repliziert werden. Die aktuelle Schemaversion eines DC lässt sich per Registry und mit LDP in Erfahrung bringen. Domänencontroller legen in der Registrierung im Schlüssel "Schema Version" die aktuelle Schemaversion ab: HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ NTDS \ Parameter. Der Wert der Schemaversion sollte der aktuell eingespielten entsprechen:

- Windows 2000: Schema Version 13
- Windows Server 2003: Schema Version 30
- Windows Server 2003 R2: Schema Version 31
- Windows Server 2008: Schema Version 44
- Windows Server 2008 R2. Schema Version 47

Auch im Verzeichnis sind die Versionsdaten des Schemas hinterlegt. Im Objekt "CN=Schema,CN=Configuration, DC=domaene, DC=tld" im Attribut "objectVersion" finden Sie die entsprechende Information. Außerdem werden während der Aktualisierung einige Verzeichnisdienstcontainer und Objekte erstellt, die über den Verlauf eines Updates informieren. In "CN=DomainUpdates,CN=System,DC=domaene,DC=tld" werden die Domänenupdates aufgelistet. Der Container "System" ist in "Active Directory-Benutzer und -Computer" nur sichtbar, wenn die erweiterten Funktionen in der MMC aktiviert wurden. Im Subcontainer "Operations" werden die durchgeführten Schritte per GUID als weitere Subcontainer angelegt. Scheitert das Update aus bestimmten Gründen, könnte der Microsoft-Support hieraus wichtige Schlüsse ziehen.

Schemaupdates von Drittanbietern prüfen

Wenn Sie Schemaupdates von Drittherstellern einspielen wollen, sollten Sie diese zunächst überprüfen. Für Schemaerweiterungen gibt es einige Werte, die innerhalb der Gesamtstruktur eineindeutig sein müssen. Diese sind:

- Die Namen des Attributes (also Name, LDAPDisplayname et cetera): Diese sollten nicht zu generisch sein, um zu vermeiden, dass ein späteres Update eines anderen Herstellers (oder des Windows- oder Exchange-Schemas) den gleichen

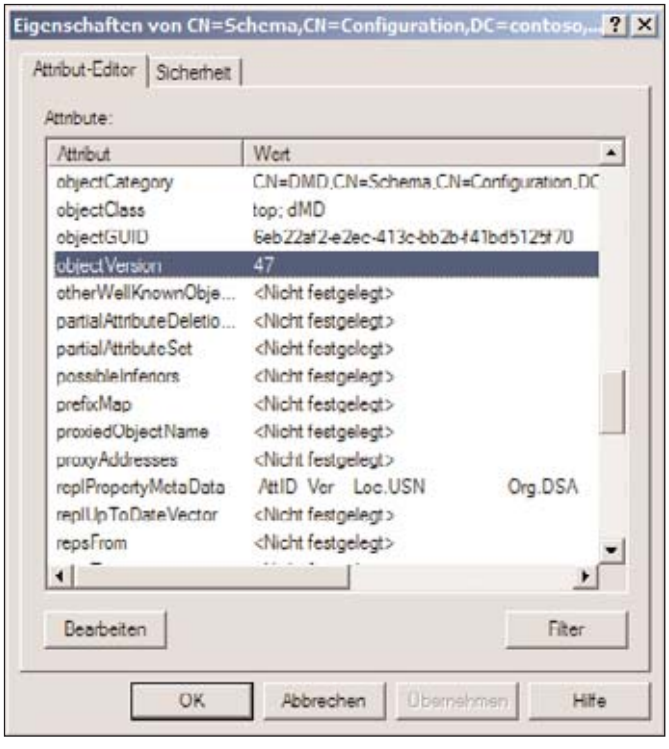


Bild 4: Die aktuelle Version des AD-Schemas ist im Attribut "objectVersion" des Schema-NCs ersichtlich

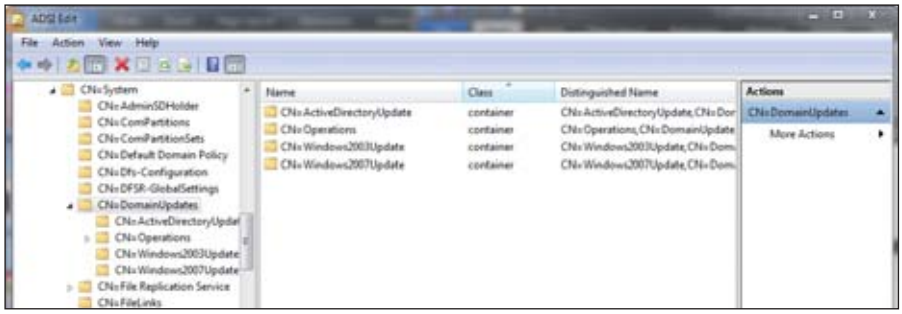


Bild 5: Für Updates am Schema und an der Domäne erzeugt das Active Directory entsprechende Container im "System"-Container der Domänenpartition

Namen verwendet. Wie empfehlen, dass alle Namen einen "Prefix" haben, der dem Hersteller entspricht (also "meineFirma-Kostenstelle" anstatt "Kostenstelle").

- OIDs: Dies sind Zahlen, die ein Objekt oder Attribut eindeutig markieren. Hierfür wird ein Zahlenbereich dem Unternehmen zur Verfügung gestellt (kann zum Beispiel bei IANA beantragt werden). Die OIDs unterhalb dieses Raums vergeben Sie selbst. Auch hier ist wichtig, dass Sie jede OID nur einmal verwenden. Zum Beispiel könnten Sie, wenn dem Unternehmen die "Root-OID" 1.2.3.4.5 zugeordnet ist, definieren, dass für das Active Directory die 1.2.3.4.5.1 verwendet wird, und die Objekte dann 1.2.3.4.5.1.1.x erhalten und Attribute 1.2.3.4.5.1.2.x.
- LinkID: Die LinkID ist die Festlegung, ob das Objekt ein Vorwärts- oder Rückwärtslink ist. LinkID ist eine Zahl, die nur einmal im Forest (auch für zukünftige Updates) vergeben werden darf. 3rd-Party Hersteller sollten möglicherweise keine LinkIDs einsetzen, da sich nicht sicherstellen lässt, dass diese nicht von späteren Microsoft-Updates oder anderen Herstellern verwendet werden. Besser ist es hierbei (ab Windows Server 2003) den "Auto-Link-ID-Mechanismus" zu verwenden. Hierbei wird einem Attribut kein fester Wert als Link zugeordnet, sondern dem Attribut mit dem Forward-Link als LinkID der Wert "1.2.840.113556.1.2.50". Ist das Attribut erstellbar, lässt sich ein weiteres Attribut mit einem Rückwärtslink hierauf konfigurieren. Dabei wird dem Attribut dann einfach als Wert für die LinkID der Name des Vorwärts-Link-Attributes zugewiesen. Der Server kümmert sich dann automatisch um die Erstellung einer zufällig generierten LinkID, die nicht verwendet wird.
- MapiID: Die MapiID wird nur für Attribute benötigt, die in der globalen Adressliste von MS Exchange sichtbar gemacht werden sollen. Für diese gilt das gleiche wie für die LinkID – sie muss eineindeutig sein und ist nicht reservierbar. Ab Windows Server 2008 gibt es daher analog zur LinkID den Auto-MapiID-Mechanismus, hierfür müssen Sie der MapiID lediglich den Wert "1.2.840.113556.1.2.49" zuweisen.

Werden diese Regeln von den Schemaerweiterungen der Drittherstellern eingehalten, ist es unwahrscheinlich, dass es mit zukünftigen Schemaerweiterungen Probleme gibt. Microsoft hat für die Prüfung von Schemaerweiterungen anderer Anbieter ein PowerShell-Skript zur Verfügung gestellt, das die LDF-Files und Textdateien, die die Änderungen am Verzeichnis repräsentieren, vorab prüft und Warnungen zu Problemen ausgibt. Das Skript *ADSchemaExtensionConflictAnalyzer.ps1* ist kein Bestandteil der AD-Module in Windows Server 2008 R2 und Sie müssen es daher bei Microsoft herunterladen [1]. Das Tool kann die aktuelle Schemapartition aus dem Livesystem lesen und verwerten. Für Testzwecke oder für die Verwendung abseits der Produktionsumgebung füttern Sie es mit einem Export der aktuellen Schemapartition. Das aktuelle Schema exportieren Sie dazu bequem per Kommandozeile:

```
ldifde -f {aktuelles-Schema.ldf} -d
  SchemaNamingContext
```

Anschließend setzen Sie damit das Skript ein:

```
ADSchemaExtensionConflictAnalyzer.ps
  1 -inputfile {Neue-Schemaerweite-
  rung.ldf} -outputfile
  {Resultate.ldf} -CurrentSchema
  {aktuelles-Schema.ldf}
```

Möchten Sie das Skript gegen die produktive Active Directory-Umgebung laufen lassen, verzichten Sie auf den Schalter "-CurrentSchema" – das Skript weiß sich dann selbst zu helfen. Gefundene Inkonsistenzen oder Probleme stellt das Skript farbig am Bildschirm dar und schreibt diese als Export in das Outputfile.

Ein letztes Wort zu Schemaerweiterungen mit ADPrep: Diese sollten Sie nicht mit *ADSchemaExtensionConflictAnalyzer.ps1* überprüfen. Die Überprüfung richtet zwar keinen Schaden an, meldet aber Fehler, die bei einem richtigen Update keine Bedeutung haben. Grund hierfür ist, dass ADPrep als priviligierter Prozess läuft und deshalb Änderungen durchführen darf, die normalen Schemaerweiterungen nicht erlaubt sind.

Fazit

Schemaupdates sind von Haus aus echte Einbahnstraßen. Wissen Sie nicht genau, was zu tun ist oder was Sie in Ihre Umgebung laden, kann es ein böses Erwachen geben, wenn die Änderungen in die Gesamtstruktur repliziert werden. Mit den richtigen Vorkehrungen und dem Überwachen der Schemaaktualisierung verhindern Sie zwar kein korruptes Schema, begrenzen den Schaden aber auf einen oder wenige Domänencontroller. *(jp)*

Links

[1] Skript ADSchemaExtensionConflictAnalyzer.ps1
http://gallery.technet.microsoft.com/ScriptCenter/en-us/0672d181-ab2c-4c92-8466-d93a67412207/

Quelle: James Steidl - Fotolia.com

Active Directory sichern

Gewappnet für den Fall der Fälle

Das Backup eines Active Directory ist relativ komplex. Jede neue Windows-Version bringt neue Möglichkeiten für die Wiederherstellung von Inhalten aus dem Verzeichnisdienst mit – aber ohne eine solide Sicherungsstrategie ist der Administrator im Fall der Fälle aufgeschmissen. In diesem Workshop erläutern wir Ihnen die Problematiken bei Sicherung und Rücksicherung des Active Directory sowie, welche Daten in einer Sicherung enthalten sein sollten.

Das Active Directory ist der Verzeichnisdienst, in dem seit Windows 2000 die Informationen über Benutzerkonten, Gruppen, Computerkonten, Konfigurationsdaten (Gruppenrichtlinien) sowie wichtige Infrastrukturelemente gespeichert werden. Ohne das Active Directory (AD) ist keine Anmeldung an der Domäne möglich, und damit hat der Anwender auch keinen Zugriff auf Ressourcen wie Dateien, Drucker oder Öffentliche Ordner in Exchange. Doch obwohl der Verzeichnisdienst eine so grundlegende Rolle in einer modernen Microsoft Windows-Infrastruktur spielt, sind sowohl die Fachkenntnisse zur Sicherung der Daten wie auch zur Rücksicherung nur selten detailliert bekannt und geübt.

Fehler nicht ohne Grund

Manchmal ist die Befürchtung zu hören, das Active Directory könnte quasi von alleine kaputt gehen. Dieser Fall dürfte jedoch selbst erfahrenen IT-Experten wohl noch nie untergekommen sein. Sollte es zu einer Wiederherstellung des Active Directory kommen müssen, sind die Ursachen häufig entweder fehlerhafte Konfigurationen (dann müssen meist nur einzelne Domänencontroller wieder hergestellt werden) oder Leichtsinnsfehler – also Administratoren oder Prozesse, die versehentlich Daten im Active Directory gelöscht oder geändert haben. Dabei ist niemandem einen Vorwurf zu machen, je nach Verwaltungskonsole kann auch eine zunächst unbeabsichtigte Löschung passieren.

Ist eine Wiederherstellung des Active Directory notwendig, so ist wahrscheinlich einer der folgenden Problemfälle eingetreten. Unterscheiden lassen sich dabei Problemfälle, die komplette Systeme und Domänen betreffen und Problemfälle, die Inhalte betreffen:

- Ein Domänencontroller (DC) ist defekt und muss ausgetauscht werden. Soll dieser über eine Sicherung wiederhergestellt werden, so sollte der Fehler ausschließlich in einer zusätzlichen Software liegen oder daran, dass nur ein DC existiert, was nicht empfehlenswert ist. In allen anderen Fällen sollten Sie den Domänencontroller neu aufbauen und die Inhalte von den anderen Domänencontrollern replizieren.
- Eine Domäne ist kaputt und lässt sich auf keinem anderen Weg retten. Dies ist ein hoffentlich seltener Fall, und würde bedeuten, dass ein Domänencontroller von einer Sicherung wieder hergestellt werden muss, mit dem anderen Domänen wieder kommunizieren und von diesem dann die Domäne mit weiteren DCs wieder aufgespannt wird.
- Eine Gesamtstruktur aus mehreren Domänen ist kaputt: Auch dieser Fall ist recht selten und bedeutet zumeist die komplette Wiederherstellung der Unternehmensinfrastruktur. Auch in diesem Fall müssen Sie die Domänen einzeln wieder herstellen.

Für den Aufbau oder die Wiederherstellung von Domänencontrollern, ganzen Domänen oder Gesamtumgebungen kann die Option "Install from Media" sehr hilfreich sein. Doch häufiger sind die Fälle, in denen nur Inhalte des Active Directory wieder hergestellt werden müssen:

- Ein einzelnes Objekt wird gelöscht.
- Mehrere Objekte, oder ein gesamter Baum an Objekten wird gelöscht, etwa beim Entfernen einer Organisatorischen Einheit (OU).
- Einzelne Werte von Attributen werden über mehrere Objekte hinweg fehlerhaft geändert oder gelöscht.

Diese Fälle sind deutlich häufiger, erfordern aber auch besonderes Wissen, da es Nebenwirkungen gibt, wenn nur ein-

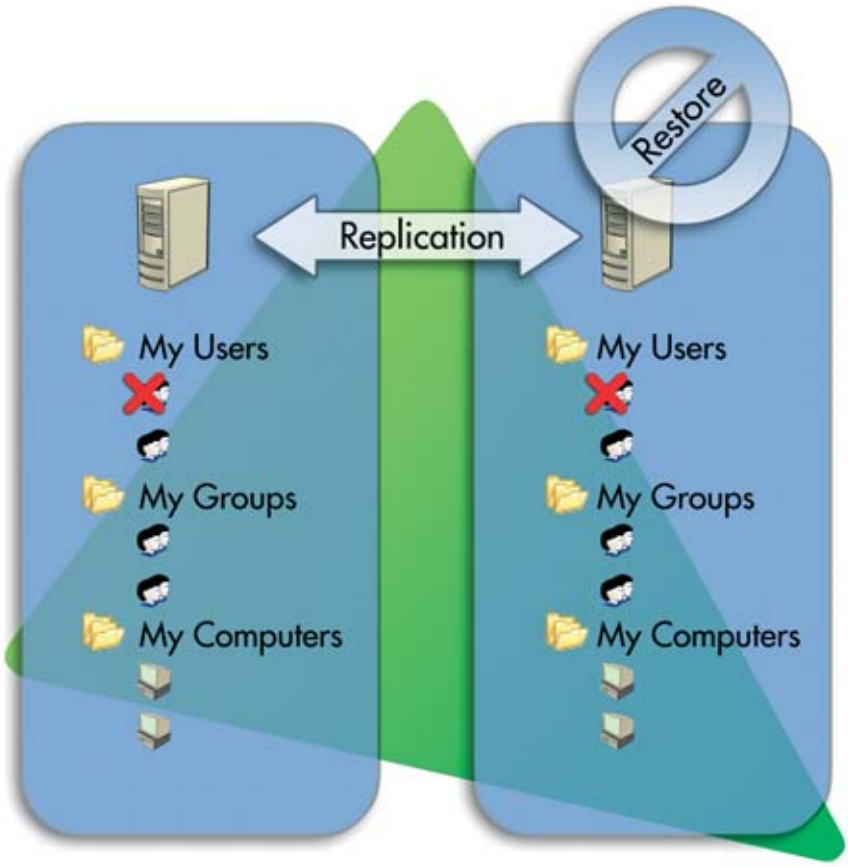


Bild 1: Nach einer Nicht-Autoritativen Wiederherstellung gleicht sich das Active Directory auf den Status der nicht-wiederhergestellten Domänencontroller ab: Ein gelöschtes Benutzerkonto wird auch auf dem wiederhergestellten Domänencontroller wieder gelöscht

zelne Inhalte wieder hergestellt werden. Die Problematiken in diesem Bereich liegen darin, dass das Active Directory per se redundant aufgebaut ist – jeder Domänencontroller einer Domäne hat die gleichen Informationen über alle Objekte dieser Domäne.

Replikation und Datenkonsistenz

Um einzelne Objekte wiederherzustellen, bedarf es klassischerweise der "Autoritativen Wiederherstellung". Das Active Directory ist ein sogenannter Multi-Master-Verzeichnisdienst, also jeder Domänencontroller darf prinzipiell auf die Inhalte schreibend zugreifen. Seit Windows Server 2008 gibt es die neue Rolle des Schreibgeschützten Domänencontrollers (Read-Only Domaincontroller, RODC), den wir in dieser Betrachtung ausklammern. Dadurch, dass jeder DC schreibend auf die Inhalte zugreifen kann und diese dann auf die anderen Domänencontroller übertragen werden müssen, ist es notwendig, die Replikation der Daten zu strukturieren. Beim Active Directory gilt – vereinfacht dargestellt – die folgende Vorgehensweise:

- Über Update Sequence Nummern (USN), die auf jedem Domänencontroller (DC) bei jeder Änderung hochgezählt werden, lässt sich feststellen, welche Änderungen seit der letzten Replikation vorgekommen sind.
- Ein Domänencontroller merkt sich, welche USNs er von welchem DC bereits erhalten hat.
- Über die Versionsnummer, die mit jedem Attribut DC-übergreifend hochgezählt wird, lässt sich feststellen, wer im Falle eines Konfliktes die neueren / häufiger aktualisierten Daten hat.
- Bei der Replikation fragt ein DC nach Attributen mit höherer USN als bei der letzten Replikation, dann überprüft er die Versionsnummern um festzustellen, welche Änderungen die aktuellen sind.
- Wenn die Versionsnummern identisch sind, wird der Zeitstempel hinzugezogen, um den neueren Wert zu bestimmen.

Sollen Objekte im Active Directory wiederhergestellt werden, müssen Sie daher beachten, dass Inhalte nicht nur auf einem, sondern auf allen Domänencontrollern der Domäne, teilweise sogar der Gesamtumgebung liegen. Wenn Sie also Teilbereiche wieder herstellen und nicht alle anderen Domänencontroller neu aufbauen möchten, berücksichtigen Sie die Replikation und stellen Sie sicher, dass die wiederhergestellten Objekte neuer erscheinen, als zum Beispiel der Tombstone des zuvor gelöschten Objektes. Andern-

In Wiederherstellungsszenarien, die ganze Domänencontroller, Domänen oder sogar die Gesamtstruktur betreffen, müssen häufig mehrere Domänencontroller wiederhergestellt werden. Die übliche Vorgehensweise ist es, alles, was nicht funktioniert zu entfernen (etwa alle Domänencontroller einer defekten Domäne) und einen der DCs von einer Sicherung wiederherzustellen. Dann muss gewährleistet werden, dass dieser DC wieder kommunizieren kann, bevor der Rest der Infrastruktur (also alle anderen DCs) neu aufgebaut wird. Das bedeutet, dass mindestens das Active Directory entfernt wurde, gegebenenfalls Reste im AD der alten Maschine entfernt werden, und dann der Server neu in die Domäne aufgenommen und zum Domänencontroller ernannt wird. Hierdurch erhält dieser eine neue, funktionierende Kopie des Active Directory.

Dies ist einfach, wenn es sich nur um einen unter mehreren Domänencontrollern am gleichen Standort handelt, oder der Standort eine gute Anbindung zu einem anderen Standort hat. Sind am gleichen Standort keine weiteren Domänencontroller vorhanden, jedoch eine Datensicherung, dann kann ab Windows Server 2003 mit dem Kommando *dcpromo.exe /adv* auch diese Datensicherung für die initiale Befüllung des Active Directories verwendet werden – nur die Neuerungen seit der Datensicherung werden dann über das Netzwerk repliziert. Ab Windows Server 2008 ist es nicht mehr notwendig, *dcpromo.exe* mit dem separaten Parameter "/adv" aufzurufen, der Installationsassistent hat einen Expertenmodus, der die Wahl einer Datensicherung zulässt.

Install from Media

seits würde das Objekt zwar auf einem DC wieder hergestellt, aber nach der nächsten Replikation von anderen DCs wieder gelöscht werden.

Autoritative Wiederherstellung

Um einzelne Objekte innerhalb einer Domäne wiederherstellen zu können, gibt es die Autoritative Wiederherstellung. Eine "Nicht-Autoritative Wiederherstellung" bedeutet lediglich, dass die Active Directory-Datenbank sowie alle abhängigen Komponenten (Dateisystem für Sysvol oder auch Registry) von einer Sicherung in einem konsistenten Zustand wiederhergestellt werden. Sie markiert aber keine Objekte als neuer – sobald die Replikation wieder startet, werden geänderte Einträge von anderen Domänencontrollern zurückgespielt.

Bei der "Autoritativen Wiederherstellung" hingegen markieren Sie als Administrator bestimmte Objekte oder Teilbäume als "neuer". Wenn nun die Replikation wieder aufgenommen wird, zählt die Kopie des Objektes auf dem wiederhergestellten Domänencontroller und gelöschte oder veränderte Objekte werden mit der alten Kopie wieder überschrieben.

Eine Autoritative Wiederherstellung folgt normalerweise einer Nicht-Autoritativen Wiederherstellung, wenn die fehlerhafte Änderung oder Löschung bereits auf alle DCs repliziert wurde. Sie kann aber auch durchgeführt werden, wenn ein DC in einem entfernten Standort noch nicht von der fehlerhaften Änderung betroffen ist. In diesem Fall wird das Objekt dann – ohne eine vorherige Rücksicherung – als aktueller markiert, bevor zum Beispiel die Löschung per Replikation eintrifft. So erscheint es, dass das nicht-gelöschte Objekt aktueller ist als die Löschung und diese damit wieder aufgehoben wird.

Wird ein Domänencontroller wieder hergestellt, erhält er eine neue Invocation ID. Dadurch erkennen die bisherigen Replikationspartner ihn als neuen DC und gleichen alle Inhalte erneut ab. Bei der Autoritativen Wiederherstellung werden dann die Versionsnummern aller Eigenschaften der betroffenen Objekte um 100.000 erhöht, damit diese bei der Replikation zum Einsatz kommen. Allerdings können Objekte durch Verknüpfungen gegenseitig referenziert sein, was später bei der Wiederherstellung gesondert berücksichtigt werden muss.

Vorsicht, Verknüpfungen

Im Active Directory gibt es Verknüpfungen wie etwa die Mitgliedschaft von Benutzerkonten in Gruppen, die Mitgliedschaft von Gruppen in Gruppen oder auch Manager- und Mitarbeiter-Verknüpfungen. Letztere werden zum Beispiel von Exchange und SharePoint verwendet und ermöglichen die Navigation durch die Unternehmenshierarchie. Bei diesen Verknüpfungen gibt es einen Vorwärtslink, der gepflegt wird (und beschreibbar ist), und einen Rückwärtslink, den das Active Directory automatisch berechnet. Ein Beispiel hierfür sind die Attribute "member" von Gruppen und "memberOf" bei Benutzern und Gruppen. "member" ist hierbei die Vorwärtsverknüpfung, das heißt, bei einem Gruppenobjekt ist im "member"-Attribut gespeichert, welche Benutzer oder Gruppen Mitglieder dieser Gruppe sind. Parallel dazu gibt es beim Benutzer und bei Gruppen das Attribut "memberOf". Hier sind nicht tatsächlich die Werte gespeichert – der Verzeichnisdienst weiß, dass es sich um eine Rückwärtige Berechnung des "member"-Attributes handelt und berechnet das Ergebnis dann auf Anforderung.

Problematisch bei der Wiederherstellung von Verzeichnisdienstinhalten ist hierbei, dass das memberOf-Attribut (sowie andere Rückwärtsverknüpfungen) nicht geschrieben werden können, also auch nicht repliziert werden oder die Versionsnummer hochgezählt wird. Daher

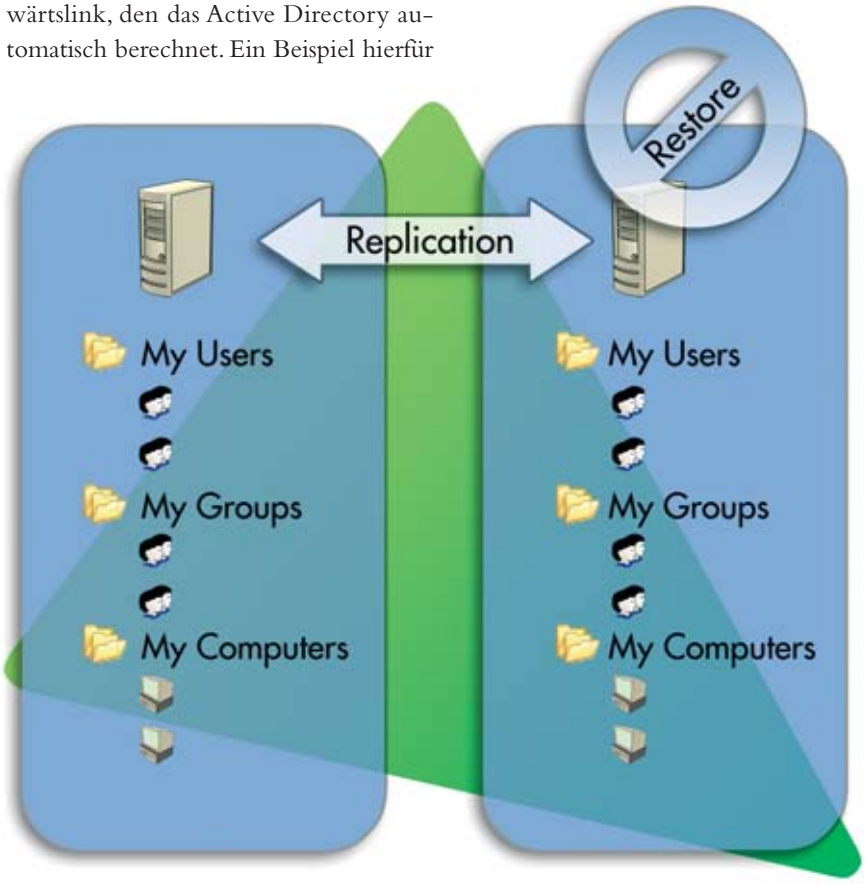


Bild 2: Nach einer Autoritativen Wiederherstellung werden vormals gelöschte Objekte als "neuer" markiert und auf anderen Domänencontrollern wiederhergestellt

müssen Sie solche Verknüpfungen nach einer Wiederherstellung gegebenenfalls zusätzlich korrigieren. Unter Windows 2000 Server und Windows Server 2003 ohne Servicepack war es daher notwendig, Objekte, die Rückwärtsverknüpfungen enthalten, sowie die Objekte, die die dazu gehörigen Vorwärtsverknüpfungen enthalten, wiederherzustellen.

Ein weiterer Effekt ist die Reihenfolge bei der Wiederherstellung, beispielsweise wenn Sie sowohl Benutzer als auch Gruppen wiederhergestellt haben. Dann konnte es sein, dass die Gruppe wiederhergestellt wurde, der Benutzer aber just in dem Moment noch nicht wiederhergestellt war und der Verzeichnisdienst daher die Vorwärtsverknüpfung nicht einrichten konnte. Auf dem wieder- hergestellten Domänencontroller waren diese Mitgliedschaften dann zwar korrekt, nicht aber auf den anderen DCs, die diese Informationen über die Replikation erhalten haben. Daher wurde häufig eine doppelte Wiederherstellung empfohlen, also Autoritativer Restore, Neustart und Replikation, dann nochmals im Verzeichnisdienstwiederherstellungs-Modus die gleichen Objekte wiederherstellen. Das hat den Vorteil, dass im ersten Schritt sichergestellt wird, dass die Objekte alle wieder vorhanden sind, und im zweiten Schritt auch die Verknüpfungen wieder korrekt sind. Zu berücksichtigen bleibt jedoch, dass auch Objekte zurückgesichert werden müssen, die eigentlich gar nicht gelöscht wurden, aber über Vorwärtsverknüpfungen zurückgesicherte Objekte enthalten. Das gilt auch Domänenübergreifend, wenn sich mehrere Domänen in der Gesamtumgebung befinden.

Seit Windows Server 2003 SP1 kommen LDF-Dateien zum Einsatz, um genau dieses Szenario zu adressieren. Diese Dateien, deren Namen Sie während des Autoritativen Restores durch *NTDSUtil.exe* genannt bekommen, helfen Ihnen dabei, die Verknüpfungen nach der Replikation mit anderen Domänencontrollern wiederherzustellen. Es wird hierbei eine Datei pro Domäne erstellt, die bei verteilter Administration dann dem jeweiligen Administrator geschickt werden kann. Dieser importiert die LDF-Datei einfach mit dem Befehl *ldifde.exe* in das AD und stellt damit sicher, dass die wiederhergestellten Benutzer erneut Mitglieder derjenigen Gruppen werden, denen sie vor dem Löschen des Benutzerobjektes angehört haben. Auch wichtig ist, dass Sie beim Autoritativen Restore wissen, wie der vollständige Name und Pfad zu dem Objekt sein soll, das Sie wiederherstellen möchten. Diese Daten sollten Sie bei der Wiederherstellung kennen.

Was gesichert werden muss

Im Allgemeinen wird davon ausgegangen, dass eine Sicherung des Systemstatus ausreicht, um eine Wiederherstellung des Active Directory durchzuführen. Dies ist zwar prinzipiell richtig, aber je nachdem, was Sie wiederherstellen müssen, stellen Sie schnell fest, dass Sie lieber noch weitere Daten hätten.

Bei der Autoritativen Wiederherstellung von einzelnen Objekten oder Teilbereichen des Active Directory müssen Sie sich an den genauen "Standort" des Objektes im Active Directory sowie die Schreibweise erinnern. Doch das Objekt wurde gelöscht, weshalb Sie nicht einfach nachsehen können, wo es sich befand und wie es hieß. Haben Sie keine zusätzlichen Informationen vorliegen und können Sie sich nicht an die genaue Schreibweise des gesamten Pfades erinnern, führen Sie eine Rücksicherung des Systemstatus (Nicht-Autoritativer Restore) durch, nehmen den Domänencontroller vom Netzwerk und starten ihn im normalen Modus.

Dadurch ist sichergestellt, dass dieser nicht replizieren kann und die Objekte gleich wieder löscht. Im Anschluss können Sie die Schreibweise und den Pfad (den distinguishedName) des wiederherzustellenden Objektes herausfinden, zum Beispiel über die Managementkonsole *ADSIEdit.msc*. Bis zu Windows Server 2008 müssen Sie anschließend noch einmal in den Verzeichnisdienstwiederherstellungsmodus (Directory Service Restore Mode, DSRM) booten – bei neueren Versionen reicht es, den Verzeichnisdienst zu stoppen – und können dann mit NTDSUtil den Autoritativen Restore durchführen. Nun nehmen Sie den Domänencontroller wieder an das Netzwerk, starten diesen im normalen Modus beziehungsweise starten den Dienst und führen die nachfolgenden Schritte wie die Bereinigung von Verknüpfungen durch. Alles in allem eine sehr umständlich Vorgehensweise. Alternativ könnten Sie in Windows Server 2008 und höher auch die Datenbankdatei *ntds.dit* zurücksichern und in diese wie in einen Snapshot hineinsehen. Auch dies funktioniert jedoch nur bei einem vollständig gestarteten Domänencontroller (nicht im DSRM).

Ein gangbarer Weg ist daher das Sichern des Systemstatus in eine Textdatei, die eine Liste aller Objekte zu dem Zeitpunkt enthält. Diese Liste können Sie mit dem folgenden Kommando erstellen:

```
dsquery * domainroot -limit 0 >
  d:\backup\ad-objects.txt
```

Mit dem Parameter "-attr" können Sie noch weitere Informationen wie den Zeitpunkt der letzten Änderung wählen, für die Wiederherstellung wichtig ist allerdings nur die Liste der Objekte. Nehmen Sie dieses Kommando am besten mit in Ihr Backupscript, noch vor dem Erstellen des Systemstatus, und stellen Sie sicher, dass die Liste auch mit in der Sicherung aufgenommen ist. Dadurch haben Sie bei einer Wiederherstellung immer die Liste aller Objekte auf dem lokalen Domänencontroller im Textformat vorliegen, die zum Zeitpunkt der Sicherung gültig waren. Diese Liste können Sie natürlich auch im Verzeichnisdienstwiederherstellungsmodus lesen, und den Pfad über Kopieren in das NTDSUtil übernehmen.

Knackpunkt Gruppenrichtlinien

Ein weiterer, heikler Punkt sind Gruppenrichtlinienobjekte. Diese wieder her-

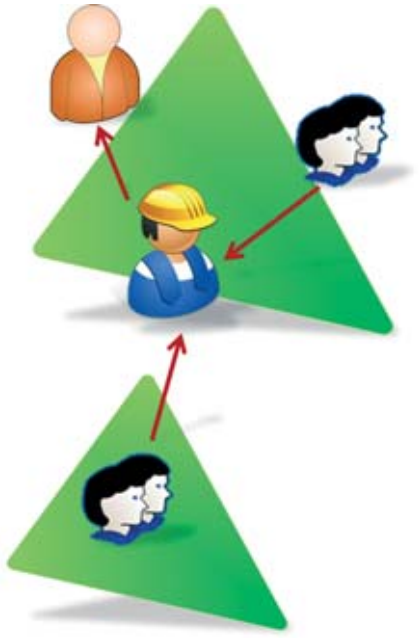


Bild 3: Bei Verknüpfungen ist es wichtig darauf zu achten, wo der "Vorwärts-Link" sitzt. Nur dieser kann geschrieben werden.

zustellen ist nicht ganz einfach, da verschiedenste Speicherorte betroffen sind:

- Im Active Directory werden an OUs, Standorten und an der Domäne die Verknüpfungen zu den Gruppenrichtlinienobjekten gespeichert (sowie deren Anwendungsreihenfolge).
- Die Gruppenrichtlinienobjekte sind im Active Directory unter "cn=Policies, cn=System,dc={domäne}" zu finden. GPOs können aber auch domänenübergreifend verlinkt werden, so dass mehrere Domänen betroffen sein können.
- Die Einstellungen der GPOs befinden sich auf der Netzwerkfreigabe SysVol, so dass diese auch autoritativ wiederhergestellt werden müsste.

Besonders, wenn nur einzelne GPOs wiederhergestellt werden sollen, gestaltet sich dies sehr schwierig. Abhilfe schafft die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC). Mit ihrer Hilfe sichern Sie Gruppenrichtlinienobjekte und stellen diese wieder her. Um die Sicherung der GPOs mit der GPMC zu automatisieren, können Sie sich vor dem nächste Migrationsschritt eines VB-Skripts bedienen. Diese sind bei der GPMC für Windows Server 2003 als separater Download Bestandteil der Installation der GPMC unter *c:\Programme\GPMC\Scripts*. Bei Windows Server 2008 wird die GPMC als Funktion über den Servermanager installiert, hier fehlen jedoch die Skripte. Diese können Sie separat runterladen (siehe Link-Kasten). Mit dem folgenden Skript sichern Sie alle GPOs in ein Dateiverzeichnis:

```
cscript.exe "C:\Program
  Files\GPMC\Scripts\backupallgpos.
  wsf" D:\GPO-Backup /comment:"ALL
  GPOs"
```

Zur Rücksicherung verwenden Sie dann einfach die GPMC.

Zusätzlich müssen Sie eine Liste mit den Gruppenrichtlinienverknüpfungen speichern, durch die Rücksicherung wird nämlich nur das Gruppenrichtlinienobjekt mit den entsprechenden Einstellungen, nicht jedoch die Verknüpfung auf OUs wiederhergestellt. Auch hierfür findet sich ein Skript der GPMC. Der folgende Aufruf erstellt eine XML-Datei mit allen Verknüpfungen:

```
cscript.exe "C:\Program
  Files\GPMC\Scripts\ListSOMPolicy-
  Tree.wsf" > d:\GPO-Backup\
  GP-Links.xml
```

Alternativ können Sie diese auch mit dem Kommando *ldifde* exportieren. Der Vorteil: Die Ausgabedatei lässt sich dann im Fehlerfall editieren und die entsprechenden Links und ihre Einstellungen einfach importieren. Für die Gruppenrichtlinienobjekte innerhalb der Domäne verwenden Sie folgendes Kommando:

```
ldifde -f
  d:\backup\DomainGpoLinks.ldf -r
  "(gplink=*)" -l gplink,gpoptions
```

Für die Gruppenrichtlinien, die auf Standorten verknüpft wurden, nutzen Sie

```
ldifde -f d:\backup\SiteGpoLinks.ldf
  -d cn=configuration,dc=firma,dc=de
  -r "(gplink=*)" -l gplink,
  gpoptions
```

Fehlt nur noch der Systemstatus. Diesen können Sie unter Windows 2000 und Windows Server 2003 einfach mit dem eingebauten NTBackup erstellen (Start /

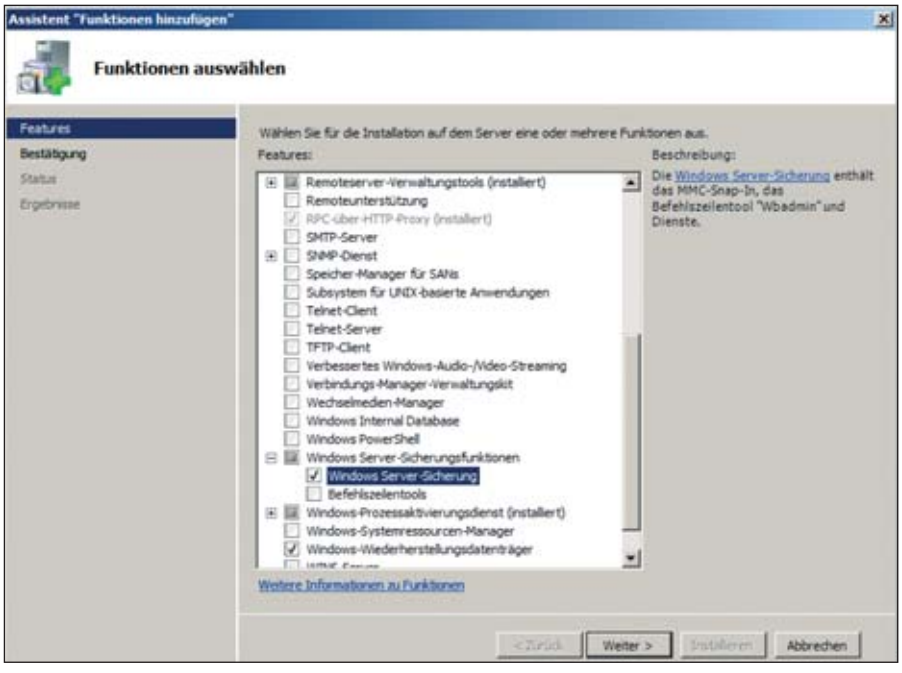


Bild 4: Die Windows Server-Sicherung muss seit Windows Server 2008 als Funktion über den Servermanager installiert werden

Im Zusammenhang mit der Active Directory-Sicherung und -Wiederherstellung taucht immer wieder der Begriff Tombstone-Lifetime auf. Nachdem das Active Directory ein Multi-Master-Verzeichnisdienst ist, kann ein Objekt wie ein Benutzerkonto nicht einfach gelöscht werden. Die anderen Domänencontroller, die der gleichen Domäne angehören, müssen darüber informiert werden, dass dieses Objekt gelöscht werden soll. Daher wird es zunächst in einen Tombstone (Grabstein) umgewandelt, die Namen geändert, sehr viele zusätzliche Informationen (zum Beispiel die Beschreibung, Gruppenmitgliedschaften, Adressen und Telefonnummern) gelöscht und das Objekt in einen "Deleted Objects"-Container verschoben. Es wird jedoch weiterhin zwischen den Domänencontrollern repliziert, so dass alle Domänencontroller erfahren, dass dieses Objekt zu löschen ist.

Ist die Lebenszeit des Tombstone (Tombstone-Lifetime) abgelaufen, kümmert sich jeder Domänencontroller selbst darum, die Überreste des Objektes zu löschen. Die Lifetime wird für die Gesamtumgebung festgelegt. Abhängig davon, welche Betriebssystemversion der erste Domänencontroller zum Zeitpunkt des dcpromo hatte, beträgt sie:

- 60 Tage bei Windows 2000
- 60 Tage bei Windows Server 2003 ohne Servicepack
- 180 Tage bei Windows Server 2003 SP1
- 60 Tage bei Windows Server 2003 R2
- 180 Tage bei Windows Server 2003 SP2, R2 SP2
- 180 Tage bei Windows Server 2008 und R2

Eine Besonderheit gilt dabei für Windows Server 2003 R2. Dieses Release besteht aus zwei CDs: Die erste enthält Windows Server 2003 mit SP1, die zweite die Komponenten zu R2. Wird zunächst die erste CD installiert, dann der Server zum Domänencontroller ernannt und erst jetzt das R2 installiert, beträgt die Tombstone-Lifetime 180 Tage. Lautet die Installationsreihenfolge erste CD, dann zweite CD und erst dann Ernennung des Servers zum Domänencontroller, beträgt die Tombstone-Lifetime 60 Tage. Hier kommt eine alte Version in den Active Directory-Installationsdateien auf der zweiten CD zum Einsatz, dies ist jedoch bekannt und nicht weiter dramatisch.

Da die Tombstone-Lifetime bestimmt, ab wann Objekte endgültig gelöscht werden, können Sie keine Datensicherungen verwenden, die älter sind als diese. Dies würde nämlich dazu führen, dass Objekte, die zurecht gelöscht wurden, aber deren "Löschinformationen" nicht mehr im produktiven Active Directory vorliegen, plötzlich wieder vorhanden wären. Dies könnte katastrophale Auswirkungen haben und daher können diese Sicherungen nicht mehr verwendet werden. Eine Ausnahme hierzu wäre mittels Active Directory Snapshots unter Windows Server 2008 möglich, aber dazu später.

Die Tombstone-Lifetime kontrollieren Sie per *ADSIEdit.msc* (bis Windows Server 2003 R2 Bestandteil der Support-Tools, ab Windows Server 2008 im Betriebssystem). Navigieren Sie zum folgenden Objekt "cn=Directory Service, cn=Windows NT,cn=Services,cn=Configuration" unterhalb der Rootdomäne. In den Eigentschaften des Objektes finden Sie das Attribut "tombstoneLifetime". Ist der Wert gesetzt, entspricht er der Tombstone-Lifetime in Tagen. Wenn er nicht gesetzt wird, sind es 60 Tage.

Tombstone-Lifetime vs. Rücksicherung

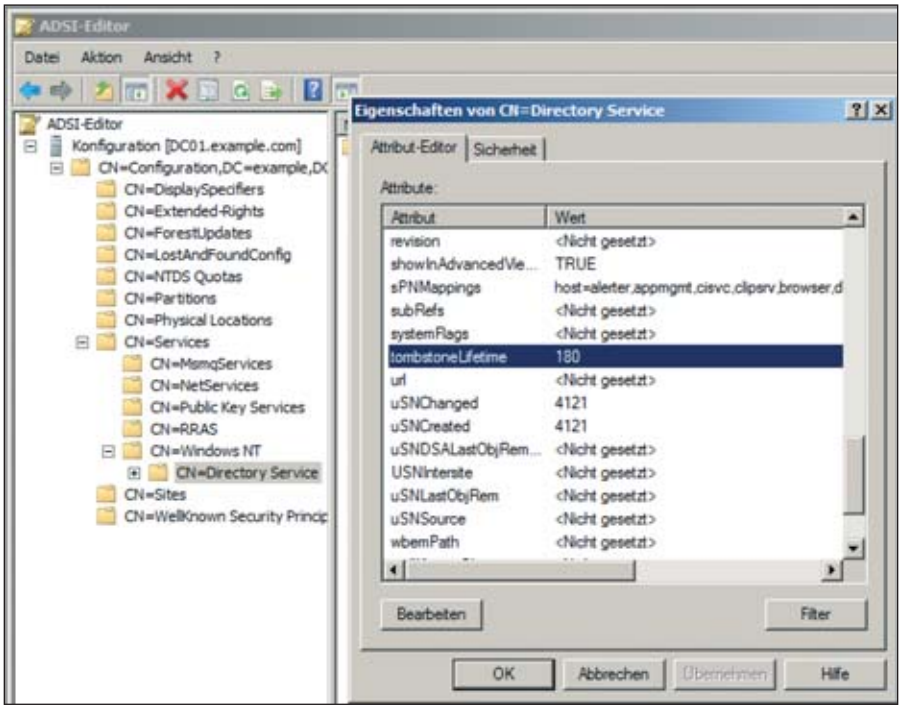


Bild 5: Die Tombstone-Lifetime und damit die Gültigkeit der Datensicherungen können Sie mittels *ADSIEdit.msc* feststellen

Programme / Zubehör / Systemprogramme / Sicherung). Am besten fertigen Sie zunächst einen Job an, der regelmäßig die Sicherung des Systemstatus durchführen soll. Hier sollten Sie außer dem konpletten Systemstatus noch die Dateien mit der Liste aller Objekte sowie der Gruppenrichtlinien mit in die Sicherung aufnehmen.

Am einfachsten wählen Sie im Expertenmodus den Systemstatus und die zusätzlichen Dateien aus, gehen dann auf "Aufträge planen / Neuen Auftrag hinzufügen". Dort geben Sie an, dass Sie die Vorauswahl an den Sicherungsorten übernehmen möchten und planen den weiteren Auftrag. Dieser kann, nachdem er fertig gestellt wurde, dann als Vorlage für das eigene Sicherungs-Skript dienen, indem er noch die zusätzlichen Sicherungsdateien erstellen lässt und dann von diesem aus die Datensicherung startet.

Unter Windows Server 2008 stellt sich das ganze etwas anders dar: Das Sicherungsprogramm "Windows Server-Sicherung" ist nicht standardmäßig installiert, Sie müssen es als "Funktion" über den Servermanager hinzufügen:

```
servermanagercmd -install Backup
```

Das neue Sicherungsprogramm erstellt Sicherungen von Datenträgern, daher kann es als Sicherungsziel nur eine Partition/Volume verwenden, die nicht in der Sicherung mit enthalten ist. Die Server sollten hierfür richtig partitioniert sein, so dass keine Daten auf dem gleichen Laufwerk liegen, auf dem Sie auch die Sicherung erstellen wollen. Die automatische Sicherung auf UNC-Pfade (\\server\share) ist noch nicht bei Windows Server 2008, jedoch bei R2 möglich. Sie können jedoch die Sicherung per Skript auf einen anderen Server kopieren. Den Systemstatus erstellen Sie mittels des Kommandozeilentools *wbadmin.exe* . Das "S:" am Ende des Kommandos gibt das Zielaufwerk für die Sicherung an:

```
wbadmin start systemstatebackup
  -backupTarget:S:
```

Zusätzlich sollten Sie überlegen, ob Sie anstatt der Systemstatussicherung lieber eine "Critical Volume"-Sicherung durchführen möchte. Diese enthält den Systemstatus, und zusätzlich weitere Daten, die für eine

Rücksicherung, auch direkt von der Installations-CD aus, genutzt werden können. Die Diskussion hierzu befindet sich im Artikel zum Windows Server Backup. Schließlich bleibt noch zu erwähnen, dass eine Sicherung nur solange genutzt werden kann, wie die "Lebenszeit" von gelöschten Objekten im Unternehmen eingerichtet ist (Tombstone Lifetime). Bei den meisten Unternehmen sind dies 60 Tage.

Mehrere Sicherungen verwalten

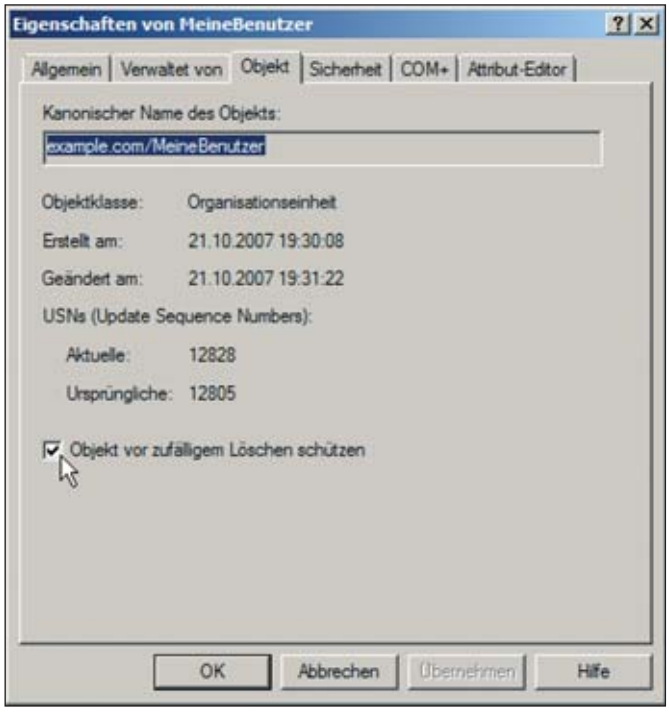
Das Windows Server Backup schreibt ein eigenes Verzeichnis für jede Sicherung auf einen UNC-Pfad. Möchten Sie Ihre Sicherungen auf einen Dateiserver schreiben, dabei jedoch zum Beispiel sicherstellen, dass nur die letzten zehn Sicherungen für jeden Server aufgehoben werden, können Sie den folgenden Code in Ihr Backup-Skript (CMD- oder BAT-Datei) integrieren:

```
Set Target="\\server\share"
Set Backup2Keep=10
Rem (..)
Rem Code für Backup hierein
Rem (..)
SETLOCAL ENABLEDELAYEDEXPANSION
set count=0
for /f "tokens=*" %%i in ('dir /o:
  -d /b %Target%\WindowsImage-
  Backup\%computername%\backup*.')
  do (
  set /a count=!count! + 1
  if !count! GTR %Backup2Keep% (
    echo DELETE   !Count!: %%i
    rd /s /q "%Target%\WindowsImage-
    Backup\%computername%\%%i"
  ) else (
    echo MAINTAIN !Count!: %%i
  )
)
```

Hierbei enthält die Variable "Target" das Backup-Ziel als UNC-Pfad. Die Variable "Backup2Keep" enthält die Zahl der Sicherungen, die pro Domänencontroller erhalten bleiben sollen. Durch den *for*-Befehl werden alle Backups in dem Zielverzeichnis für den lokalen Server dem Datum geordnet dargestellt. Das Skript durchläuft danach die ermittelten Verzeichnisse, schont die ersten, die unterhalb der Backups2Keep-Nummer liegen, und löscht den Rest. Erstellen Sie ein Skript, das einem Domänencontroller zum Beispiel über Gruppenrichtlinien zugeordnet werden kann, sollten Sie sicherstellen, dass das Windows Server Backup installiert ist. Zu diesem Zweck können Sie die PowerShell mit dem folgenden Befehl im Skript nutzen:

```
powershell.exe
-command
"&{import-module
ServerManager;
add-windowsfeature
Backup}"
```

Das Skript überprüft nun, ob Windows Server Backup vorhanden ist, installiert es gegebenenfalls und fährt erst dann mit den nachfolgenden Zeilen fort.



Bld 6: Über das Häkchen "Objekt vor zufälligem Löschen schützen" werden die Verbote für das Löschen des Objektes und der Unterobjekte in der Sicherheitsregisterkarte gesetzt

Welche DCs gesichert werden müssen

Häufig wird diskutiert, welche Domänencontroller gesichert werden müssen. Dies hängt ganz stark von der Active Directory-Infrastruktur des Unternehmens ab und vor allem davon, wie die Rücksicherung geplant ist. Da Sie normalerweise bei Ausfällen von Domänencontrollern diese eher durch Neuinstallation als durch Rücksicherung ersetzen werden, werden Sicherungen eigentlich nur selten benötigt. Stellen Sie dabei sicher, dass mindestens zwei Domänencontroller pro Domäne gesichert werden. Diese sollten, bei AD-Integriertem DNS, auch DNS-Server sein, jedoch keine FSMO-Rollen innehaben. Vermeiden Sie, Letztere zurückzusichern. Stellen Sie stattdessen sicher, dass die ehemaligen Besitzer nicht mehr online gehen können und übertragen Sie einem DC die entsprechende Rolle.

Auch Standorte spielen noch eine Rolle bei der Entscheidung, welche DCs gesichert werden müssen. Sind Filialen nur über eine langsame Leitung angebunden und erhalten ihre Serverhardware nicht aus der Zentrale, sondern von einem Anbieter direkt, kann es auch sinnvoll sein, dort Daten für die Rücksicherung vorzuhalten. Ob dies ein Domänencontroller-Backup ist oder nur eine automatische Installationsmethode und die AD-Inhalte dann auch repliziert werden können, hängt von dem jeweiligen Unternehmen und deren Anforderungen ab. Wichtig ist auch, dass Sie regelmäßig überprüfen, ob die Sicherungen auch funktionieren und noch alle Daten beinhalten, die Sie bei der Rücksicherung erwarten.

Präventivmaßnahmen

Zwar ist eine Datensicherung wichtig, um im schlimmsten Fall reagieren zu können. Wichtiger jedoch ist es, einen solchen Fall von vornherein zu vermeiden. Den wichtigsten Ansatzpunkt bil-

det ein gutes Administrationsmodell. Jeden Administrator gleich zum Domänenadministrator zu ernennen – vielleicht auch noch mit nur einem Benutzerkonto zum Internetsurfen, Mailen wie auch zur Administration selbst – ist fast schon ein Garant dafür, dass sich schwerwiegende Fehler einschleichen. Dabei müssen diese Fehler garnicht unbedingt aus Unwissenheit passieren. Es kann tatsächlich auch einmal vorkommen, dass der Admin mit der Maus auf einer OU hängenbleibt und diese verschiebt (wem ist das noch nicht im Explorer mit Dateien passiert), oder dass er bei der täglichen Administration ein Objekt zu viel markiert hat oder durch eine Tastenkombination eine falsche Aktion auslöst. Je mehr die Rechte eines Admins auf seine Aufgaben angepasst sind, desto weniger kann passieren.

Neben einem definierten und implementierten administrativen Rollenmodel können Sie noch weitere Maßnahmen treffen. Windows Server 2008 bietet auch hierbei Neues: Standardmäßig wird jede Organisatorische Einheit (Organizational Unit, OU) die mit "Active Directory-Benutzer und -Computer" von Windows Server 2008 angelegt wird, mit einem Löschschutz versehen. Das Häkchen hierfür finden Sie sowohl beim Erstellen einer neuen OU als auch auf der Registerkarte "Objekt" in den Eigenschaften der OU (hierfür muss die "Erweiterte Funktionen" im Menü Ansicht eingeschaltet sein).

Dieser Löschschutz ist aber kein neuer Wert im Active Directory, sondern konfiguriert nur die Zugriffskontrollliste im Reiter "Sicherheit" des Objekts mit zusätzlichen Berechtigungen. Dies sind "Verweigern"-Berechtigungen für die Gruppe "Jeden" zum "Löschen" und "Löschen von Unterobjekten". Wenn ein Administrator eine OU absichtlich Löschen möchte, muss er jetzt in die Eigenschaften des Objektes gehen und entweder das Häkchen oder die Berechtigungen entfernen. Da dies ein Feature der "Active Directory-Benutzer und -Computer"-Managementkonsole ist, wirkt es sich aber nur auf neue OUs aus. Und außerdem interessant: Die Berechtigungen gibt es ja bereits in heutigen Active Directorys. Sie können das "Feature" auch ohne Windows Server 2008 nutzen, indem Sie in die Eigenschaften des Objektes gehen und dort die oben genannten Berechtigungen setzen, oder Sie können dies auch über eine Kommandozeile mit dem folgenden Befehl tun:

```
dsacls ou=Benutzer,dc=example,dc=com
  /d Everyone:SDDT
```

Dies funktioniert mit jeder Version des Active Directory, und schon ist die OU-Struktur vor versehentlichem Löschen oder Verschieben geschützt.

Wurde die Infrastruktur migriert, sind OUs, die mit älteren Versionen der Managementkonsole erstellt wurden, nicht automatisch geschützt. Aber es ist empfehlenswert – egal welche Version des Betriebssystems eingesetzt wird – einen Löschschutz zu implementieren. Hierfür erstellen Sie entweder ein Skript mit dem obigen Befehl oder verwenden mit Active Directory Commandlets aus der PowerShell von Windows Server 2008 R2 die neue Scripting-Sprache. Um eine einzelne OU vor versehentlichem Löschen zu schützen, führen Sie einfach das folgende Kommando aus:

Windows Server 2008 TechCenter
http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx

Group Policy Management Console with SP1
http://www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887

GPMC Sample Scripts
http://www.microsoft.com/downloads/details.aspx?familyid=38c1a89b-a6d2-4f2a-a944-9236999aee65

Links

```
import-module ActiveDirectory
set-adorganizationalunit ou=Benut-
  zer,dc=example,dc=com -protectfro-
  maccidentaldeletion:$true
```

Um alle OUs zu schützen, nutzen Sie folgenden Befehl:

```
import-module ActiveDirectory
get-adorganizationalunit -filter * |
  set-adorganizationalunit -protect-
  fromaccidentaldeletion:$true
```

Der Schutz vor versehentlichem Löschen lässt sich bei allen Versionen des Active Directories einschalten. Wenn die 2008er-Konsolen noch nicht zur Verfügung stehen, müssen die relevanten Admins benachrichtigt werden, denn das absichtliches Löschen funktioniert nur dann, wenn die "Verweigern"-Berechtigung für "Jeden" zuerst entfernt wird.

Auch weitere Maßnahmen können in diesem Zusammenhang helfen, so sollten Sie sowohl ein Change-Management, eine Überwachung des AD sowie Monitoring in Erwägung ziehen – all das kann helfen, einen Fehler im Vorfeld zu vermeiden, im Fehlerfall die Ursachen zu finden oder nach einer Wiederherstellung die letzten validen Änderungen nachzuführen.

Fazit

In diesem Beitrag haben wir die Problematiken bei der Sicherung des Active Directory versionsübergreifend betrachtet und vermittelt, welche Daten in einer Sicherung enthalten sein sollten, damit Sie alle für eine Rücksicherung relevanten Daten besitzen. Außerdem haben wir betrachtet, wie Sie Ihre Umgebung zusätzlich sichern können, damit der Fehlerfall nicht so leicht eintritt. Im weiteren Verlauf dieses Sonderheftes erfahren Sie, wie Rücksicherungen gemacht werden und wie neue Funktionen bei Windows Server 2008 und R2 helfen können, die Möglichkeiten bei der Datensicherung und Rücksicherung zu erweitern. *(dr)*

Wiederherstellung des Active Directory

Zurück in die Zukunft

Das Recovery eines Active Directory ist sehr komplex. Neue Funktionen des Windows Server 2008 sowie R2 vereinfachen dem Administrator die Wiederherstellung von Inhalten aus dem Verzeichnisdienst. In diesem Artikel zeigen wir unterschiedlichen Möglichkeiten zur Wiederherstellung auf und nutzen den neuen Active Directory-Papierkorb, um den Vorgang zu vereinfachen und zu beschleunigen.

Datensicherung und Rücksicherung sind besonders beim zentralen Verzeichnisdienst Active Directory (AD) immer wieder ein spannendes Thema. Zum einen dient der Verzeichnisdienst in einer Windows-Server-Infrastruktur der Authentisierung (Wer ist berechtigt, sich anzumelden?) und Autorisierung (worauf hat wer welche Rechte?), und ist damit der Speicherort für alle Benutzer, Computer und Gruppen. Zum anderen dient der Verzeichnisdienst als sogenanntes Infrastrukturverzeichnis auch weiteren angeschlossenen Komponenten, wie der Verwaltung über Gruppenrichtlinien, der Darstellung der Standorttopologie für Replikation, den Datei- und Druckdiensten sowie Exchange (in einigen Versionen). Klar ist: das Active Directory ist unternehmenskritisch, es muss funktionieren und Ausfälle müssen minimiert werden.

Tatsächlich läuft das AD in den meisten Unternehmen sehr stabil, aber Ausfälle können schnell sehr kostspielig werden. Um sich zu versichern, sollte jedes Unternehmen in eine Sicherungsstrategie des AD sowie in das Know-how zur Wiederherstellung investieren.

Dass dieses Thema auch wirklich brisant ist, zeigt sich in Untersuchungen von Microsoft, die feststellten, dass das Löschen von Objekten die häufigste Ursache für Wiederherstellungen ist. Daher hat das Unternehmen mit dem Active Directory-Papierkorb in Windows Server 2008 R2 (Active Directory Recyclebin) speziell dieses Thema adressiert.

Im Artikel "Active Directory sichern" ab Seite 72 haben wir dargestellt, warum eine Wiederherstellung von Inhalten des Active Directory so komplex ist, welche "Fehlerszenarien" es gibt und welche Inhalte gesichert werden müssen. In diesem Beitrag erklären wir Ihnen, welche Möglichkeiten die unterschiedlichen Versionen des Active Directory bieten, um Inhalte wiederherzustellen. Zudem lesen Sie, was die neuen Snapshots der Windows Server 2008 Active Directory-Domänendienste bieten und wie Sie diese mit einfachen Skripten verwenden, um Inhalte im AD wiederherzustellen. Zusätzlich wird erklärt, wie Sie unter Windows Server 2008 R2 den "Papierkorb für das Active Directory" einschalten und damit arbeiten.

Ausflug in die Vergangenheit

Das Active Directory wie wir es kennen wurde mit Windows 2000 geboren. Damals war es ein Verzeichnis, das für alle Größen von Unternehmen konzipiert wurde. Es stellte sich aber heraus, dass es in großen Unternehmen und in der Vielzahl von Einsatzmöglichkeiten das eine oder andere Limit aufwies. Microsoft stellte damals zwei Wiederherstellungsmethoden bereit: die Autoritative und die Nicht-Autoritative Wiederherstellung.

Die Nicht-Autoritative Wiederherstellung stellt einen kompletten Domänencontroller (DC) wieder her, ohne jedoch das AD zu modifizieren. Da sich das AD aber Domänencontroller-übergreifend merkt, welche Änderungen erfolgt sind und auch mit sogenannten "Tombstones" (Grabsteinen) einen Vermerk über das Löschen von Objekten repliziert, bekommt der nicht-autoritativ wiederhergestellte DC, nachdem er an der Replikation wieder teilnimmt, den gleichen Stand wie seine Kollegen. Diese Methode ist also nur zur Wiederherstellung eines DCs geeignet, wenn alle Inhalte des AD in Ordnung sind.

Die Autoritative Wiederherstellung hingegen markiert vom IT-Administrator ausgewählte Objekte als "neuer". Sie können eine Autoritative Wiederherstellung direkt nach einer Nicht-Autoritativen Wiederherstellung durchführen, wenn Sie einen älteren Stand von Objekten oder Objektbäumen benötigen (oder Objekte wieder erhalten möchten, die versehentlich gelöscht wurden). Hierbei ist zu beachten, dass der Domänencontroller zwischenzeitlich nicht replizieren darf. Da beide Arten der Wiederherstellung im Verzeichnisdienstwiederherstellungsmodus durchgeführt werden, in dem keine Replikation möglich ist, sind Sie auf der sicheren Seite, solange Sie den Domänencontroller nicht zwischendurch neu starteten (beziehungsweise ihn vom Netzwerk trennen oder sicher stellen, dass Sie ihn wieder im Verzeichnisdienstwiederherstellungemodus – Directory Service Restore Mode, DSRM – starten).

Interessant dabei ist, dass eine Autoritative Wiederherstellung sich auch ohne eine vorige Nicht-Autoritative Wiederherstellung durchführen lässt, wenn der Server, auf dem

```
Administrator: Eingabeaufforderung - ntdsutil

C:\Users\Administrator.DC01>ntdsutil
ntdsutil: activate instance ntds
Aktive Instanz wurde auf "ntds" gesetzt.
ntdsutil: authoritative restore
authoritative restore: restore subtree cn=Users,dc=example,dc=con

Die DIT-Datenbank wird geöffnet... Der Vorgang ist abgeschlossen.

Aktuelle Zeit 01-22-08 23:14.42.
Die letzte Datenbankaktualisierung erfolgte um 01-22-08 20:01.02.
Die Versionsnummern des Attributs werden um 100000 erhöht.

Die zu aktualisierenden Datensätze werden gezählt...
Gefundene Einträge: 0000000065
Der Vorgang ist abgeschlossen.


65 Einträge wurden für die Aktualisierung gefunden.

Datensätze werden aktualisiert...
Verbleibende Datensätze: 0000000000
Der Vorgang ist abgeschlossen.


65 Datensätze wurden einwandfrei aktualisiert.

Die folgenden Textdatei, die eine Liste autorisiert wiederhergestellter Objekte
enthält, wurde im aktuellen Arbeitsverzeichnis erstellt:
        ar_20080122-231442_objects.txt

Mindestens ein angegebenes Objekt in dieser Domäne verfügt über rückwärtige Verk
nüpfungen. Die folgenden LDIF-Dateien mit Verknüpfungswiederherstellungsvorgänge
n wurden im aktuellen Arbeitsverzeichnis erstellt:
        ar_20080122-231442_links_example.com.ldf

Die autorisierende Wiederherstellung wurde erfolgreich abgeschlossen.

authoritative restore:
```

Bild 1: *NTDSUtil.exe* markiert im Verzeichnisdienstwiederherstellungsmodus rückgesicherte Objekte im Active Directory als "Neuer"

Sie diese durchführen, zum Beispiel von der versehentlichen Änderung oder dem versehentlichen Löschen noch nichts erfahren hat (über die Replikation). Nach einer Autoritativen Wiederherstellung werden die gewünschten Objekte als neuer markiert, und "gewinnen" bei der Replikation gegenüber den alten Objekten, die gelöscht wurden oder die die falschen Daten enthalten.

Autoritativer Restore

Seit Windows 2000 müssen Sie, um bestimmte Objekte wieder herzustellen, eine Autoritative Wiederherstellung durchführen. Starten Sie hierfür den Domänencontroller im Verzeichnisdienstwiederherstellungsmodus. Hierbei sind das Active Directory sowie die Replikation nicht aktiv. Arbeiten Sie an einem DC, der zum Beispiel die Löschung per Replikation noch nicht erhalten hat, haben Sie Glück und können den nächsten Punkt überspringen. Ansonsten müssen Sie eine Wiederherstellung des Systemstatus einleiten. Damit setzen Sie die AD-Datenbank, die Registierungsdatenbank, wichtige Systemdateien, Zertifikatsinformationen sowie SysVol (mit den Inhalten der Gruppenrichtlinien und Anmeldeskripte) auf einen einheitlichen Stand zurück.

Jetzt starten Sie das Kommandozeilentool *NTDSUtil.exe*, mit dem Sie einzelne Objekte oder einen Teil des Baumes des Verzeichnisdienstes als "neuer" markieren. Das ist notwendig, weil der DC nach der Wiederherstellung der Datensicherung zwar den "alten" Stand aufweist, aber sobald er im normalen Modus wieder gestartet wird, die Änderungen durch die Replikation abgeglichen werden. Also würden alle Objekte, die im produktiven AD aktueller sind, wieder überschieben werden. Wenn Sie die Objekte als "neuer" markieren, wird die Versionsnummer um standardmäßig 100.000 erhöht, und damit setzen sich die Objekte im nächsten Replikationszyklus durch.

Hierzu rufen Sie nach dem Nicht-Autoritativen Restore (der Rücksicherung der Datensicherung) *NTDSUtil.exe* auf. Ab Windows Server 2008 müssen Sie zunächst auswählen, dass Sie die "Active Directory Domain Services" bearbeiten möchten – das Kommandozeilentool ist nämlich auch in der Lage, den kleineren Bruder, AD-LDS (Lightweight Domain Services, früher bekannt als AD Application Mode) zu verwalten:

```
Activate Instance NTDS
```

Als nächstes wählen Sie den Unterbereich des autoritativen Restore:

```
Authoritative Restore
```

Jetzt wählen Sie aus, ob Sie einen Verzeichnisdienstbereich (Baum) oder nur ein einzelnes Objekt als "neuer" markieren (zuerst der Befehl für den Baum, dann für ein Objekt):

```
Restore Subtree "ou=Meine
  Benutzer,dc=example,dc=com"

Restore Object "cn=Dummy,pu=Meine
  Benutzer,dc=example,dc=com"
```

Reparatur von Links

Ab Windows Server 2003 SP1 erhalten Sie zusätzlich eine Benachrichtigung, dass LDF-Dateien erstellt wurden, um "rückwärtige Verknüpfungen" wieder herzustellen. Wie wir im vorangegangenen Artikel beschrieben haben, gibt es im AD Verknüpfungen zwischen Objekten, seien es Gruppenmitgliedschaften, technisches wie Links von AD-integrierten Voice-over-IP-Telefonobjekten auf die Benutzer oder die Unternehmenshierarchie über das Manager-Attribut. Hierbei sind immer nur die "Vorwärts-Links" beschreibbar (Gruppe auf Gruppenmitglied, Mitarbeiter auf Manager), nicht aber die Rückwärtslinks ("Mitglied von" eines Benutzerkontos).

Bei der Autoritativen Wiederherstellung lassen sich nur die Vorwärts-Links wieder herstellen und auch nur dann, wenn das Zielobjekt zum Zeitpunkt der Wiederherstellung existiert. Werden zum Beispiel Benutzer und Gruppen gleichzeitig wiederhergestellt, oder zufälligerweise der

```
6 Einträge wurden für die Aktualisierung gefunden.

Datensätze werden aktualisiert...
Verbleibende Datensätze: 0000000000
Der Vorgang ist abgeschlossen.


6 Datensätze wurden einwandfrei aktualisiert.

Die folgenden Textdatei, die eine Liste autorisiert wiederhergestellter Objekte
enthält, wurde im aktuellen Arbeitsverzeichnis erstellt:
        ar_20090930-081438_objects.txt

Mindestens ein angegebenes Objekt in dieser Domäne verfügt über rückwärtige Verk
nüpfungen. Die folgenden LDIF-Dateien mit Verknüpfungswiederherstellungsvorgänge
n wurden im aktuellen Arbeitsverzeichnis erstellt:
        ar_20090930-081438_links_firma.de.ldf

Die autorisierende Wiederherstellung wurde erfolgreich abgeschlossen.

authoritative restore:
```

Bild 2: Bei einer Autoritativen Wiederherstellung unter Windows Server 2003 SP1 (und neuer) werden LDF-Dateien erzeugt, über die der Administrator die fehlenden Verknüpfungen wiederherstellen kann

Mitarbeiter vor dem Manager, wird zwar versucht den Link zu schreiben, da das Zielobjekt aber nicht existiert, wird er wieder verworfen.

Die Problematiken mit den verlinkten Attributen sind enorm und müssen dementsprechend berücksichtigt werden. Zum einen müssen Sie die Objekte, die vielleicht gar nicht gelöscht wurden, aber einen Link auf ein gelöschtes Objekt enthalten, auch wiederherstellen. Zum anderen ist dies vor allem auch domänenübergreifend der Fall, wenn das zurücksichernde Benutzerkonto in einer Gruppe aus einer anderen Domäne enthalten ist.

Mit dem Servicepack 1 von Windows Server 2003 hat Microsoft dann erstmals das Thema mit den Verknüpfungen in Angriff genommen. Wird eine Autoritative Wiederherstellung durchgeführt, werden Dateien mit der Erweiterung "LDF" (sogenannte LDIF-Dateien) erstellt, die die nicht wiederherstellbaren Links enthalten. Wenn Sie diese Dateien nach der Wiederherstellung der Objekte in den entsprechenden Domänen mit dem Tool *LDIFDE.exe* einspielen, werden alle Verknüpfungen wieder hergestellt. Trotzdem ist der Prozess aufwendig – in größeren Umgebungen kann das Zurückspielen der Links länger dauern als der eigentliche autoritative Restore.

Snapshots des Active Directory

Bei Windows Server 2008 führte das Schicksal dazu, dass ein weiteres maßgebliches Feature in diesem Bereich eingeführt wurde: In den ersten Beta-Versionen der eingebauten Datensicherung "Windows Server Backup" hatten die Entwickler vergessen, dass für die Sicherung eines Domänencontrollers eine "Systemstatussicherung" notwendig ist. Das Active Directory-Team hat daraufhin reagiert und die Active Directory-Snapshots entwickelt. Diese ermöglichen es dem Administrator, ein konsistentes Abbild des Zustands der AD-Datenbank online zu einem beliebigen Zeitpunkt zu erstellen. Und mit dem Befehl *dsamain.exe* lässt sich sowohl der Schnappschuss der Datenbank als auch eine Datenbank aus der Sicherung heraus als nur-lesbarer Verzeichnisdienst starten und die Inhalte lesen.

Auf diese Inhalte können Sie auch mit allen Applikationen und Skripten zugreifen, so dass Sie mit relativ einfachen Mitteln Objekte online wiederbeleben und dann die Daten aus dem Snapshot einspielen – ohne jemals in den Wiederherstellungsmodus zu wechseln. Und das in wenigen Minuten.

Snapshots vs. Backup

Den Begriff Snapshot – im Deutschen am ehesten mit "Momentaufnahme" übersetzt – kennt der Administrator üblicherweise aus dem Bereich Storage oder der Datensicherung. Hierbei wird eine Momentaufnahme des Dateisystems gemacht, und der Administrator kann auf diese später wieder zurückgreifen. In Windows sind dies zum Beispiel die Schattenkopiedienste (seit Windows Server 2003), die eine Momentaufnahme des Dateisystems erstellen. Der Administrator kann auf diese Momentaufnahme zurückgreifen, zum Beispiel um ältere Versionen von Dateien wiederherzustellen. Er kann sogar den Anwendern im Windows Explorer unter den Eigenschaften von Dateien oder Ordnern erlauben, auf "Vorherige Versionen" ("Previous Versions" im englischsprachigen Betriebssystem) und auf ältere Daten – zum Beispiel im Homelaufwerk – wieder zuzugreifen.

Auch bei der Datensicherung werden häufig Snapshots verwendet – auch bei der in Windows mitgelieferten "einfachen" Datensicherung. Würde eine Datensicherung nur einfach "Dateien kopieren", hätten diese bei einem größeren Umfang einen zeitlich inkonsistenten Stand. Nehmen wir zum Beispiel an, eine Datensicherung eines bestimmten Dateiservers in unserem Unternehmen dauert vier Stunden und startet um Mitternacht. Beim einfachen Kopieren der Dateien wäre die erste gesicherte Datei von Stand um Mitternacht, während die letzte Datei in der gleichen Sicherung von 4 Uhr morgens ist. Der Einsatz von Momentaufnahmen stellt sicher, dass der Zustand aller Dateien genau um Mitternacht gesichert wird. Damit sind alle Dateien vom gleichen Moment, selbst wenn sie sich während der Datensicherung ändern.

Als Neuerung bietet der Windows Server 2008 an, solche Momentaufnahmen des Active Directory zu erstellen und auf

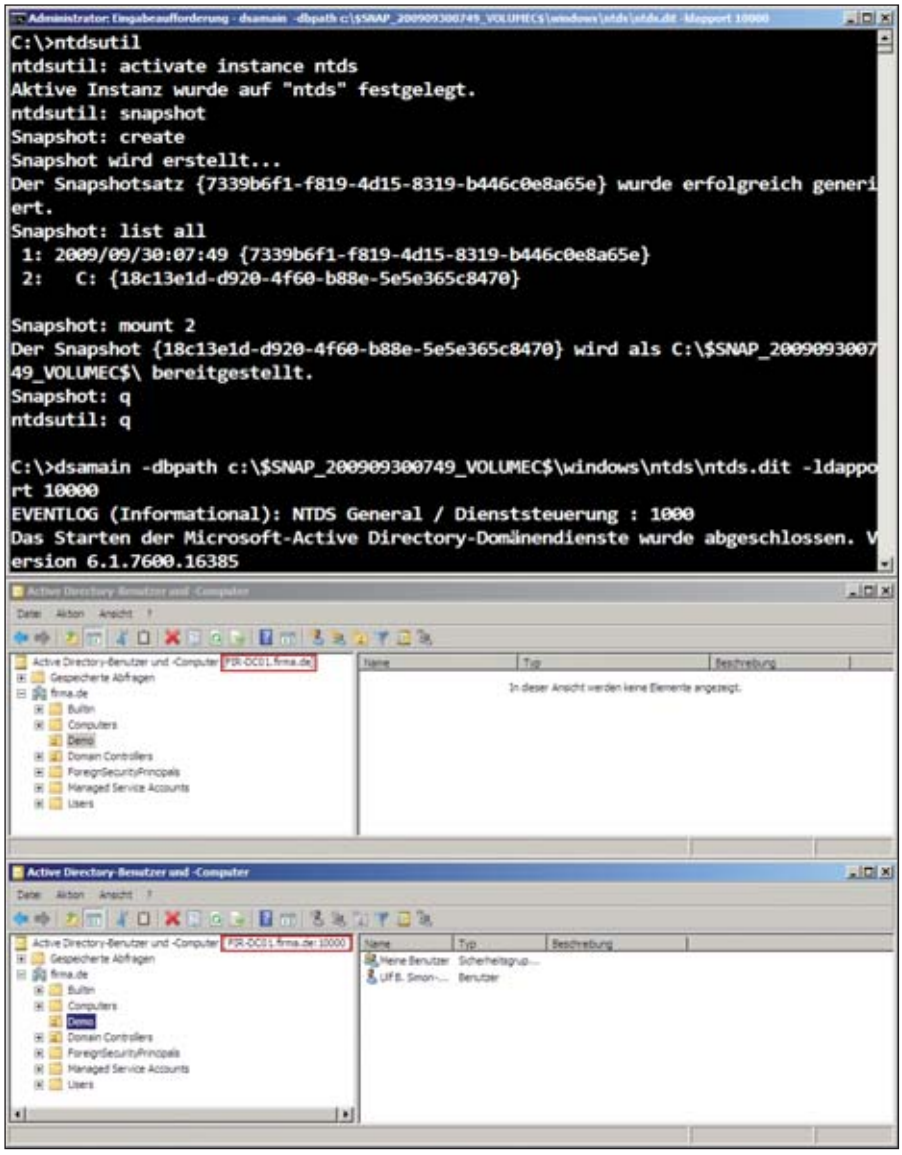


Bild 3: Wie eine Zeitmaschine: Über Snapshots lassen sich vergangene Stati des Active Directory einsehen (wie durch die Angabe des Ports zu sehen, stellt die untere Konsole den Snapshot dar)

diese dann später sogar lesend zuzugreifen. Das klingt auf den ersten Blick etwas unspektakulär, hat aber enorme Vorteile. Um auf die Momentaufnahmen lesend zuzugreifen, starten Sie diese als zusätzlichen LDAP-Verzeichnisdienst und greifen darauf mit den gleichen Mitteln zu, die Ihnen von der AD-Verwaltung bekannt sind (Details dazu später in diesem Artikel). Besonders Skripte können Sie hier einsetzen, um Informationen aus dem "alten" Stand des AD auszulesen und diese sogar in der Produktivumgebung wieder zu setzen. Und – wie wir später zeigen – damit sogar Benutzerkonten oder Gruppen wiederherstellen, sollten Sie diese versehentlich gelöscht haben.

Dies ersetzt allerdings nicht eine Datensicherung des Active Directory beziehungsweise des Systemstatus. Es ist jedoch eine gute und sinnvolle Ergänzung. Die Snapshots können Sie nicht dazu verwenden, um Teile der Konfigurations- oder Schema-Partition wiederherzustellen. Dies wird nicht von Microsoft unterstützt. Auch gibt es derzeit keine Möglichkeit, die Inhalte ohne Skripte wiederherzustellen. Und auch Passwörter gehen normalerweise verloren, wenn die Momentaufnahme genutzt wird, um ein Benutzer- oder Computerkonto wieder zum Leben zu erwecken. Aber eine Datensicherung wird üblicherweise nur nachts durchgeführt und eine Wiederherstellung aus dieser ist aufwendig – Momentaufnahmen können Sie dagegen leicht mehrmals unter Tags durchführen und die Wiederherstellung ist relativ einfach.

Erstellen von Snapshots

Das Erstellen einer Momentaufnahme des Active Directory führen Sie mit dem Tool *NTDSUtil.exe* durch. Der Hintergrund hierfür ist die Funktionsweise: Da das Active Directory in einer Datenbank gespeichert ist (in einer Extensible Storage Engine, genau wie Exchange) muss vor dem Erstellen einer Momentaufnahme sichergestellt werden, dass die Datenbank in sich konsistent ist. Daher reicht es nicht aus, einfach eine "Schattenkopie" im Betriebssystem zu erstellen, sondern NTDSUtil kümmert sich um den Ablauf.

Für den Administrator stellt sich das recht einfach dar. In der Kommandozeile des Windows Server 2008 Domänencontrollers geben Sie den Befehl *NTDSUtil* ein. Dann erstellen Sie mit den folgenden Kommandos eine Momentaufnahme. Zunächst *snapshot*, dann wechseln Sie in den Kontext "Snapshot" des NTDSUtil. Mit

```
Activate Instance NTDS
```

geben Sie an, dass Sie die Active Directory-Domänendienste bearbeiten möchten, und nicht eine Instanz der Active Directory-Leighweight Domain Services (AD-LDS, vormals bekannt als ADAM).

Über *create* erstellen Sie nun die Momentaufnahme. Um zu ermitteln, welche Momentaufnahmen auf dem System bereits erstellt wurden, nutzen Sie das Kommando: *List All*. Zu guter Letzt können Sie über *Delete {GUID}* auch Snapshots löschen. Hierbei müssen Sie den Global Unique Identifier (die lange, hexadezimale Zahl in geschweiften Klammern) angeben oder die Nummer des Snaps-

```
Administrator: Eingabeaufforderung - ntdsutil
C:\>ntdsutil
ntdsutil: snapshot
Snapshot: activate instance ntds
Aktive Instanz wurde auf "ntds" festgelegt.
Snapshot: create
Snapshot wird erstellt...
Der Snapshotsatz {5303a66b-83d8-4b96-8556-ff15c61f8fcd} wurde erfolgreich generi
ert.
Snapshot: list all
 1: 2008/02/14:00:22 {5303a66b-83d8-4b96-8556-ff15c61f8fcd}
 2:   C: {1b98a220-25fe-4202-a548-2e9e6f49f030}

Snapshot: mount {1b98a220-25fe-4202-a548-2e9e6f49f030}
Der Snapshot {1b98a220-25fe-4202-a548-2e9e6f49f030} wird als C:\$SNAP_2008021400
22_VOLUMEC$\ bereitgestellt.
Snapshot: _
```

Bild 4: Über NTDSUtil lassen sich die Snapshots des Domänencontrollers verwalten

```
Administrator: Eingabeaufforderung - dsamain -dbpath c:\$SNAP_200802140022_VOLUMEC$\Window...
C:\>dsamain -dbpath c:\$SNAP_200802140022_VOLUMEC$\Windows\NTDS\ntds.dit -ldappo
rt 10000
EVENTLOG (Informational): NTDS General / Dienststeuerung : 1000
Das Starten der Microsoft-Active Directory-Domänendienste wurde abgeschlossen. V
ersion 6.0.6001.18000
```

Bild 5: Mit DSAMain startet ein Snapshot als separater Verzeichnisdienst

hots, die Sie über *List All* erhalten haben. Mit *Delete* * löschen Sie alle Momentaufnahmen auf dem System.

Natürlich lässt sich das Erstellen von Momentaufnahmen auch durch eine geplante Aufgabe ("Scheduled Task") erledigen, hierzu nutzen Sie:

```
NTDSUtil.exe Snapshot "Activate
  Instance NTDS" Create Quit Quit
```

Einsicht in einen Snapshot oder eine Datensicherung

Um in eine Momentaufnahme oder eine Datensicherung hinein zu sehen, müssen Sie zunächst auf die Datenbankdatei *NTDS.dit* in der Momentaufnahme oder Datensicherung zugreifen. Für eine Datensicherung ist das nicht schwer: Sie sichern die Datei einfach an eine andere Stelle zurück. Die Datei befindet sich standardmäßig unter *c:\windows\ntds*, wird aber bei größeren ADs auch häufig auf andere Festplatten oder Partitionen verschoben.

Einen Snapshot müssen Sie zunächst verbinden, was Sie wieder mit NTDSUtil erledigen. Hierzu dient der Befehl *Mount* im Subkontext "Snapshot". Nachdem Sie zunächst *List All* nutzen, können Sie einfach die Index-Nummer des Snapshots verwenden (ansonsten müssen Sie den Global Unique Identifyer (GUID) angeben):

```
Mount {GUID}
```

Dieser Befehl bindet die Momentaufnahme in das Dateisystem in ein virtuelles Verzeichnis "c:\$SNAP_..." (der weitere Name ergibt sich aus dem erstellten Datum sowie dem Laufwerksbuchstaben) ein. Um jetzt in die Active Directory-Datenbank sehen zu können, starten Sie diese als zusätzlichen Verzeichnisdienst auf einem anderen Netzwerk-Port. Dies erledigen Sie mit dem Befehl *DSAMain*. Der Befehl muss dabei mindestens die Parameter "-dbpath" (mit dem kompletten Dateinamen der *NTDS.dit*) und "-ldapport" (mit der Portnummer, auf der der LDAP-Dienst angeboten werden soll) enthalten. Wichtig ist zu beachten, dass der Active Directory-Verzeichnisdienst immer vier Ports benötigt: einen für LDAP, einen für LDAP via SSL/TLS, einen für den Globalen Katalog und einen für den Globalen Katalog via SSL/TLS. Wenn Sie nur den LDAP-Port angeben, werden die anderen Dienste auf den drei nächsthöher gelegenen Ports zur Verfügung gestellt.

```
DSAMain.exe -dbpath
  {c:\$snap...\windows\system32\ntds
  \ntds.dit} -ldapport 10000
```

Um jetzt in den Snapshot hineinzusehen, nutzen Sie die Standard-Administrationswerkzeuge wie "Active Directory-Benutzer und -Computer", *ADSIEdit.msc*, *LDP.exe* und die verschiedenen DS-Tools.

In "Active Directory-Benutzer und -Computer" klicken Sie unter Windows Server 2008 mit der rechten Maustaste auf den obersten Knoten, der als "Active Directory-Benutzer und -Computer" bekannt ist und wählen "Domänencontroller ändern ..." aus. Im folgenden Dialog können Sie zwischen existierenden Domänencontrollern wählen oder Sie geben einen DC (wahlweise mit Port) manuell an. Dies nutzen Sie, um sich mit dem Snapshot zu verbinden. Hier geben Sie den Namen Ihres DCs ein und danach einen Doppelpunkt und die Portnummer (in unserem Beispiel 10.000). Jetzt können Sie die Inhalte der Momentaufnahme betrachten.

Wiederbeleben gelöschter Objekte

Wenn Objekte wie Benutzerkonten, Computerkonten oder Gruppen gelöscht werden [1], markiert das Active Directory diese zunächst als gelöscht (setzt das Attribut "isDeleted" auf "WAHR"), ändert die Namen (beinhalten die GUID),

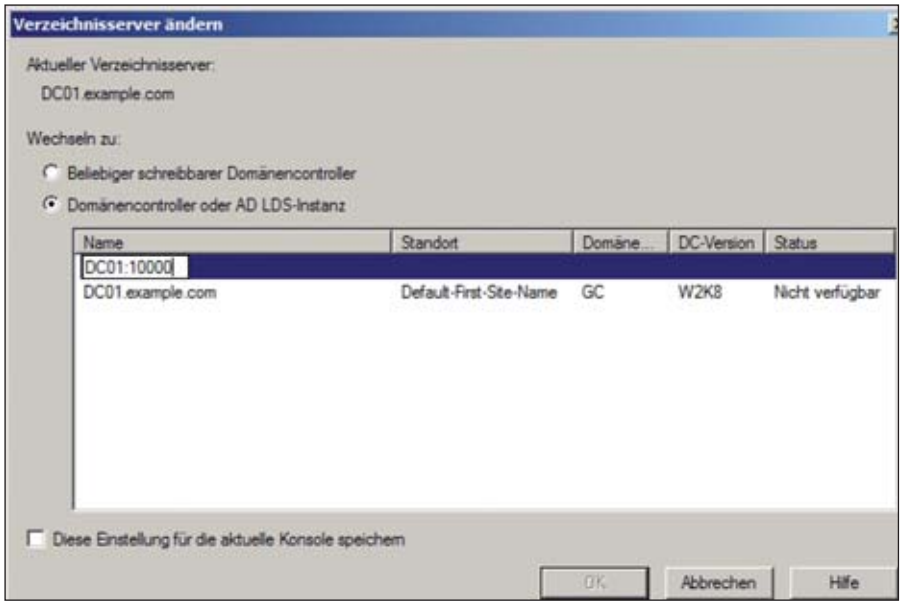


Bild 6: Sogar "Active Directory-Benutzer und -Computer" kann der Administrator verwenden, um in die Momentaufnahme einzusehen – hierzu muss er lediglich den Server und die Portnummer manuell eingeben

verschiebt das Objekt in den "Deleted Objects"-Container und löscht die meisten Attribute. Einige Attribute bleiben jedoch erhalten, wie zum Beispiel der Security-Identifyer (SID), über den die Berechtigungen laufen. Die gelöschten Objekte werden auch Tombstone (Grabstein) genannt. Diese bleiben für die Tombstone-Lifetime (standardmäßig 60 beziehungsweise 180 Tage, siehe Kasten "Wie lange ist das Backup gut?") im Active Directory, damit sichergestellt wird, dass alle DCs wissen, dass dieses Objekt gelöscht werden soll. Wenn die Tombstone-Lifetime abgelaufen ist, kümmert sich der Aufräumvorgang (Garbage Collection, dieser läuft alle 12 Stunden) auf jedem DC darum, das Objekt endgültig zu entfernen. Das ist für uns interessant, weil Sie das Benutzerkonto mit seiner alten SID wieder herstellen können, da sich diese Tombstones auch wieder in "normale" Benutzerkonten umwandeln lassen.

In den Internet-Communities sind damals (zu Windows 2000-Zeiten) schon Tricks aufgekommen, wie sich ein gelöschtes Objekt (Tombstone) wiederbeleben lässt. Zwar beinhaltet der Tombstone fast keine Daten mehr, allerding hat es noch den gleichen Security Identifier, der für die Vergabe der Berechtigungen in der Windows-Welt wichtig ist. Alle anderen Daten mussten per Hand gefüllt werden.

Unter Windows Server 2003 unterstützte Microsoft dann das Wiederbeleben der Tombstones offiziell. Es gab eine API hierfür und Hersteller wie Aelita (später Quest), NetPro (jetzt auch Quest) und weitere Tools wie ADRestore [2] von SysInternals (jetzt Microsoft) wurden offiziell unterstützt, wenn sie die API verwendeten.

Wenn Sie zum Beispiel ein gelöschtes Benutzerkonto wieder zum Leben erwecken möchten, lassen Sie sich mit ADRestore zunächst eine Liste aller gelöschter Objekte anzeigen:

```
adrestore.exe
```

Um Objekte wiederherzustellen, verwenden Sie den Parameter "-r" in ADRestore. Zusätzlich können Sie auch einen Suchfilter mit eingeben. Nehmen wir an, Sie bearbeiten ein gelöschtes Benutzerkonto. Wie Bild 7 darstellt, enthielt das Benutzerkonto vor der Löschung zahlreiche Attribute.

Um den Benutzer mit ADRestore aus einem Tombstone wiederherzustellen, nutzen Sie den folgenden Befehl:

```
adrestore.exe -r "Mannfred
  Mustermann"
```

Das so restaurierte Benutzerobjekt hat jetzt aber fast keine Attribute mehr, nicht nur die Beschreibungen, Homelaufwerk und Profilpfade fehlen, sondern auch zahlreiche weitere Informationen. Auch die Gruppenmitgliedschaften wurden aufgeräumt (dazu später mehr).

Was Sie nicht über andere Wege zurückerhalten, ist das Passwort – das setzen Sie gleich auf einen neuen Wert und teilen es dem Anwender mit. Alle anderen wichtigen Informationen erhalten Sie aus einem Snapshot zurück.

Informationen aus Snapshots recovern

Um Informationen aus einem Snapshot zurückzuholen, müssen Sie etwas Scripting einsetzen. Bleiben wir bei unserem wiederbelebten Benutzerkonto: Um die weiteren Informationen des Benutzerkontos aus der Momentaufnahme zu erhalten, exportieren Sie diese in eine LDF-Datei. Eine LDIF-Datei (oder LDF unter Wind-

Die Deleted-Objects-Lifetime ist der Zeitraum, in der ein Objekt zwar gelöscht wird, aber zunächst noch vollständig erhalten bleibt und sich inklusive aller Verknüpfungen wiederherstellen lässt. Die Tombstone-Lifetime bezeichnet die Dauer, in der ein Objekt gelöscht und aufgehoben wird, damit alle Domänencontroller mitbekommen, dass dieses Objekt zu löschen ist.

Standardmäßig entspricht die Deleted Objects Lifetime der Tombstone Lifetime. Diese wiederum ist davon abhängig, auf Basis welches Betriebssystems die Gesamtstruktur errichtet wurde:

- Vor Windows Server 2003 SP1: 60 Tage
- Windows Server 2003 SP1: 180 Tage
- Windows Server 2003 R2: 60 Tage
- Windows Server 2003 (R2) SP2: 180 Tage
- Windows Server 2008 und höher: 180 Tage

Wie lange ist das Backup gut?

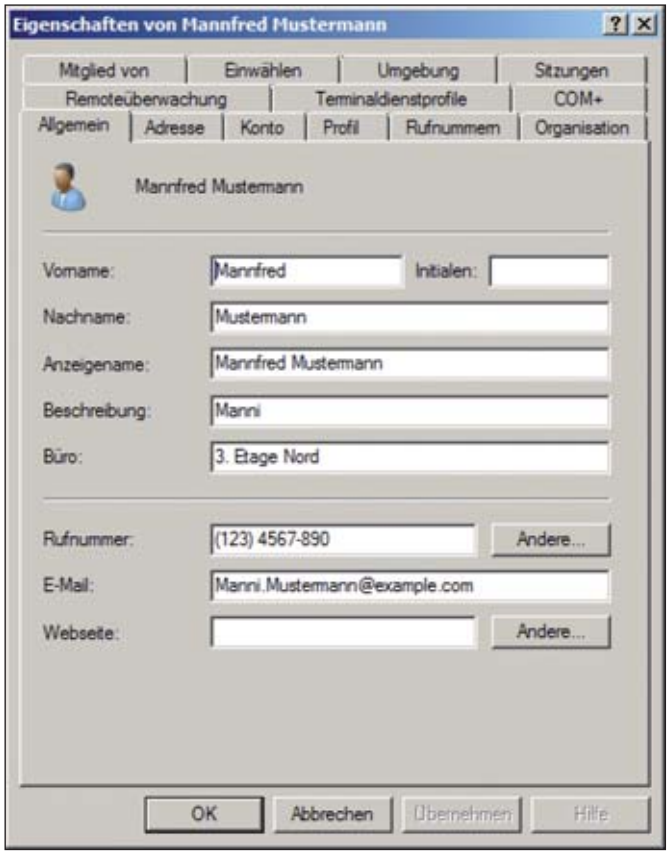


Bild 7: Ein Benutzerkonto hat eine Menge zusätzlich Attribute, bevor es gelöscht wird

ows) ist ein gebräuchliches Import-/Exportformat für LDAP-Verzeichnisdienste. Unter Windows steht Ihnen hierfür das Kommandozeilenwerkzeug *LDIFDE.exe* zur Verfügung. Mit dem Parameter "-t" legen Sie eine alternative Portnummer fest, über "-f" steuern Sie den Dateinamen für die Ausgabe.

```
ldifde.exe -r "(sn=Mustermann)" -t
  10000 -f {c:\Mannfred.ldf}
```

In der LDF-Datei finden sich nun alle Attribute des Benutzerobjektes. Allerdings ist die Datei dafür ausgelegt, neue Benutzer zu erzeugen. Wir haben den Benutzer jedoch wiederbelebt, um die SID und damit seine Berechtigungen zurück zu erhalten. Daher können Sie mit der LDF-Datei keinen neuen Benutzer mit dem gleichen Namen anlegen. Was wir eigentlich wollen, ist eine LDF-Datei, die alle Attribute des Benutzers auf die alten Werte des Snapshots ändert. Hierzu müssen Sie die LDF-Datei so modifizieren, dass jedes Attribut einzeln behandelt wird und der "changetype" von "add" auf "modify" geändert wird.

Hierbei hilft uns ein Skript. Das Beispielskript in Listing 1mit der Unterroutine "ModifyLDIF" konvertiert eine LDF-Datei in den "changetype modify".

Nachdem Sie die LDF-Datei umgewandelt haben, können Sie das Objekt jetzt ändern. Hierzu müssen Sie die Datei lediglich importieren. Da Sie alle Werte exportiert haben, aber einige der Werte vom System verwaltet werden (zum Beispiel, wann ein Objekt zuletzt geändert wurde) geben Sie dem LDIFDE-Kommando folgende Parameter mit, um "nicht beschreibbare" Attribute zu ignorieren und mit den Änderungen fortzusetzen:

```
ldifde.exe -i -z -k -v -f
  c:\mod-Manni.ldf
```

Anschließend hat das Objekt wieder alle Werte, die es auch vor dem Löschen hatte.

Eine ähnliche Vorgehensweise wählen Sie auch, wenn nur bestimmte Attribute über mehrere Benutzer hinweg gelöscht oder geändert wurden. Dies kann zum Beispiel durch ein fehlerhaftes Skript, oder die Mehrfachselektion und -änderung in "Active Directory-Benutzer und -Computer" passieren. In diesem Fall gebe Sie mit dem Parameter "-l" in LDIFDE an, welche Attribute exportiert werden sollen.

Gruppenmitgliedschaften sind jedoch – wie oben beschrieben – sogenannte "Backlinks" auf dem Benutzerobjekt, also nicht beschreibbar. Hier müssen Sie die "Forwardlinks" beschreiben, also das "Member"-Attribut des Gruppenobjektes. Dabei behelfen Sie sich mit einer einfachen Kommandozeile. Über das DSget-Kommando starten Sie eine Anfrage gegen den Globalen Katalogserver des Snapshots. Dessen Portnummer liegt zwei über dem LDAPPort (oder Sie geben eine Portnummer explizit in DSamain ein). Mit dem DSget-Kommando fragen Sie das "MemberOf"-Attribut des Objektes ab und erhalten eine Liste aller Gruppen (der Domäne sowie Universeller Gruppen), bei denen das Objekt zum Zeitpunkt der Momentaufnahme Mitglied war:

```
dsget.exe user "cn=Mannfred Muster-
  mann,ou=Meine Benutzer,dc=exam-
  ple,dc=com" -s localhost:10002
  -memberof
```

Um jetzt die Gruppen zu ändern und das Objekt neu hinzuzufügen, pipen Sie

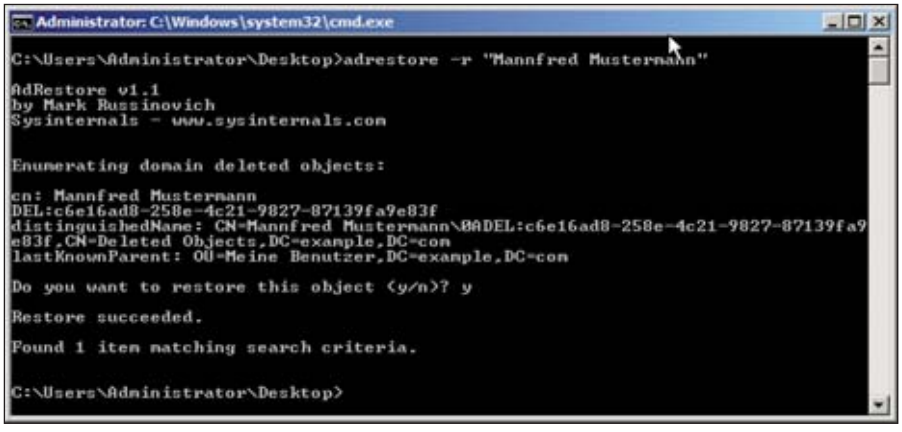


Bild 8: Mit ADRestore lässt sich ein Objekt aus einem Tombstone wieder zum Leben erwecken

die Ausgabe von DSget einfach in ein DSmod-Kommando. Somit fügen Sie das Objekt im produktiven Active Directory zu den Gruppen hinzu, in denen es schon zum Zeitpunkt des Snapshots enthalten war.

```
dsget.exe user "cn=Mannfred Muster-
  mann,ou=Meine Benutzer,dc=exam-
  ple,dc=com" -s localhost:10002
  -memberof | dsmod.exe group
  -addmbr "cn=Mannfred
  Mustermann,ou=Meine
  Benutzer,dc=example,dc=com"
```

Hierbei kann es sein, dass Sie Fehlermeldungen erhalten. Die Fehlermeldung bezüglich der Domänenbenutzer können Sie getrost ignorieren, da diese vom System verwaltet werden. Auch in anderen Fällen (Domänenübergreifende Gruppen und Berechtigungen auf diese) kann es sein, dass Sie die Vorgehensweise geringfügig ändern müssen, aber die prinzipiellen Techniken sind die gleichen.

Snapshots können Sie also verwenden, um häufiger einen Zwischenstand des Active Directory zu speichern und diese Informationen zur Recherche (wer war wann in welchen Gruppen, wie waren die Einstellungen gestern, als es noch funktioniert hat), zum Zurückspielen von einzelnen Attributen oder sogar von ganzen Benutzerobjekten zu nutzen.

Der Papierkorb für das Active Directory

In Windows Server 2008 R2 wurde das Thema "Wiederherstellung von Objekten" zum ersten Mal konsequent adressiert. Da dies die häufigste Ursache für Active Directory-Wiederherstellungen ist, musste es einfacher gestaltet werden. Dazu hat Microsoft mit dem Papierkorb [3] die Möglichkeit geschaffen, gelöschte Objekte durch einen einfachen Befehl komplett wieder herzustellen – mit allen Gruppenmitgliedschaften und sonstigen Verknüpfungen.

Vereinfacht betrachtet, besitzt in der Datenbankstruktur des AD jedes Objekt in der Datentabelle eine Zeile, die einen primären Schlüssel aufweist. Daneben existiert eine Link-Tabelle, die zum Beispiel von dem Schlüssel für eine Gruppe auf den Schlüssel eines Benutzers verweist, wenn dieser Mitglied in der Gruppe ist. Wird ein Benutzer gelöscht, löscht Windows Server 2008 (und frühere Versionen) die meisten Eigenschaften des Objekts, da diese ja nicht mehr benötigt werden. Des Weiteren verschiebt das System das Objekt in den "Deleted Objects"-Container, ändert den Namen und setzt den Wert "isDeleted" auf "Wahr". Alle Links, die das Objekt referenzieren, werden gelöscht und zwar direkt von jedem Domänencontroller. Das Objekt, das jetzt nur noch ein Tombstone ist, wird als solcher repliziert. Damit erfahren alle DCs, dass es zu löschen ist und entfernen dabei auch die Links. Daher gab es auch keine Möglichkeit, ein Objekt einfach wieder herzustellen – zumindest um die Verknüpfungen mussten sich die Administratoren kümmern.

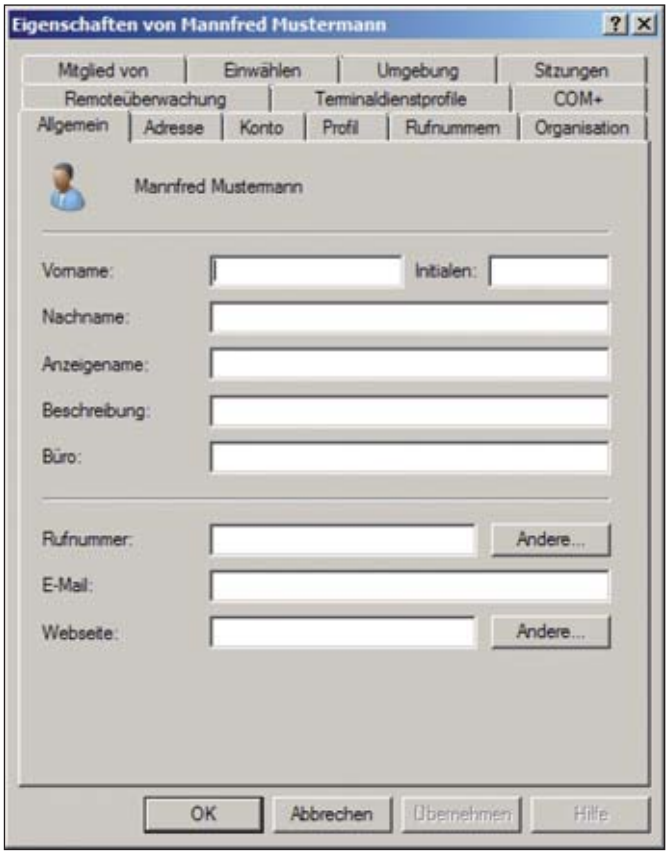


Bild 9: Nach dem Wiederbeleben eines Benutzerkontos sind nur noch wenige Attribute vorhanden

Seit Windows Server 2008 R2 können Sie den Active Directory-Recyclebin einschalten. Dieser unterscheidet zwischen gelöschten und recycelten Objekten. Gelöschte Objekte behalten die Werte aller Eigenschaften, werden jedoch als gelöscht

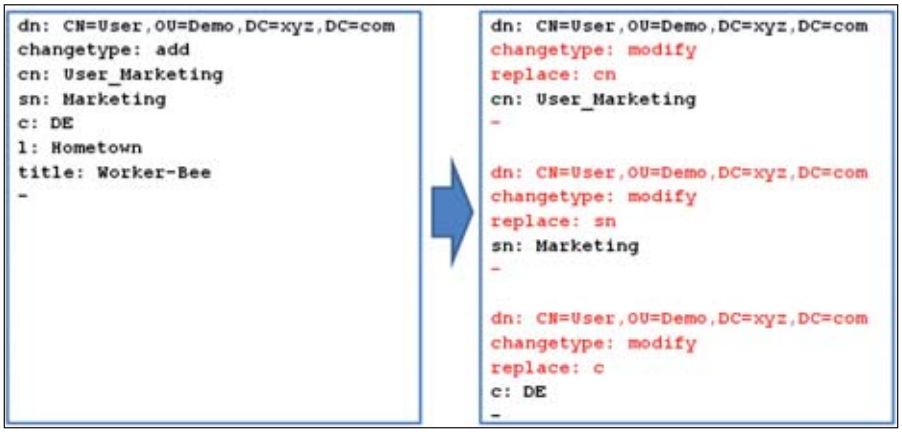


Bild 10: Die LDF-Datei muss geändert werden, so dass sich – anstatt neue Objekte hinzuzufügen – alle Attribute eines existierenden Objekts ändern

Das Skript dient zur Umwandlung von LDF-Dateien von Changetype ADD zu Changetype MODIFY, das heißt, jedes Attribut wird einzeln geändert.
Verwendete Parameter:
- sInput: Vollständiger Dateiname der Eingabedatei (LDF)
- sOutput: Vollständiger Dateiname der Ausgabedatei (LDF)
- bDelSource: wenn TRUE, wird die Eingabedatei hinterher gelöscht

```
set objArgs = WScript.Arguments
if objArgs.Count = 0 or objArgs.Count > 3 then
   ShowUsage
sInput = objArgs(0)
if objArgs.Count > 1 then
  sOutput = objArgs(1)
else
  sOutput = ""
  arrOut = split(sInput,"\")
  for i = 0 to ubound(arrOut)-1
    sOutput = sOutput & arrOut(i) & "\"
  next
  sOutput = sOutput & "mod_" & arrOut(ubound(arrOut))
end if
if objArgs.Count > 2 then
  bDelSource = objArgs(2)
else
  bDelSource = FALSE
end if
sOut = "ModifyLDIF.vbs" & vbcr
sOut = sOut & "(c) Ulf B. Simon-Weidner,
   www.msmvps.com/ulfbsimonweidner" & vbcr
sOut = sOut & vbcr
sOut = sOut & "Inputfile:  " & sInput & vbcr
sOut = sOut & "Outputfile: " & sOutput & vbcr
if bDelSource then sOut = sOut & "Inputfile will be
   deleted after conversion" & vbcr
WScript.Echo sOut
ModifyLDIF sInput, sOutput, bDelSource
WScript.Quit

sub ModifyLDIF(sInput,sOutput,bDelSource)
  Set oFSO = CreateObject("Scripting.FileSystemOb-
   ject")
  Set oInput = oFSO.OpenTextFile(sInput, 1)
  set oOutPut = oFSO.OpenTextFile(sOutput, 2, True)
  sParm2 = ""
  bEndOfDataOpen = FALSE
  Do While oInput.AtEndOfStream <> True
    sLine = oInput.ReadLine
    if sLine<>"" then
      select case left(sLine,1)
        case " "
           oOutput.WriteLine sLine
        case "-"
          'oOutput.WriteLine sLine
        case else
          if bolBinary then
            oOutput.WriteLine "-"
            oOutput.WriteLine ""
            bolBinary = FALSE
          end if
          sParm = left(sLine,instr(sLine,":")-1)
          sValue = trim(mid(sLine,instr(sLine,":")+1))
          if left(sValue,1) = ":" then
            'First line of a binary value
            if bEndOfDataOpen then
              oOutput.WriteLine "-"
              oOutput.WriteLine ""
              bEndOfDataOpen = FALSE
            end if
            oOutput.WriteLine "dn: " & sCurrentDN
            oOutput.WriteLine "changetype: modify"
            oOutput.WriteLine "replace: " & sParm
            oOutput.WriteLine sParm & ":" & sValue
            bolBinary = TRUE
          else
            select case sParm
              case "dn"
                sCurrentDN = sValue
              case "changetype"
                ' ignore this one
              case "-"
                ' ignore this one as well
              case sParm2
                ' MultiValue
                oOutput.WriteLine sParm & ": "
                    & sValue
              case else
                if bEndOfDataOpen then
                  oOutput.WriteLine "-"
                  oOutput.WriteLine ""
                  bEndOfDataOpen = FALSE
                end if
                oOutput.WriteLine "dn: " & sCurrentDN
                oOutput.WriteLine "changetype: modify"
                oOutput.WriteLine "replace: " & sParm
                oOutput.WriteLine sParm & ": "
                    & sValue
                bEndOfDataOpen = TRUE
            end select
          end if
          sParm2 = sParm
      end select
    end if
  Loop
  if bEndOfDataOpen then
    oOutput.WriteLine "-"
    oOutput.WriteLine ""
    bEndOfDataOpen = FALSE
  end if
  oInput.Close
  oOutput.Close
  set oInput = nothing
  set oOutput = nothing
  if bDelSource then
    oFSO.DeleteFile(sInput)
  end if
  set oFSO = nothing
end sub

sub ShowUsage
  WScript.Echo "ModifyLdif.vbs <inputfile.ldf>
   [<outputfile.ldf> [<deleteinput>]]"
  WScript.Echo "  inputfile:
   Filename of the inputfile"
  WScript.Echo "  outputfile:
   Filename of the outputfile"
  WScript.Echo "
   If not provided, the filename of the inputfile"
  WScript.Echo "
   will be prefixed with a ""mod_"""
  WScript.Echo "
   deleteinput: True or False (default),
   if True the inputfile"
  WScript.Echo "
   will be deleted after the outputfile is written"
  WScript.Quit
end sub
```

Listing: ModifyLDIF.vbs

markiert. Die Verknüpfungstabelle wird mit dem Einschalten des Papierkorbs erweitert – Verknüpfungen von gelöschten Objekten lassen sich deaktivieren. Diese gelöschten Objekte bleiben eine Zeit in der Infrastruktur erhalten und zwar für die "Deleted Objects Lifetime". Wenn diese abgelaufen ist, werden die Objekte recycled: Die Werte der Eigenschaften und die deaktiverten Links werden gelöscht. Die recycelten Objekte werden dann wie gehabt für die Dauer der Tombstone-Lifetime mitrepliziert (damit auch alle DCs von der Änderung erfahren) und danach komplett gelöscht. Durch diese Vorgehensweise lassen sich bei eingeschaltetem Papierkorb Objekte einfach wieder herstellen, indem sie wiederbelebt werden. Alle Eigenschaften und sogar die Gruppenmitgliedschaften bleiben erhalten.

Einschalten des Papierkorbs

Ein Wermutstropfen ist, das diese Funktion einen neuen Gesamtstrukturmodus benötigt: Alle Domänencontroller aller Domänen der Gesamtstruktur bedürfen Windows Server 2008 R2 oder höher als Betriebssystem. Nur dann können Sie den Gesamtstrukturmodus anheben und den Papierkorb einschalten. Wenn wir überlegen, wie das Ganze funktioniert, wird auch klar: Das Löschen/Deaktiveren der Links erfolgt auf jedem DC einzeln, Verknüpfungen können auch domänenübergreifend existieren. Nur indem jeder DC in der Lage ist, die Werte der Eigenschaften zu erhalten und die Links nur zu deaktivieren, kann das Feature funktionieren. Aber ein kleiner Lichtblick bleibt: Seit Windows Server 2008 R2 ist es möglich, das Anheben des Domänen- oder Gesamtstrukturlevels wieder rückgängig zu machen, solange keine Funktionen aktiv sind, die dies verhindern. Der Recyclebin ist eine solche Funktion (und auch die einzige derzeit existierende Funktion).

Zunächst müssen Sie also den Level aller Domänen auf Windows Server 2008 R2 heben. Anschließend heben Sie den Level der Gesamtstruktur auf Windows Ser-

```
Administrator: C:\Windows\system32\cmd.exe
C:\>dsget user "cn=Mannfred Mustermann,ou=Meine Benutzer,dc=example,dc=com" -s l
ocalhost:10002 -memberof | dsmod group -addmbr "cn=Mannfred Mustermann,ou=Meine
Benutzer,dc=example,dc=com"
dsmod war erfolgreich:CN=GG_MannisAbteilung,OU=Meine Benutzer,DC=example,DC=com
dsmod Fehler:CN=Domänen-Benutzer,CN=Users,DC=example,DC=com:Entweder ist das ang
egebene Benutzerkonto bereits ein Mitglied der angegebenen Gruppe, oder die ange
gebene Gruppe kann nicht gelöscht werden, da sie ein Mitglied enthält.
Geben Sie "dsmod /?" ein, um die Hilfe anzuzeigen.
C:\>
```

Bild 11: Mit einem einfachen Kommandozeilenbefehl lassen sich auch die Gruppenmitgliedschaften wiederherstellen

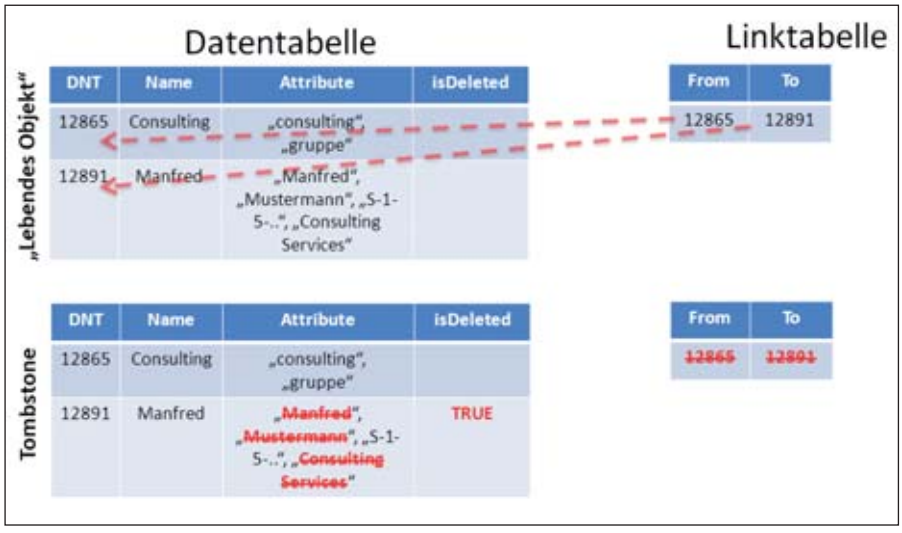


Bild 12: Unter Windows Server 2008 hat ein gelöschtes Objekt kaum noch Eigenschaften und Verknüpfungen

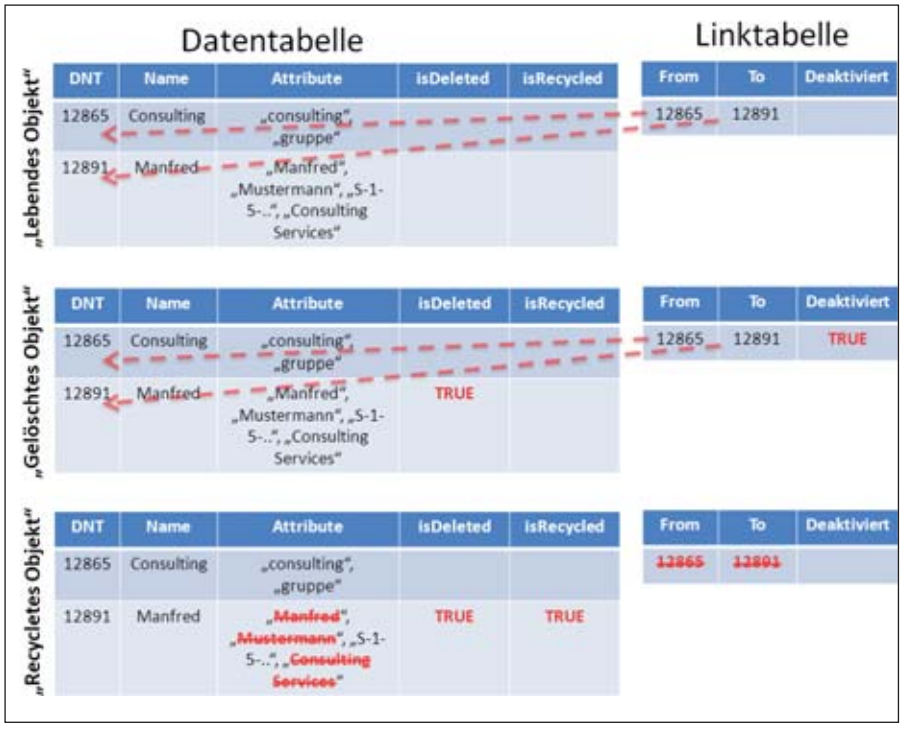


Bild 13: Wenn ein Objekt beim eingeschalteten Papierkorb (R2) gelöscht wird, bleiben alle Eigenschaften erhalten und Verknüpfungen werden nur deaktiviert. Nachdem die "Deleted Objects Lifetime" abgelaufen ist, werden diese wie bisher gelöscht und als "Tombstones / Recycled Objects" repliziert.

ver 2008 R2. Sind Sie sich sicher, dass Sie das neue Level beibehalten möchten und keine Windows Server 2008 (ohne R2)-DCs mehr promoten möchten, können Sie den Recyclebin einschalten.

Während Sie das Hochsetzen des Domänen- und Gesamtstrukturmodus mit den üblichen Verwaltungskonsolen bewerkstelligen, benötigen Sie sowohl für das Herunterstufen des Levels wie auch für das Einschalten des Papierkorbs die PowerShell unter Windows Server 2008 R2 (oder Windows 7 mit den Remote Server Administration Tools für Windows Server 2008 R2), die die neuen Active Directory-Cmdlets [4]enthalten.

Am einfachsten starten Sie die PowerShell über das Active Directory mittels "Startmenü / Verwaltung / Active Directory-Modul für Windows Powershell". Sollten Sie die PowerShell über das Symbol in der Taskbar gestartet haben, laden Sie mit folgendem Befehl die Active Directory-Module:

```
Import-Module ActiveDirectory
```

Hierbei wird das Active Directory-Modul geladen und ein virtuelles Laufwerk verbunden – geben Sie *cd AD:* ein und verwenden Sie die "dir"- und "cd"-Befehle, um durch das AD zu navigieren (Achtung – Sie müssen immer den RDN, also zum Beispiel "cd cn=users" verwenden). Nach dem Laden des Active Directory-Moduls können Sie den Domänenmodus anheben (wenn alle DCs auf Windows Server 2008 R2 sind). In unserem Beispiel hat die Domäne den DNS-Namen "firma.de":

```
Set-ADDomainMode -identity firma.de
  -DomainMode Windows2008R2Domain
```

Laufen alle Domänen auf dem R2-Domänenmodus, heben Sie analog dazu den Gesamtstrukturmodus mit

```
Set-ADForestMode -identity firma.de
  -ForestMode Windows2008R2Forest
```

```
Administrator: Windows PowerShell
PS C:\> Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurat
ionSet -Target 'firma.de' -server FIR-DC01
WARNUNG: Das Aktivieren von "Recycle Bin Feature" auf
"CN=Partitions,CN=Configuration,DC=firma,DC=de" kann nicht rückgängig gemacht
werden. Wenn Sie den Vorgang fortsetzen, können Sie "Recycle Bin Feature" auf
"CN=Partitions,CN=Configuration,DC=firma,DC=de" nicht deaktivieren.

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Enable" für das Ziel "Recycle Bin Feature".
[J] Ja  [A] Ja, alle  [N] Nein  [K] Nein, keine  [H] Anhalten  [?] Hilfe
(Standard ist "J"):j
PS C:\>
```

Bild 14: Nach der Anhebung des Domänen- und Forestmodus lässt sich der AD-Papierkorb über die PowerShell einschalten

an. Ein Herunterstufen des Forest- und dann auch des Domänenmodus funktioniert ebenso mit "Windows2008Domain" und "Windows2008Forest" (auf niedrigere Modi wird das Herunterstufen nicht unterstützt). Nun schalten Sie den Active Directory-Papierkorb über

```
Enable-ADOptionalFeature 'Recycle
  Bin Feature' -Scope ForestOrConfi-
  gurationSet -Target 'firma.de'
  -server FIR-DC01
```

ein. Mit dem folgenden Befehl lassen Sie sich eine Liste aller gelöschten Objekte (hier mit dem Vornamen "Ulf") anzeigen:

```
Get-ADObject -filter 'givenname
  -eq "Ulf"' -includeDeletedObjects
```

Diese Benutzer stellen Sie einfach wieder her, indem Sie die Liste an das Cmdlet "restore-ADObject" weiterleiten:

```
Get-ADObject -filter 'givenname
  -eq "Ulf"' -includeDeletedObjects
  | restore-ADObject
```

Hierbei müssen Sie beachten, dass die OU, in der das Benutzerkonto Mitglied war, existieren muss, ansonsten geben Sie mit dem Parameter "-TargetPath" eine neue OU an.

Fazit

Nach wie vor gibt es den Autoritativen Restore, den Sie anwenden sollten, wenn große Inhalte des Active Directory gelöscht wurden und der AD-Papierkorb noch nicht zur Verfügung steht. Auch wenn Objekte nicht gelöscht wurden, sondern auf einen alten Stand gebracht werden müssen, wenn Rücksicherungen der Configuration-Partition notwendig sind oder Objekte zum Zeitpunkt des Löschens schon nicht mehr brauchbar waren, können Sie den Papierkorb nicht nutzen. Mit den Momentaufnahmen (Snapshots) im Active Directory hat der Administrator endlich die Möglichkeit, mehrere Stände seines Verzeichnisdienstes zu unterschiedlichsten Zeiten festzuhalten und diese bei Bedarf einzusehen. Skripte erlauben zudem, einzelne Objekte (oder auch einzelne Werte) des Active Directory wiederherzustellen, ohne dass dazu eine Wiederherstellung eines Domänencontrollers und ein Autoritativer Restore notwendig ist. Mit den gelieferten Möglichkeiten lässt sich auch feststellen, welche der Datensicherungen für die Wiederherstellung verwendet werden soll.

Der Active Directory-Papierkorb ist ein sehr interessantes Feature, um Löschungen im Active Directory rückgängig zu machen. Es hilft jedoch nicht, wenn Sie auf ältere Versionen der Objekte oder Attribute zurück greifen wollen – in diesem Fall sind die Active Directory-Snapshots und etwas Skripting (ab Windows Server 2008) eine Lösung. Des Weiteren ersetzt der Papierkorb nicht die Datensicherung oder Vorbereitung auf Wiederherstellungsszenarien, da für Domänen- oder Gesamtstrukturwiederherstellungen eine Datensicherung benötigt wird. In Kombination mit der Datensicherung und eventuell Snapshots ist der Papierkorb aber eine sehr umfassend und überlegt konzipierte Funktion, die dem Administrator im Fall der Fälle sehr viel Arbeit erspart und in den häufigsten Situationen ausreichend sein dürfte. *(jp)*

Tipps zum AD-Papierkorb

Microsoft unterstützt mit Windows Server 2008 R2 kein Wiederbeleben von Tombstones mehr, wie es bisher der Fall war. Auch Autoritative Restores sind nicht gerne gesehen, da diese – zumeist nicht im Detail bekannte – Schwierigkeiten mit sich bringen. Sobald alle DCs unter Windows Server 2008 R2 laufen und der Papierkorb eingeschaltet ist, lassen sich neu gelöschte Objekte einfach wieder herstellen. Eine Versionierung ist mit diesem Feature nicht möglich – ein Objekt wird genau in dem Zustand wieder hergestellt, in dem es gelöscht wurde.

Stellen Sie ein Objekt über den Papierkorb wieder her, muss entweder das ursprüngliche übergeordnete Objekt (normalerweise cn=Users oder eine OU) vorhanden sein oder Sie wählen ein neues übergeordnetes Objekt. Eine gesamte Struktur lässt sich nur über zusätzliche Skripte wiederherstellen.

Neben diesem Feature können Sie seit Windows Server 2008 (auch ohne R2 möglich) auch Objekte vor versehentlichem Löschen schützen. Dies erledigt das System bei neuen OUs (mit der neuen Version der Managementkonsole) automatisch, bei bisherigen sollten Sie dies einschalten.

Links

[1] Wiederherstellen gelöschter Benutzerkonten und ihrer Gruppenmitgliedschaften in Active Directory
http://support.microsoft.com/kb/840001/

[2] ADRestore auf Microsoft/Sysinternals
http://technet.microsoft.com/en-us/sysinternals/bb963906.aspx

[3] Active Directory Recycle-Bin im Windows Server 2008 R2 TechCenter
http://technet.microsoft.com/en-us/library/dd391916(WS.10).aspx

[4] Active Directory Powershell-Blog
http://blogs.msdn.com/adpowershell/

AD anhalten dank Directory Services Restore Mode

Stop and Go im Verzeichnisdienst

Das Active Directory wie einen Dienst vorübergehend anhalten zu können – diese Forderung wurde in den zehn Jahre seit Erscheinen des Verzeichnisdienstes an die Microsoft-Produktgruppe wiederholt laut. So ist ein aktiver Verzeichnisdienst mitunter hinderlich bei der Administration. Mit Windows Server 2008 hat Microsoft diese Forderung nun endlich erfüllt. Was es mit dem "Directory Services Restore Mode" auf sich hat und welche Möglichkeiten es gibt, den Wiederherstellungsmodus sinnvoll zu verwalten, zeigen wir Ihnen in diesem Workshop.

Quelle: Fotomenne - Fotolia.com

Der Directory Services Restore Mode lässt das Active Directory bei Bedarf deaktiviert

Bei jedem Start eines Domänencontrollers (DC) fahren automatisch die Active Directory-Domänendienste und die zugehörigen Komponenten wie DNS und Kerberos mit hoch, um ohne Admin-Interaktion die kritischen Domänenaufgaben ausführen zu können. Damit läuft das Active Directory (AD) stets im Hintergrund, so dass im Domänencontrollerbetrieb fortwährend ein lesender und schreibender Zugriff auf die AD-Datenbank durchgeführt wird. Bei der Verwaltung des AD existieren jedoch Fälle, in denen eine aktive Datenbank hinderlich ist und für die ein Offlinemodus benötigt wird. Ein Beispiel hierfür ist das Zurückspielen von Sicherungen einschließlich des Systemstatus, bei dem die Verzeichnisdatenbank offline in einem konsistenten Zustand überschrieben werden muss. Für solche Offlinefälle gibt es den "Verzeichnisdienstwiederherstellungsmodus" oder "Directory Services Restore Mode", kurz DSRM. Der DSRM ist eine besondere Windows-Startoption, die Sie über das Bootmenü beim Rechnerstart mittels F8 auswählen. Windows startet daraufhin seine Dienste, ohne das AD und seine verwandten Komponenten zu laden.

Für die Anmeldung am Offline-Domänencontroller ohne aktives AD dient der "DSRM-Administrator", dessen Passwort Sie beim Heraufstufen des Domänencontrollers mit dem DCPromo-Assistenten festlegen. Dieser Account ist in der lokalen Benutzerdatenbank SAM gespeichert, und nicht wie alle AD-Konten in der Verzeichnisdatenbank. Er ist der bei Mitgliedsservern bekannte lokale Administrator, nur dass er auf einem Domänencontroller nur im speziellen Fall des DSRM zur Verfügung steht. Nach erfolgreicher Anmeldung steht der Domänencontroller zur Verfügung – allerdings nur ohne laufende AD-Instanz, so dass sich Wartungsarbeiten oder Wiederherstellungen zum Beispiel ganz einfach mit dem NTDSUtil-Werkzeug durchführen lassen.

Stop and Go

Für Änderungen auf Datenbankebene des Verzeichnisses war stets ein Neustart im Verzeichnisdienstmodus notwendig. Immer dann, wenn an der Datenbank und ihrer Konfiguration Hand angelegt werden sollte, musste der DC im Wiederherstellungsmodus per F8 (oder Bootmanageroption) neu gestartet werden – das bedeutete zwangsläufig Downtime für den betreffenden DC. Microsoft hat sich dieses Problems angenommen und das Active Directory mit Windows Server 2008 zu einem Dienst gewandelt. Dieser AD-Dienst startet per unveränderbarer Konfiguration automatisch beim Rechnerstart, kann aber im laufenden Betrieb gestoppt werden. Wie andere Dienste auch, stoppen und starten Sie den Verzeichnisdienst mit den folgenden Befehlen:

```
net stop NTDS
net start NTDS
```

Natürlich geht dies auch über die normale Diensteverwaltung. Mit dem Starten und Stoppen von AD DS werden weitere, AD-abhängige Dienste angehalten und neu gestartet: die Dateireplikationen mittels FRS und DFS, der Kerberos-Schlüsseldienst für die AD-Authentifizierung, DNS im AD-integrierten Modus und der Intersite Messanging-Dienst.

Bei gestopptem Active Directory lassen sich zahlreiche Verwaltungsaufgaben erledigen. So ist etwa die Defragmentie-

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator>net stop ntds
Die folgenden Dienste hängen vom Dienst Active Directory-Domänendienste ab.
Das Beenden des Dienstes Active Directory-Domänendienste beendet auch diese Dienste.

   Kerberos-Schlüsselverteilungscenter
   Standortübergreifender Messagingdienst
   DNS-Server
   DFS-Replikation

Möchten Sie diesen Vorgang fortsetzen? (J/N) [N]: J
.
Kerberos-Schlüsselverteilungscenter wurde erfolgreich beendet.

Standortübergreifender Messagingdienst wird beendet.
Standortübergreifender Messagingdienst wurde erfolgreich beendet.

DNS-Server wird beendet.
DNS-Server wurde erfolgreich beendet.


DFS-Replikation wurde erfolgreich beendet.

Active Directory-Domänendienste wird beendet.
Active Directory-Domänendienste wurde erfolgreich beendet.


C:\Users\Administrator>_
```

Bild 1: Da Abhängigkeiten zwischen den benötigten AD-Diensten existieren, fährt ein Domänencontroller mehrere Dienste beim AD-Stopp herunter

rung und Prüfung der Verzeichnisdatenbank auf Integrität im gestoppten Dienstmodus möglich. Ebenso können Sie die Logdaten und die Datenbank selbst verschieben. Das Verschieben der Datenbank geschieht mittels NTDSUtil im Kontext "files" über *move DB to D:\NTDS*, um im "File maintenance"-Kontext von NTDSUtil die Datenbank von ihrem Ursprungspfad nach *D:\NTDS* zu verschieben. Anschließend rät das System, eine Sicherung der Datenbank zu erstellen, da es beim Zurückspielen von Backups mit altem DB-Pfad Probleme geben kann. Mit der Datenbank sollten auch die Logfiles verschoben werden, um alle AD-Daten auf ein neues Laufwerk umzuziehen: *move logs to D:\NTDS*.

Das Komprimieren der Datenbank ist auch im gestoppten Modus möglich. Einige Unternehmen führen eine regelmäßige Offline-Defragmentierung durch – teils unnötigerweise. Diese hatten es bisher schwer, diese Aufgabe per Skript zu steuern, war doch ein Reboot in den Verzeichnisdienstwiederherstellungsmodus, Anmeldung mit DSRM-Admin, Starten der Defragmentierung, Ersetzen der Dateien und Neustart als Domänencontroller notwendig. Mit der Möglichkeit, diese Aufgabe bei gestopptem Verzeichnisdienst zu erledigen, geht all dies jetzt deutlich einfacher per Skript. Aber warum überhaupt Defragmentieren? Das AD löscht Datenbankseiten nicht einfach und gibt den Speicherplatz wieder frei – es markiert die Seiten als "frei" und verwendet sie zu einem späteren Zeitpunkt wieder, um neue Daten darauf zu schreiben. Eine Verzeichnisdatenbank wird also von allein niemals schrumpfen. Um Platz zu gewinnen, kann sie komprimiert werden und somit von "Whitespaces", den leeren Bereichen, befreit werden – erneut mit NTDSUtil im Kontext "file maintenance" lautet der Befehl *compact to D:\NTDS\compact*. Der Pfad im Befehl gibt an, wohin NTDSUtil die neue Datenbankdatei erstellen soll und darf nicht dem aktuellen Standort der AD-Datenbank entsprechen. In der Tat erstellen Sie so eine neue AD-Datenbankdatei, da alle belegten und verwendeten Datenbankseiten, ohne die unbenutzten Whitespaces, in eine neue Datei geschrieben werden. Diese neu erstellte Datenbankdatei können Sie anschließend über die bisherige Datenbank kopieren. NTDSUtil empfiehlt nebst der Erfolgsmeldung, alte Logdateien im Verzeichnis der aktuellen Datenbank zu löschen und liefert gleich den passenden Befehl mit.

Im Anschluss an die Defragmentierung sollte die Datenbank auf ihre Konsistenz und Integrität geprüft werden. Innerhalb der AD-Datenbank existieren viele Verknüpfungen und Verweise unter den Objekten. Der simple Befehl *Integrity* startet die Integritätsprüfung. Weiterhin nicht möglich und auch nicht von Microsoft unterstützt sind Wiederherstellungen, solange Windows nicht im DSRM gestartet wurde. Rücksicherungen werden hier nicht unterstützt, da das Active Directory Daten aus der Datenbank für den schnelleren Zugriff im Cache hält und benötigte Dienste wie die lokale Sicherheitsauthorität (LSASS) im Nicht-DSRM-Zustand zu korrupten Daten und falschem Cacheverhalten führen könnten. Für Wiederherstellungen aus Backups ist es weiterhin notwendig, einen DC im Wiederherstellungsmodus zu starten. Was jedoch unterstützt wird – wenn auch nur ohne einen eingeschalteten Recycle-Bin bei R2 – ist der autoritative Teil einer Wiederherstellung.

Die Datenbank darf nicht bei gestopptem AD überschrieben werden, sollte dies aus Versehen passieren ist es unbedingt notwendig, den DC unmittelbar danach neu

```
Administrator: Eingabeaufforderung - ntdsutil
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Aktive Instanz wurde auf "ntds" festgelegt.
ntdsutil: files
file maintenance: compact to C:\Windows\NTDS_compact
Defragmentierungsmodus wird initialisiert...
     Quelldatenbank: E:\NTDS\ntds.dit
     Zieldatenbank: C:\Windows\NTDS_compact\ntds.dit

                    Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ....................................................

Es empfiehlt sich, umgehend eine Sicherung dieser Datenbank
vorzunehmen. Durch Wiederherstellen einer Sicherung, die vor der
Defragmentierung erstellt wurde, wird die Datenbank wieder in den Zustand versetzt,
in den sie sich zum Zeitpunkt der Sicherung befand.

Die Komprimierung war erfolgreich. Sie müssen:
   "C:\Windows\NTDS_compact\ntds.dit" "E:\NTDS\ntds.dit" kopieren
und die folgenden Protokolldateien löschen:
   del E:\NTDS\*.log

file maintenance: _
```

Bild 2: NTDSUtil zeigt den Verlauf der Datenbank-Defragmentierung an und weist Administratoren auf weitere Schritte hin

zu aktivieren, ohne zuvor den Verzeichnisdienst per *net start NTDS* zu starten, damit alle Daten aus dem Cache gelöscht werden. Wenn jedoch ein Objekt in einem Standort gelöscht wurde und an einem anderen Standort noch existiert, so kann das AD in diesem entfernten Standort sofort gestoppt werden und auf diesem DC dann per NTDSUtil im Autoritativen Restore das Objekt als "Neuer" markiert werden. Da die Datenbank hierfür nicht von einer Sicherung überschrieben wurde, kann das AD hinterher sofort wieder gestartet werden und die "Löschung" des Objektes wird rückgängig gemacht.

AD-Defragmentierung – sinnvoll oder nicht?

Experten streiten sich darüber, ob die AD-Defragmentierung wirklich Vorteile bietet oder nicht. Die Defragmentierung selbst sorgt dafür, dass die Datenbank von leeren Datenbankseiten befreit wird und erzeugt eine neue komplett neue Datenbankdatei *NTDS.DIT*. Diese muss nach der Defragmentierung von Hand in das entsprechende NTDS-Verzeichnis kopiert werden und die ursprüngliche Datenbankdatei ersetzen. Es folgt eine empfohlene Prüfung der Semantiken und Integrität.

Sogenannte Whitespaces in der AD-Datenbank sind nicht "verloren", da das System sie bei der Erstellung neuer Objekte überschreibt und selbstständig für neue Daten nutzt. So kann es vorkommen, dass eine Datenbank nach einer umfangreichen Objektlöschung für einige Zeit ihre Größe nicht verändert. Mit dem Registrierungsschlüssel "HKLM\ SYSTEM\ CurrentControlSet\ Services\ NTDS\ Diagnostics" –"6 Garbage Collection" und dem Erhöhen des Wertes von 0 auf 1 schreibt der Domänencontroller zweimal täglich während der Garbage Collection Statistiken in sein Eventlog. Eine Meldung mit der EventID 1646 zeigt, wie viel Speicherplatz die Datenbank gerade belegt und wie viel Whitespace sie beinhaltet. Dies gibt einen guten Überblick darüber, wie viel potentiellen Speicherplatz durch die Defragmentierung zu Erwarten ist. In der Regel rechnet sich jedoch der Einsatz dieser Defragmentierungsmechanismen nicht, da keine Performancesteigerung eines DCs zu erwarten ist – die Defragmentierung ist eine reine Komprimierung der Datenbank. Die AD-Datenbank ist so aufgebaut, dass sie selbst mit größten Datenmengen effizient arbeiten kann – auch mit Whitespaces.

Durchgeführt werden sollte eine Defragmentierung auf alle Fälle, wenn ein Domänencontroller "In-Place" auf ein neues Betriebssystem aktualisiert wurde. Hier müssen Bereinigungen im AD durchgeführt werden, wie den "Single Instance Store" für Berechtigungen, die nur durch die Datenbank-Defragmentierung gemacht werden.

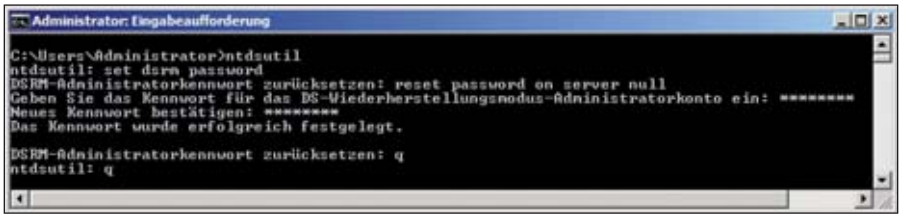


Bild 3: Eine Möglichkeit, das DSRM-Passwort zu ändern, besteht über das Kommandozeilentool NTDSUtil

Das DSRM-Passwort ändern

Ist das DSRM-Passwort verloren oder nicht mehr auffindbar, kann es seit Windows Server 2003 über NTDSUtil im laufenden DC-Betrieb geändert werden. Nach dem Aufruf von NTDSUtil wartet das Werkzeug auf Kommandos. Das korrekte Stichwort lautet *set dsrm password*, gefolgt von der Zeile *reset password on server null*. Der Wert "null" bedeutet hier, dass das Passwort auf dem lokalen DC geändert werden soll. Möchten Sie das DSRM-Passwort eines anderen DCs ändern, findet dessen Servername stattdessen Verwendung: *reset password on server ITA-DC02*. Anschließend fordert das System die zweimalige Eingabe des neuen Passwortes ein.

Unter Windows 2000 war dies noch nicht möglich, daher hatte Microsoft mit dem SP4 im aktualisierten Ressourcekit seinerzeit das Tool *SetPwd.exe* mitgeliefert. Da sich in NTDSUtil das zweimalige Setzen des Passwortes nur schwer skripten lässt, haben sich einige Administratoren damit beholfen, das SetPwd-Tool zu verwenden, um mit einem kurzen Skript das Setzen des Passwortes auf allen DCs zu automatisieren. Mit Windows Server 2008 werden wir eine weitere Möglichkeit kennen lernen.

DSRM-Passworte synchronisieren

Das automatische Setzen des DSRM-Passwortes auf diese Weise ist nicht trivial. Für Windows Server 2008 hat sich Microsoft deshalb einen Trick einfallen lassen: Anstatt das Passwort vom Administrator per Eingabe einzufordern, lässt NTDSUtil nun die Einmal-Synchronisation eines Benutzerpasswortes aus dem Active Directory zu und übernimmt dieses für den DSRM-Adminaccount. Hierfür müssen Sie bei Windows Server 2008 ohne Servicepack den Hotfix aus dem Knowledgebase-Artikel 961320 einspielen – bei Windows Server 2008 SP2 oder Windows Server 2008 R2 ist die Möglichkeit bereits im Betriebssystem enthalten. Der Befehl hierfür lautet in NTDSUtil *set dsrm password* und anschließend *sync from domain account {account}*, wobei der Accountname für die Einmalsynchronisation angegeben werden muss. Das System synchronisiert daraufhin das DSRM-Passwort mit dem des angegebenen Benutzers. Der Benutzer muss dabei kein aktiver Benutzer sein, sondern kann deaktiviert in einer beliebigen OU, zusammen mit anderen Serviceaccounts, liegen.

Dieses Feature lässt es zu, die DSRM-Accounts über Skripte zu verteilen ohne dass

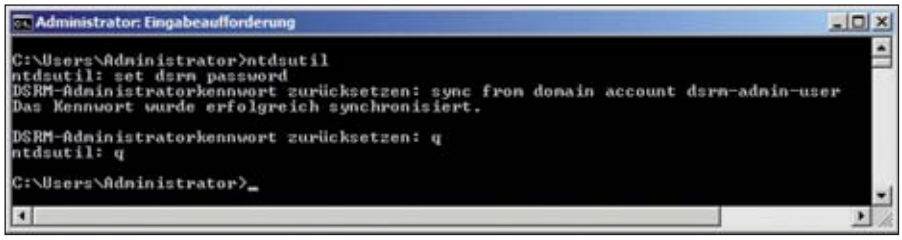


Bild 4: Automatisiert funktioniert ab Windows Server 2008 auch die Synchronisation des Passwortes eines Domänenaccounts

das Passwort sichtbar im Skript steht. Kombiniert mit dem Einsatz von Gruppenrichtlinien und geplanten Tasks kann das Passwort fast wie bei Gruppenrichtlinien regelmäßig synchronisiert werden. Zunächst wird ein entsprechendes Benutzerkonto für die Synchronisation erstellt. Ihm wird das DSRM-Administratorpasswort zugewiesen. Verschoben wird das neu erstellte Konto dann in eine eigene OU und anschließend deaktiviert, um Anmeldungen daran zu verhindern. Ist das Konto fertig, folgt der Befehl für die Synchronisation. NTDSUtil kommt mit Batchaufrufen sehr gut zurecht, sodass der folgende Befehl die Arbeit erledigt:

```
NTDSUtil "set dsrm password" "sync
  from domain account dsrmAdminPas-
  sUser" q q
```

Der Batchaufruf könnte mit einem Computerstartskript auf Gruppenrichtlinienebene erfolgen – dieses würde aber nur bei DC-Neustarts ausgeführt werden, was in der Regel recht selten vorkommt. Ein geplanter Task, der die Passwortsynchronisation regelmäßig aufruft, ist die elegantere Variante. Hierbei geben Sie im Punkt "Aktion" das entsprechende Batch-Skript als Referenz an sowie als "Trigger" ein bestimmtes, regelmäßiges Ereignis. Da das Skript keine Last auf den DCs auslöst, spricht nichts gegen eine mehrmals tägliche oder tägliche Ausführung der Synchronisation. Sollen alle DCs dasselbe DSRM-Passwort erhalten, können Sie den geplanten Task mittels Gruppenrichtlinien und einer Verknüpfung an die "Domain Controllers"-OU verteilen. GP Preferences machen dies durch ihren Push-Mechanismus für "Geplante Aufgaben" sehr einfach. Die Änderung des DSRM-Passwortes für alle Domänencontroller der Domäne ist dann so einfach, wie dem Referenzkonto ein neues Passwort zuweisen – und dies sollte ohnehin zu den regelmäßigen Aufgaben der Domänenadministration gehören.

Booten in den DSRM

Gelegentlich kann es auch vorkommen, dass Sie die jüngste fehlerfreie Replikation einer Active Directory-Datenbank auf einem Domänencontroller haben, auf den kein unmittelbarer physikalischer Zugriff möglich ist. In diesen Fällen bietet sich die Remoteunterstützung an. Im Prinzip wird diese als Remote Desktop auf allen Servern aktiviert. Da jedoch für das Starten im "Verzeichnisdienst-Wiederherstellungsmodus" Tasten auf der Konsole während des Bootvorgangs gedrückt werden müssen, kann dies standardmäßig nicht aus der Ferne geschehen. Daher haben Sie die Möglichkeit, die Bootoptionen entsprechend zu modifizieren. Seit Windows Server 2008 und höher muss hierzu wie folgt vorgegangen werden: Zunächst erstellen Sie einen neuen Boot-Eintrag – etwa indem Sie den aktuellen, standardmäßigen kopieren:

```
bcdedit /copy {current} /d
  "Directory Services Restore Mode"
```

In der Ausgabe des Befehls erscheint eine GUID, die Sie kopieren müssen, um anschließend den Booteintrag entsprechend anzupassen:

```
bcdedit /set {GUID} safeboot
  dsrepair
```

In einem Fehlerfall können Sie jetzt wie folgt auf den Server zugreifen:

1. Auf den Server per Remote Desktop verbinden
2. In den Systemeigenschaften in der Registerkarte "Erweitert" unter dem Schalter "Starten und Wiederherstellen" unter Standardbetriebsystem die Option "Directory Repair Mode" auswählen
3. Dialogboxen mit "OK" schließen, dann den Server neu starten. Achten Sie darauf, dass der Punkt "Neu Starten" gewählt ist, nicht "Herunterfahren".
4. Mittels Pings können Sie nun über-

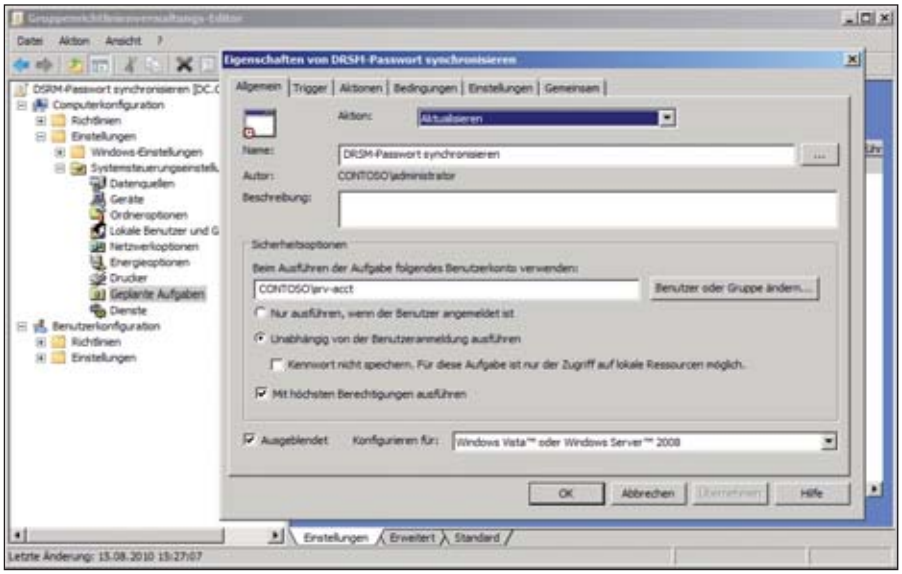


Bild 5: Erhalten alle DCs ein gemeinsames DSRM-Passwort, können Gruppenrichtlinien für die Erstellung des geplanten Tasks eingesetzt werden

prüfen, wann der Rechner wieder online ist.

5. Nun verbinden Sie sich erneut mittels Remote-Desktop-Verbindung auf den Server.

Sie befinden sich jetzt remote auf dem Rechner im "Verzeichnisdienst-Wiederherstellungsmodus". Nun können Sie alle notwendigen Aktionen zum Beispiel für eine authoritative Wiederherstellung der Datenbank vornehmen. Sind Sie mit den Aktionen fertig, beschreiben Sie die Bootoptionen wieder wie vorher und stellen Sie diese auf den alten Default-Wert. Starten Sie abschließend den Server neu.

Anmelden im DSRM-Modus

Der DSRM-Admin ist per Vorgabe nur dazu in der Lage, Anmeldungen am lokalen Domänencontroller durchzuführen – und das auch nur, wenn der Domänencontroller im DSRM gestartet wurde. Bei laufendem AD oder an einem Client im Netzwerk kann er sich nicht anmelden, sondern nur im Offline-Zustand. Bei Umgebungen mit nur einem DC kann es daher zu Problemen kommen, wenn das AD denn einmal gestoppt wurde. Der DSRM-Admin dürfte sich hier auch nicht anmelden. Daher lässt sich dieses Vorgabeverhalten ebenfalls ab Windows Server 2008 ändern – der DSRM-Administrator kann sich dann an einem DC anmelden, der nicht im DSRM gestartet wurde. Um dieses Verhalten herbeizuführen, erstellen und passen Sie einfach den Registrierungsschlüssel "HKLM \ System \ CurrentControlSet \ Control \ Lsa \ DSRMAdminLogonBehavior" an, der im Normalzustand nicht existiert. Der Schlüssel kennt drei Zustände: Versehen mit dem Wert "0", was dem Standardzustand entspricht, lässt ein Domänencontroller keine Anmeldungen des DSRM außer im Verzeichnisdienstwiederherstellungsmodus zu. Mit dem Wert "1" darf sich ein DSRM-Admin anmelden, wenn das AD manuell gestoppt wurde, auch wenn sich der DC nicht im Wiederherstellungsmodus befindet und mit dem Wert "2" ist es dem DSRM-Admin gestattet, sich jederzeit anzumelden – egal in welchem Zustand sich der DC und das Active Directory gerade befinden.

Administratoren sollten sich dieser Einstellungsmöglichkeit bewusst sein, da DSRM-Administratoren lokale Administratoren auf Domänencontrollern sind und auch im "Online-Modus" Vollzugriff auf einen DC und das Active Directory besitzen. Da sich der Registrierungsschlüssel auch im DSRM erfolgreich ändern lässt, sollten nur Mitarbeiter das DSRM-Passwort kennen, die ohnehin Domänen-Admins sind und als solche agieren. Keinesfalls sollten Supportmitarbeiter, die sonst keine Berechtigungen im AD besitzen, das DSRM-Administratorpasswort kennen. Denn mit erfolgreicher Änderung des Registrierungsschlüssels sind DSRM-Admins in der Lage, die volle Kontrolle des AD im laufenden Betrieb zu übernehmen. Zusätzlich sei erwähnt, dass der DSRM-Account bereits seit Windows 2000 die Berechtigungen des lokalen Administrators besitzt (defakto ist er der lokale Administrator) und seither wichtige Berechtigungen im Betriebssystem genießt. Auch wenn die Möglichkeiten der Nutzung eingeschränkt waren, der DSRM-Administratoraccount gehörte und gehört nur in die Hände von geschultem Personal.

Fazit

Den Verzeichnisdienst zu stoppen, kann manche administrative Arbeit erleichtern, ist aber nicht für alle Aufgaben ausreichend. Das Konto für die Verzeichnisdienstwiederherstellungsmodus-Anmeldung muss trotzdem verwaltet werden, und kann auch dazu dienen sich auf einem DC mit gestopptem Verzeichnisdienst anzumelden, wenn dies entsprechend eingerichtet wurde. Der Wiederherstellungsmodus kann auch über Remote Desktop verwendet werden, und diese Option sollte für die Notfallhandlung bei einer versehentlichen Löschung vorgesehen werden – zumindest, bis der Recycle-Bin mit Windows Server 2008 R2 im Unternehmen eingeschaltet ist. *(dr)*


Quelle: pmphoto - Fotolia.com

Windows Backup

Datensicherung auf neuen Wegen

"Never change a running system" – das ist unter Systemverwaltern ein sehr bekanntes Mantra. Admins aus aller Welt sprechen diese Formel, wenn es um Änderungen oder Anpassungen funktionierender Systeme geht, die sie eigentlich nicht anfassen möchten. Neben Neuinstallationen, Konfigurationsänderungen und Updates in Form von Patches oder Produktaktualisierungen versuchen Administratoren, ihre Systeme aber vor allem vor einer besonders gefürchteten Art von Modifikationen zu schützen: den ungewollten Änderungen.

Der Großteil der Windows-Administratoren wird schon einmal mit dem Windows-Bordmittel "NTBackup" Bekanntschaft gemacht haben, mit dem sie seit den frühen NT 3-Zeiten Datensicherungen und deren Wiederherstellung durchführen konnten. Bis Windows Server 2003 lieferte Microsoft NTBackup als Bestandteil des Betriebssystems mit, um Basisfunktionen zum Sichern des Systems zu bieten. NTBackup hat jedoch ausgedient – in Windows Server 2008 führte Microsoft einen Generationswechsel in seinem Backupsystem ein und verabschiedete NTBackup in den Ruhestand. Das Nachfolgemodell, "Windows Server Backup", wartet mit einigen Neuerungen und Einschränkungen auf, mit denen der Nutzer sich erst vertraut machen muss und die er vor allem bereits beim Serverdesign planen muss.

Microsoft wollte damit nicht nur alte Zöpfe abschneiden, sondern das Backupsystem von Windows grundlegend verändern. Die wohl einschneidenste Veränderung für NTBackup-Kenner dürfte die fehlende Bandunterstützung sein. Windows Server Backup speichert nicht auf Bänder – vielmehr sind nur Datenträger und Volumes sowie Netzwerkfreigaben und DVDs für Backups vorgesehen. WSB ist eine reine Disk-to-Disk und Disk-to-Optical-Lösung. Wer seine Datensicherungen weiterhin auf Band speichern will, muss ein Drittanbieterwerkzeug für das Kopieren der Sicherung auf das Band verwenden.

Sicherung in virtuellen Festplatten

Weiterhin änderte sich das genutzte Datensicherungsformat. Wo NTBackup zuvor das bekannte BKF-Format nutzte, schreibt WSB seine Sicherungen in virtuelle Festplatten im VHD-Format. Hierfür speichert das System Daten nicht mehr dateiweise, sondern Block für Block von der Festplatte in die Ziel-VHD. Hilfreich hierbei ist der Schattenkopiedienst (Volume Shadow Copy Service, VSS) in Windows, der von Quell- und Zieldatenträger Snapshots erstellen kann und, wiederum auf Blockebene, Differenzen zwischen aktuellen Daten und vorher erstellten Sicherungen herausstellen kann. Unterscheiden sich Daten zwischen Quelle und Ziel, werden nur veränderte Blöcke anstelle ganzer Datei weggesichert – unveränderte Blöcke können übersprungen werden. Das spart Zeit und Platz auf dem Backupdatenträger. Trotzdem kennt WSB keine "inkrementellen" Sicherungen. Obwohl durch die Blocksicherung nur Deltas gespeichert werden müssen, können Sie zu jedem Backup mit einem einzigen Restore zurückkehren. Jede Datensicherung, auch wenn nur die Block-Deltas gesichert werden, kann als vollständige Sicherungen zurückgespielt werden, Sie müssen nicht wie bisher verschiedene Sicherungen nacheinander wieder einspielen.

Auch eine Kommandozeilenversion des Sicherungssystems bietet Microsoft an. NTBackup konnte per Kommandozeile angestoßen werden, teilweise aber etwas unkomfortabel, da eine Datei benötigt wurde, die die Sicherungsinhalte beschreibt. Das Kommandozeilen-Programm zu Windows Server Backup ist WBAdmin. Sie können WBAdmin dazu nutzen, um Backupjobs zeitgesteuert anzustoßen und Wiederherstellungen durchzuführen.

Ein Wermutstropfen bleibt jedoch: So können mit NTBackup gesicherte Daten nicht mit Windows Server Backup zurückgespielt werden. Microsoft liefert in

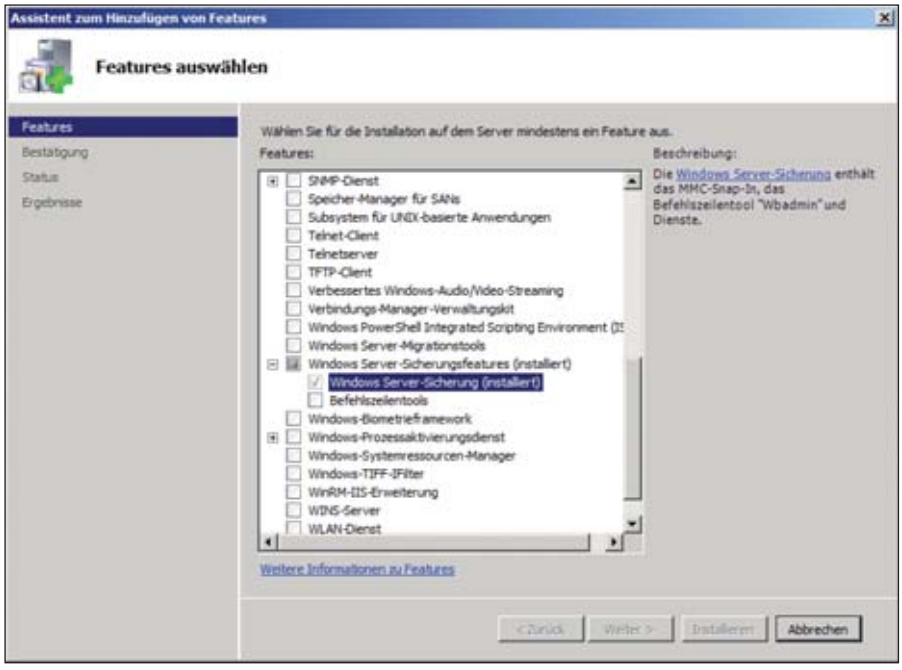


Bild 1: Die Windows Server-Sicherungsfeatures werden für die Backuperstellung benötigt. Befehlszeitentools sind optional.

der Grundinstallation kein Werkzeug hierfür. Möchten Sie dennoch Dateien aus einem NTBackup zurücklesen, können Sie sich unter [1] eine "Restore"-Version von NTBackup für Windows Server 2008 und Windows Vista herunterladen, die BKF-Backups lesen und wiederherstellen kann. Sicherungen sind damit allerdings nicht möglich.

Windows Server Backup installieren

Eine weitere Besonderheit von Windows Backup ist, dass das Sicherungssystem nicht direkt mit Windows installiert wird. Die Sicherung ist ein "Feature" und wird somit über den gleichnamigen Knoten im Servermanager mit "Features hinzufügen" nachinstalliert. Das Feature "Windows Server-Sicherungsfeatures" kennt hierbei zwei Unterfunktionen: "Windows Server-Sicherung" und "Befehlszeilentools".

Die "Windows Server-Sicherung" beinhaltet alle für die Windows-Sicherung notwendigen Tools – das MMC-Snapin für Windows Server Backup sowie das Kommandozeilenprogramm WBAdmin. Wer weiterhin PowerShell-Unterstützung für die Sicherung benötigt, sollte die "Befehlszeilentools" zusätzlich installieren. Sie enthalten PowerShell-Cmdlets, die Sie für die Sicherungsverwaltung, deren Erstellung und Wiederherstellung nutzen können. Um die Komponenten per Skript zu aktivieren, fügen Sie das Feature per Kommandozeile hinzu. Der Befehl

```
start /w ocsetup WindowsServerBackup
```

weist das Komponentensetup-Programm an, die Backupkomponenten zu installieren. Natürlich lässt sich das Feature auch über die PowerShell installieren, hierzu geben Sie die folgendes Kommado ein:

```
Import-Module ServerManager
Add-WindowsFeature Backup
```

Mit dem Parameter "Backup" wird die Windows Server-Sicherung installiert, mit dem Parameter "Backup-Tools" die PowerShell Erweiterungen, und mit dem Parameter "Backup-Features" beides.

Den Systemstatus sichern

Noch von früheren Windows-Versionen ist der Systemstatus als die Sicherungsoption bekannt, die AD-Administratoren am häufigsten auswählten. In der Tat enthält die Systemstatussicherung alle für das Active Directory und dessen Betrieb notwendige Daten, um im Fall eines Crashs den Betriebszustand wiederherstellen zu können. Auch in Windows Server 2008 ist der Systemstatus als Backupoption möglich – wenn auch in deutlich umfangreicherer Form als bisher. Wo der Systemstatus in Prä-Windows Server 2008-Versionen, natürlich abhängig vom System und den installierten Komponenten, meist nur mehrere hundert MByte Platz verschlang, frisst das WSB-Systemstatusbackup über 6 GByte auf einem Standard-DC – deutlich mehr als zuvor. Die gesicherten Komponenten haben sich zwischen den Serverversionen nicht wesentlich verändert. Was den Größenunterschied ausmacht, sind die Dateien des Betriebssystems, die schon in der Grundinstallation deutlich umfangreicher ausfallen. Nichtsdestotrotz besteht das Systemstatusbackup weiterhin aus den folgenden Komponenten:

- Windows Registrierung
- Systemdateien und Dateien, die dem Windows-Dateischutz unterliegen
- COM+ Klassenregistrierungsdatenbank
- Die Startdateien und die zugehörigen Systemdaten
- Die Zertifikatsdatenbank (falls es sich um einen Zertifikatsserver handelt)
- Die Active Directory-Datenbank (falls es sich um einen Domänencontroller handelt)
- Das SYSVOL-Verzeichnis (falls es sich um einen Domänencontroller handelt)
- Das IIS-Metaverzeichnis (falls IIS auf dem Server installiert ist)
- Clusterdienstinformationen (falls der Server Mitglied eines Clusters ist)

Das Systemstatus-Backup wird auf einfachste Art und Weise per Kommandozeile angestoßen. Für ein Backup auf das Volume e: verwenden Sie folgenden Befehl:

```
Wbadmin start systemstatebackup
  -backuptarget:e:
```

Das Systemstatus-Backup in Windows Server 2008 (nicht R2) ist an dieser Stel-

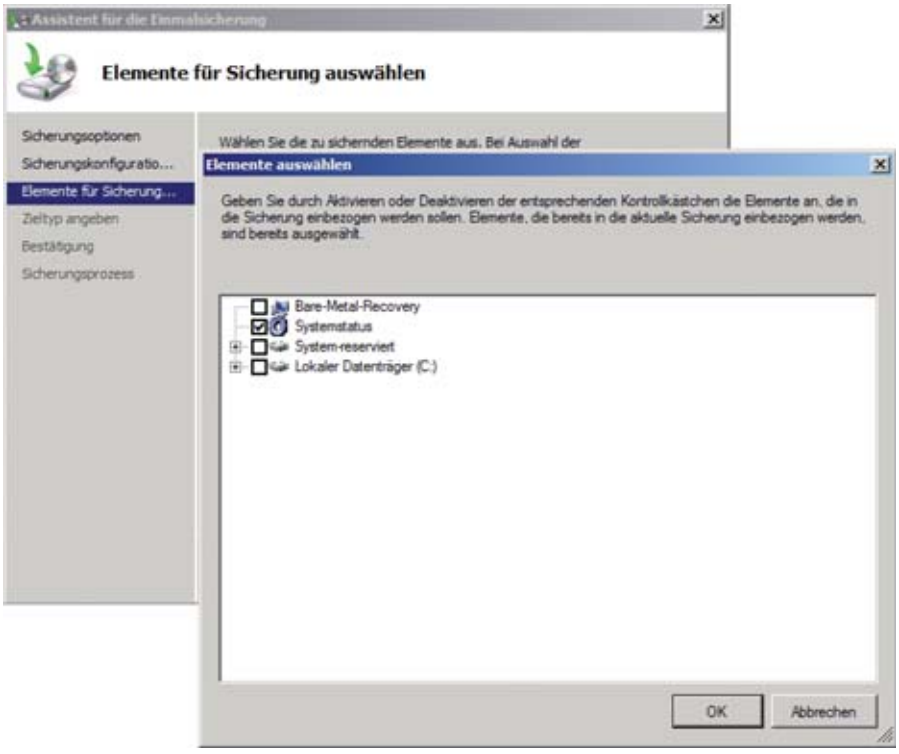


Bild 2: Erst mit R2 kann der Systemstatus auch in der Windows Server Backup-MMC gesichert werden

le eingeschränkt. Das Sicherungsziel muss zwingend auf einem lokalen Volume liegen und darf nicht, wie in Windows Server 2008 R2, ein Netzlaufwerk sein. Sollen die Backupdaten dennoch auf einen zentralen Server kopiert werden, müssen Sie einen manuellen Backup-Job einrichten, der die gesicherten Daten anschließend auf den Server kopiert. In R2 sind Netzlaufwerke für Systemstatus-Sicherungen erlaubt:

```
wbadmin start systemstatebackup
  -backuptarget:\\big-storage\backups
```

Des Weiteren steht der Systemstatus erst in Windows Server 2008 R2 in der Windows Backup Verwaltungskonsole zur Verfügung – die Erstfassung unterstützt diese Sicherung nur per WBAdmin über die Kommandozeile. Ein Umstand, der sich leicht verschmerzen lässt, wollte Microsoft doch für sein neues Windows keine separate Systemstatus-Option mehr anbieten. Die Kommandozeilen-Option wurde während der Beta-Phase durch Kundenfeedback nachträglich zum Verkaufsstart eingepflegt. Dies ist auch der Grund, weshalb Active Directory-Snapshots entwickelt wurden – die Active Directory-Gruppe musste sich damit auseinandersetzen, dass es gegebenenfalls keine Systemstatussicherung mehr geben würde.

Finden lässt sich die Systemstatus-Sicherung über die Option "Einmalsicherung" aus dem Aktionen-Menü, die den Einmalsicherungs-Assistenten anstößt, der Sie durch die Sicherungsoptionen führt. Per "Unterschiedliche Optionen" und "Benutzerdefinierte Optionen" im folgenden Schritt wählen Sie in "Elemente für Sicherung auswählen" die zu sichernden Komponenten aus. Eine gewünschte Option, neben dem "Bare-Metal-Recovery" und den einzelnen Volumes des Rechners, ist der Systemstatus. Der folgende Schritt erlaubt in der R2-MMC auch die Auswahl eines Netzlaufwerkes als Speicherort für die Sicherung.

Geht der Speicherplatz auf dem Ziellaufwerk langsam zuneige, hilft der "Delete"-Befehl in *wbadmin*, das älteste, verfügbare Backup zu entfernen und für verfügbaren Speicherplatz zu sorgen:

```
wbadmin delete systemstatebackup
  -backupTarget:e: -deleteOldest
```

Serversicherungen durchführen

Bei Systemausfällen oder Ausfällen der Hardware bietet sich oft die "Bare-Metal-Sicherung" an, die das vollständige Windows-System mit allen zugehörigen Daten von Grund auf einspielt. Die Bare-Metal-Sicherung sichert alle Volumes eines Systems, die für den Windows-Betrieb notwendige Daten enthalten. Dies kann unter Umständen mehrere Volumes umfassen, beispielsweise wenn mehrere Datenträger für Auslagerungsdateien ausgewählt wurden. Der Unterschied zum "vollständigen" Backup besteht darin, dass im vollständigen Backup alle Volumes und alle Daten gesichert werden, die sich auf dem Server befinden – auch Volumes, die keine systemkritischen Daten enthalten. Mit der Bare-Metal-Sicherung lässt sich Windows in Problemsituationen komplett wiederherstellen. Hierzu starten Sie die Wiederherstellung von der Installations-DVD (oder einer Kopie auf einem USB-Stick) und wählen im Installationsmenü den Menüpunkt "Komplettwiederherstellung". Bei der Wiederherstellung muss es sich nicht um die gleiche oder eine baugleiche Maschine handeln – Bare-Metal-Backups können auf anderen Maschinen wiederhergestellt werden.

Ein Bare-Metal-Backup stoßen Sie mit dem Befehl

```
wbadmin start backup -allcritical
  -backuptarget:e:
```

an. Der Schalter "-allcritical" weist WBAdmin an, die für eine Wiederherstellung notwendigen Volumes wegzusichern. Die Volumes werden ihrer Reihenfolge nach einzeln per VSS gesichert, sofern sich das Ziel auf einer lokalen Festplatte befindet.

In der Backupkonsole ist das Bare-Metal-Backup analog zum Systemstatus angeordnet und wird in "Benutzerdefinierte Optionen" und "Elemente für Sicherung auswählen" angewählt. Interessant hierbei

ist, dass der Assistent mehrere andere Optionen aktiviert, falls Sie das Bare-Metal-Backup auswählen. Zusätzlich wird die "Systemstatus"-Option gewählt, was bedeutet, dass Sie auch von einem Bare-Metal-Backup den Systemstatus zurückspielen können oder eine "Install-From-Media"-Installation von Active Directory möglich ist.

Neben der "allcritical"-Sicherungsvariante besteht die von Windows Vista und auch Windows 7 bekannte Methode der Komplettsicherung. Im Assistentenschritt "Sicherungskonfiguration auswählen" entspricht dies der Option "Vollständig (empfohlen)", die alle Daten des Servers inklusive Anwendungsdaten und nicht nur die systemkritischen Volumes sichert. Die vollständige Sicherung beinhaltet somit alle Daten eines Bare-Metal-Backups und folglich auch alle Daten des Systemstatus. Das "vollständige" Backup entspricht dem Kommandozeilenkommando für die Backuperstellung, in dem alle im System vorkommenden Volumes enthalten sind, etwa:

```
Wbadmin start backup
  -include:c:,d:,e: -backuptar-
  get:\\backupsrv\vollbackup
```

Allcritical oder Systemstatus

Wie bereits beschrieben, existieren diese beiden Backupmethoden und sichern unterschiedliche Daten, wobei der Systemstatus im Bare-Metal-Backup enthalten ist. Nüchtern betrachtet scheint für Sicherungen des Verzeichnisdienstes oder bei Serverszenarien, in denen kein Vollbackup gewünscht ist, der Systemstatus ausreichend zu sein. Nicht in allen Lebenslagen ist jedoch der Systemstatus die beste Variante – denn die beiden Methoden unterscheiden sich auch in der Art, in der die gesicherten Daten hinterlegt und bei erneuten Backups abgerufen werden.

Das "allcritical"-Backup verwendet nämlich den Volume Shadow Copy Service-Provider für die Erstellung seiner Backups. Vor der Speicherung werden die zu sichernden Daten per VSS-Snapshot analysiert. Aus dem Snapshot heraus kann Windows Backup dann erkennen, welche Blöcke der Quelle sich verändert haben oder auf dem Ziel nicht existieren und kann diese auf das Zielvolume schreiben. Existieren bereits vollständige Backups auf dem Ziel, kann Windows Backup effizienter bei der Sicherung vorgehen: Das System sichert nicht alle betroffenen Volumes erneut, sondern vergleicht, ebenfalls blockweise, wo Änderungen zwischen Quelle und dem letzten Backup auf dem Ziel entstanden sind. WSB erstellt dazu sowohl von Quelle als auch Ziel einen VSS-Snapshot und vergleicht diese. Das Delta zwischen den beiden Datensätzen sichert das System anschließend blockweise als neues Backup.

Diese Methode ist sehr interessant – denn nur das erste Backup ist wirklich so groß wie die zu sichernde Datenmenge. Alle folgenden Sicherungen enthalten nur Änderungen. Trotzdem darf dieses Verhalten nicht als inkrementelles Backup verstanden werden, denn bei der Wiederherstellung des Systems wird nur ein einziges Backup zurückgespielt. Das System erkennt, welche Daten aktuell sind und welche sich seit der ersten Sicherung nicht veränderten und kann daraufhin den zum Backup passenden, aktuellen Satz der Daten zurückspielen.

In Bild 3 sehen Sie, wie Windows Backup vorgeht. Nur während der ersten Sicherung (#1) werden alle Daten komplett gesichert, in weiteren Sicherungen werden jeweils nur Unterschiede auf Blockebene gespeichert (#2). Von Sicherung zu Sicherung übernimmt das System im Archiv die beibehaltenen Blöcke jeweils für das neueste Backup. Mit jeder Sicherung wächst das Gesamtarchiv – jedoch nur das letzte Backup ist so groß wie die Quelldaten – frühere Sicherungen enthalten nur die Blöcke, die sich vom neu erstellten Kindsbackup unterscheiden (#3 und #4).

Die logische Folge dieses effizienten Backupverfahrens ist, dass nur das erste Backup einer Bare-Metal-Sicherung wirklich groß ist – folgende Sicherungen dagegen kleiner und effizienter. Die Systemstatussicherung kann nicht von diesem Vorgehen profitieren, da der VSS-Dienst die darin enthaltenen Daten nicht blockweise wegschreiben kann. Für Systemstatusbackups werden stets alle Daten aufs Neue gesichert – ohne Deltaberücksichtigung. Verglichen mit der "allcritical"-Sicherung führt das System die erste Systemstatussicherung schneller und platzsparender aus, jede weitere Sicherung aber wird mit "allcritical" platzsparender und kürzer sein. Zudem kann ein Systemstatus-Backup nur für die Rettung des Systems verwen-

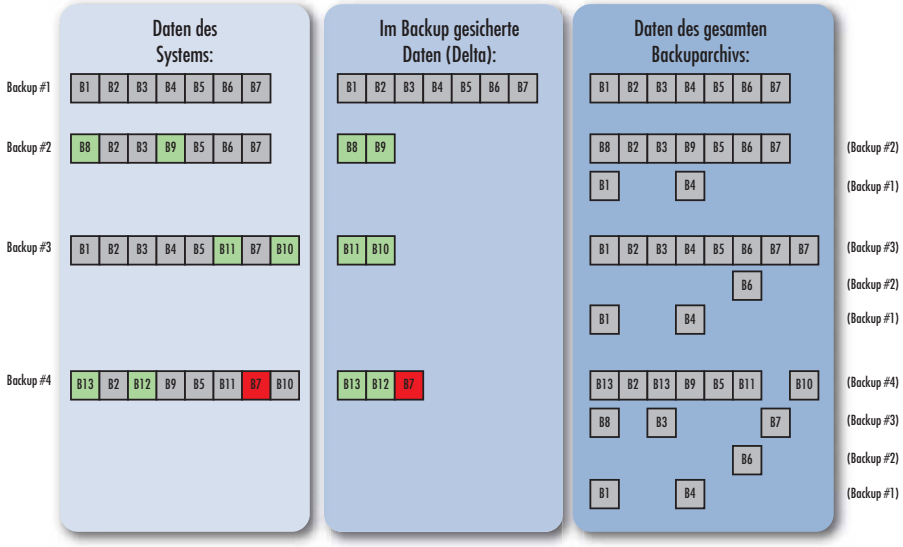


Bild 3: Wenn WSB mit dem Volume Shadow Copy Service sichern kann, können Backups platzeffizient und zeitsparend erstellt werden – ohne im Ernstfall mehrere inkrementelle Backups rücksichern zu müssen

det werden, wenn die Maschine neu aufgesetzt wurde und Rahmenbedingungen wie etwa gleicher Rechnername und gleiche Hardware gegeben sind – siehe dazu [2]. Technisch sind auch andere Konstellationen denkbar, Microsoft unterstützt jedoch nur diese Art der Wiederherstellung mit dem Systemstatus.

Doch Sie können, selbst wenn Sie nur den Systemstatus für Active Directory, SYSVOL oder IIS sichern möchten, trotzdem zur "allcritical"-Variante greifen. Gerade bei regelmäßigen Backups macht sich das VSS-basierende Backupverfahren von Windows Backup bezahlt. Funktionell lässt sich das "allcritical"-Backup überall dort einsetzen, wofür Sie sonst ein Systemstate-Backup verwenden – inklusive "Install-From-Media"-Installation des Active Directory. Wer vereinzelt Backups des Systemstatus erstellen muss oder den Zielorts des Backups ständig wechselt, kann guten Gewissens den Systemstatus gesondert sichern. Auf alle Fälle sollten Sie beide Versionen testen und vergleichen – je nach Konfiguration können die Unterschiede größer oder nahezu unbedeutend sein.

Dateien und Ordner sichern

Bislang haben wir beschrieben, wie Sie mit Hilfe von Windows Backup Volumes und den Systemstatus sichern und in Folge eines Problems zurückspielen. Manchmal sind es jedoch nicht ganze Volumes, die vor versehentlicher Löschung oder Problemen geschützt werden sollen, sondern einzelne Ordner und Dateien. Die Sicherung von Ordnern und Dateien wurde von Microsoft für Windows Server Backup zuerst nicht vorgesehen – die in Windows Server 2008 ausgelierte Version des Features beherrscht keine Backups auf Dateiebene. Erst mit R2 schafften die Redmonder die Option des Dateibackups – sowohl für WBAdmin als auch für die Oberfläche der MMC.

Mit WBAdmin nutzen Sie das Kommando *start backup* mit dem Schalter "-include". Ab R2 verarbeitet der Schalter eine kommaseparierte Liste von Dateien und Ordnern, die dann weggesichert werden:

```
Wbadmin start backup
  -include:C:\Users\Florian\Docu-
  ments,C:\Images\ -backuptarget:e:
```

Einzelne Verzeichnisse oder Dateien werden mit "-exclude" ausgeschlossen. Das folgende Kommando sichert alle Daten aus "C:\Users\Florian\Documents" und "C:\Images", überspringt jedoch die Unterverzeichnisse "vhds" und "Office":

```
Wbadmin start backup
  -include:C:\Users\Florian\
  Documents,C:\Images\
  -exclude:C:\Users\FlorianDocu-
  ments\vhds,C:\Images\Office
  -backuptarget:e:
```

In der WSB-MMC werden auch hier einzelne Dateien und Ordner über die bekannten Optionen "Benutzerdefiniert" und "Elemente hinzufügen" gewählt. Sie nutzen hier die Baumansicht und versehen gewünschte Objekte mit einem Haken. Wie gewohnt werden die Daten dann, nach entsprechender Auswahl, auf einem Netzlaufwerk oder einem lokal angeschlossenen Volume abgelegt.

Dateien und Ordner wiederherstellen

Das Wiederherstellen der Daten ist ebenfalls denkbar einfach: Auf dem Startbildschirm der Backup-Verwaltungskonsole wählen Sie den Punkt "Wiederherstellung" aus. WSB öffnet daraufhin den Wiederherstellungsassistenten, der Sie durch die Wiederherstellung führt. Im ersten Schritt will der Assistent wissen, wo die Sicherung gespeichert wurde, die zurückgespielt werden soll – ist es ein Netzlaufwerk oder eine DVD, ist die Option "eine an einem anderen Standort gespeicherte Sicherung" korrekt. Im Falle einer lokalen Sicherung wird die Option "Dieser Server" ausgewählt. Im nächsten Schritt des Assistenten wählen Sie das Backup aus. Mit dem Kalender-Applet können Sie zwischen Tagen und Monaten wechseln. Fett markiert sind die Tage, an denen ein Backup erstellt wurde. Existieren mehrere Backups eines Tages, zeigt das Dropdown-Menü zur Uhrzeit die möglichen Varianten des Backups an. Per Klick auf "Weiter" erscheint der Auswahlbildschirm der wiederherzustellenden Daten. Es werden nur Optionen eingeblendet, die das aktuell ausgewählte Backup unterstützt. Mit der Auswahl von "Dateien und Ordner" zeigt der folgende Assistentenschritt die im Backup verfügbaren Dateien und Ordner an.

Wählen Sie nun den Zweig der Baumstruktur, den Sie zurückspielen möchten. In "Wiederherstellungsoptionen angeben" befinden sich die aus NTBackup bekannten Optionen zum Restore. Soll das Backup an einen alternativen Ort zurückgespielt werden, wird dies hier konfiguriert. Auch das Verhalten des Systems, wenn Daten des Backups bereits auf dem Ziel existieren, legen Sie hier fest. Anschließend wird die Auswahl der Daten bestätigt und die Wiederherstellung durchgeführt.

Sicherungen planen

Sicherungen zu planen, war unter NTBackup nicht so einfach möglich. NTBackup besaß keine eingebaute Planfunktion für Backups, sondern musste per Batchjob geskriptet und dann über "Geplante Aufgaben" eingebaut werden. Windows Server Backup ist hier einen Schritt weiter: Es besteht weiterhin die Option, Backupskripte mit WBAdmin zu erstellen und auf diese Weise Jobs anzulegen. Microsoft hat Windows Server Backup zusätzlich einen eigenen Jobmechanismus spendiert.

Für die Jobplanung stehen alle Sicherungstypen zur Verfügung, die auch als Einzelbackups genutzt werden können. Der Backupjob wird mit dem Befehl *wbadmin enable backup* erstellt, auf den mehrere Schalter folgen können. Einer der wichtigsten Schalter ist "-schedule", der die Zeitplanung aktiviert. Bare-Metal-Backups erstellen Sie wie folgt:

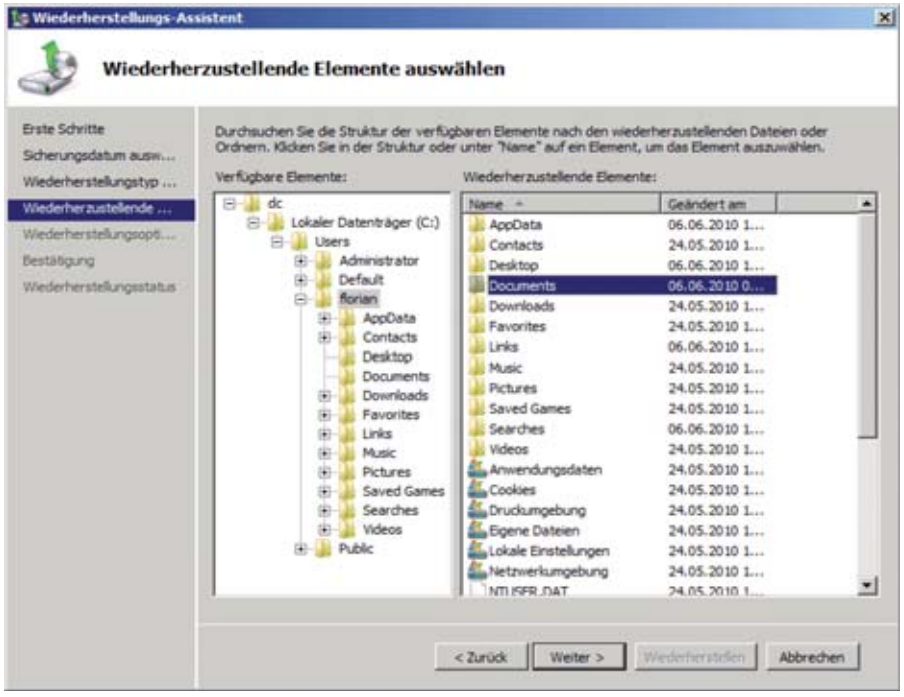


Bild 4: Der Assistent begleitet die Wiederherstellung Schritt für Schritt

```
wbadmin enable backup -allcritical
  -schedule:8:00,14:00,20:00
  -backuptarget:e:
```

Der Befehl plant drei Bare-Metal-Backups täglich ein – für 8 Uhr, 14 Uhr und 20 Uhr. Windows Server Backup geht davon aus, dass Server zumindest einmal täglich gesichert werden – und bietet deshalb von der Kommandozeile und in der Konsole nur die Option für tägliche Backups. Eingeplante Backups werden mit *wbadmin enable backup* aufgelistet. Um Sicherungspläne zu verwerfen und alle Zeitpläne zu löschen, nutzen Sie den Befehl *wbadmin disable backup*. Dabei besteht jedoch keine Möglichkeit, Backupaufträge temporär auszusetzen, um etwa tägliche Sicherungen am Wochenende zu unterbrechen – hierzu müssen Sie für Samstag ein *wbadmin disable backup* skripten und für Montag die entsprechende Wiedererstellung des täglichen Plans für Wochentage mit *wbadmin enable backup […]*.

Seltenere Backups erstellen Sie mit dem Taskplaner. Möchten Sie etwa weiterhin nur wöchentlich oder monatlich Daten sichern, können Sie das über eine geplante Aufgabe zu NTBackup-Zeiten tun – wie etwa das Systemstatusbackup einmal wöchentlich, freitags um 20 Uhr:

```
schtasks /create /sc wöchentlich /D
  FR /TN "wöchentliches Systemsta-
  tusbackup" /RL Highest /ST 20:00
  /TR "wbadmin start systemstateba-
  ckup -backuptarget:e:" /ru {domä-
  ne}\<benutzername /rp *
```

Das Kommando bittet anschließend um die Angabe des Kennworts des angegebenen Benutzers, unter dessen Account der Job nun wöchentlich ausgeführt wird.

Auch für die Nutzung von Netzlaufwerken wird Backupskript mit *schtasks* empfohlen, denn WSB funktioniert nur eingeschränkt mit Freigaben. Für Netzlaufwerke gibt es nämlich keine VSS-Unterstützung, weshalb die Deltasicherung, die zeit- und platzeffizient ist, nicht funktioniert. Außerdem unterstützt WSB in geplanten Sicherungen nicht mehrere Backupversionen, was es dazu veranlasst, das letzte Backup zu löschen, bevor es mit der neuen Sicherung beginnt. Wenn Sie Ihre Sicherungen auf Netzlaufwerken speichern, sollten Sie deshalb ein Backupskript erstellen, das Backups stets an einen neuen Ort kopiert, bevor das nächste Backup durchgeführt wird.

Die MMC-Konsole bietet für die Joberstellung den "Assistenten für Sicherungszeitplan". Schritt für Schritt wird hier – ganz in gewohnter Manier – die Backupart ausgewählt, um anschließend, im zweiten Schritt, die Sicherungszeit anzugeben. Auch hier sind nur tägliche Sicherungen konfigurierbar. Wie oft jedoch an einem Tag gesichert wird, ist frei konfigurierbar. Der folgende Schritt konfiguriert den Sicherungszieltypen. Die Auswahl besteht aus dedizierter Festplatte, Volume oder Netzlaufwerk.

Anschließend wählen Sie das entsprechende Sicherungsziel und schließen den Assistent ab. Die neue Sicherung ist nun in der MMC-Konsole unter "geplante Sicherungen" und "wbadmin enable backup" angelegt.

Fazit

Windows Server Backup bringt so manche Veränderungen mit sich. Administratoren und Storage-Verantwortliche werden sich zusammensetzen müssen, um die Neuerungen von Windows Backup zu planen und umzusetzen. Doch der Aufwand lohnt sich: Kleinere tägliche Sicherungen und schnellere Wiederherstellungen entlohnen den Umstieg von einer dateibasierten Sicherung wie ntbackup zur blockbasierten Lösung mit Windows Server Backup. *(dr)*

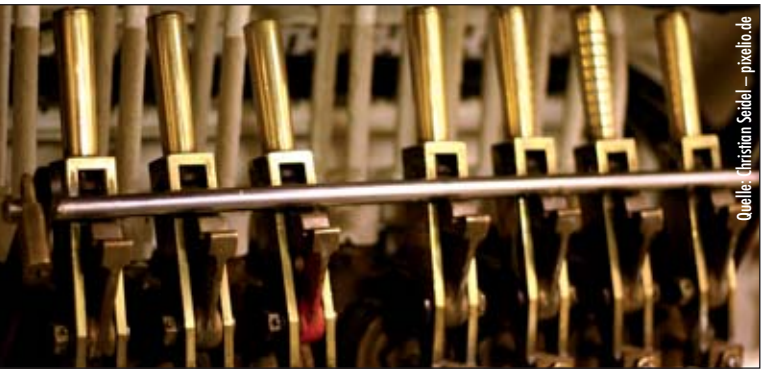
Links

[1] **Download Details: Windows NT Backup – Restore Utility**
www.microsoft.com/downloads/details.aspx?FamilyID=7da725e2-8b69-4c65-afa3-2a53107d54a7&DisplayLang=en

[2] **How to move a Windows installation to different hardware**
http://support.microsoft.com/kb/249694/

Active Directory-Verwaltung über die Kommandozeile

Routinejobs im Handumdrehen


Quelle: Christian Seidel – pixelio.de

In Active Directory-Infrastrukturen aller Größen existieren Aufgaben, die nicht nur einmal, sondern regelmäßig durchgeführt werden müssen. Nicht nur, wenn die Ausführung der Aufgabe an seelische Grausamkeit grenzt, lohnt es sich eine Skriptlösung für die wiederkehrenden Tasks. In diesem Workshop zeigen wir Ihnen spezielle Kommandozeilen-Tools, die Lösungen für bekannte Probleme bieten und sich einfach nutzen lassen.

Meist ist die Zeit, die für die Kommandoerstellung aufgewendet wird, nach zwei oder drei Skript- durchläufen amortisiert. Klug erstellte Kommandos sind flexibel und auch für mehr als nur ein Gebiet einsetzbar. Das massenhafte Anlegen von Benutzeraccounts oder das flinke Entsperren mehrerer Benutzer eines OU-Zweiges sind nur zwei Beispiele. Mit Windows Server 2003 wurden für derartige Arbeiten die DS-Tools eingeführt. Microsoft entwickelte hierbei eine Reihe von Kommandozeilenprogrammen, die Abfragen und Objektselektionen sowie Massenänderungen von der Konsole aus erleichtern. Bei der Namensfindung hat es sich der Hersteller selbst sowie den Nutzern relativ einfach gemacht – die Tools sind schlicht nach ihrem Zweck und Nutzen benannt: DSadd, DSmod, DSrm, DSmove, DSget und DSquery.

DSadd fügt dem Active Directory (AD) neue Objekte hinzu. Dabei haben Sie die Auswahl zwischen Computern, Benutzern, Kontakten, OUs, Gruppen und AD-Quotas – diese Objekttypen werden von DSadd unterstützt. DSmod führt Attributänderungen an bestehenden Objekten durch. DSrm löscht Objekte aus dem Verzeichnis anhand eines angegebenen LDAP-Pfades. Es kann dabei einzelne Objekte oder ganze Zweige aus dem Verzeichnisbaum entfernen. DSmove ist in der Lage, Objekte zwischen Orten im Verzeichnisbaum zu verschieben. Ziel- und Quell-OU empfängt das Programm per LDAP-Pfad. DSquery führt Active Directory-Suchen anhand frei wählbarer Suchkriterien durch und gibt die Suchergebnisse aus. Das letzte Programm, DSget, listet Attribute zum gewählten Objekt aus.

Die verwendete Syntax aller DS-Tools ist durchweg sehr ähnlich – bestimmte Kommandos aus DSadd akzeptiert auch DSmod mit nur minimalen Anpassungen. Bei der Verwendung von DSget und DSquery dürfen Sie sich nicht verwirren lassen: DSquery sucht Objekte aus dem Verzeichnis, während DSget ihre Eigenschaften und Attribute genauer anzeigt. Die beiden Tools werden oft in Kombination verwendet, um erst eine Selektion vorzunehmen und um diese dann anschließend genauer zu untersuchen. Wer es gerne eine Stufe mächtiger hat und sich komplexeren Abfragen hingeben möchte, wird um ADfind und ADmod nicht umher kommen. Beide Werkzeuge werden in diesem Sonderheft in mehreren Beiträgen erwähnt. Nicht zu vergessen ist die mächtige PowerShell, die in immer mehr Produkten aus Redmond Einzug hält. Auch sie kommt nicht zu kurz.

Benutzer automatisiert anlegen

Vielen mag die lästige Arbeit bekannt sein, mehrere Benutzeraccounts im Active Directory anzulegen. Selbst gut vorbereitet geht es von Hand nur schwerfällig voran, gerade wenn mehrere Attribute pro Benutzeraccount mit personifizierten Daten zu füllen sind. Glücklich ist, wer eine Benutzerliste im Excel- oder Textformat vorliegen hat, die er den DS-Tools zum Import vorlegen kann. DSadd ist das Werkzeug der Wahl, das Benutzeraccounts wie folgt anlegt:

```
dsadd user "CN=Michael Donner,OU=
  Benutzer,OU=Einkauf,DC=contoso,DC=
  com" -samid mdonner -pwd {Pass-
  wort} -upn mdonner@contoso.com
```

Als ersten Parameter legen Sie den DN des neuen Benutzerkontos fest. Enthält der Domänenname Leerzeichen wie in unserem Beispiel, müssen Sie den kompletten Pfad in Anführungszeichen mit einschließen. Als Nächstes definieren Sie den Anmeldenamen "sAMAccountname" per "-samid". Der UPN ist dabei optional. Hilfreich ist zusätzlich die De-

finition eines Passwortes. Wird kein Passwort angegeben, legt DSadd den Benutzer deaktiviert an. Das Kennwort setzen Sie entweder per Direkteingabe in Klartext, oder mit "-pwd *", wonach DSadd dann, ohne die eingetippten Zeichen zu verraten, nach der Eingabe des Passworts fragt.

Für das massenhafte Anlegen von Benutzern sind einzelne Befehle keine Hilfe. Liegt eine Liste der Benutzer und deren zu verwendenden Attribute vor, wird aus einem einfachen Kommando ein mächtiges Batchskript. Da Batchskripte Textdateien leicht verarbeiten und nach Textstellen durchforsten können, wird eine Liste von Informationen – separiert in Zeilen, die Eigenschaften getrennt durch Kommata oder Semikolons – für DSadd zur ergiebigen Datenquelle:

```
Braun,Jennifer,jbraun,88374
Hauser,Dorothea,dhauser,88375
Meisner,Franka,fmeisner,34442
```

Der Befehl

```
for /F "eol=; tokens=1,2,3,4
  delims=," %%i in (benutzer.txt) do
  dsadd user "cn=%%j
  %%i,OU=Users,OU=Sales,OU=
  Freiburg,DC=contoso,DC=com" -samid
  %%k -fn %%j -ln %%i -display "%%j
  %%i" -empid %%l -pwd {Passwort}
```

erledigt das Anlegen der Benutzer. Die erste Zeile dient als Schleife, die durch die Zeilen des Textfiles *benutzer.txt* iteriert. Die Zeilen werden gesucht und in Stücke, erkennbar durch das Komma als Trennzeichen, zerhackt. Anschließend wird jede Zeile und ihre gefundenen, separierten Informationen in DSadd weiterverwendet – als Variablen %%i bis %%l – aus den Token 1 bis 4. Die Nachnamen sind jeweils in Variable %%i gespeichert, Vornamen in %%j. Der Anmeldename aus der dritten Spalte wird in %%k abgelegt und die Mitarbeiternummer in %%l. DSadd legt hieraus den Benutzer mit den definierten Informationen an: "-fn" ist der "forename", also der Vorname, "-ln" der Lastname, "-display" definiert den Anzeigenamen im Verzeichnis, der ohne Angabe automatisch vom Tool errechnet wird. Die Mitarbeiternummer, "-empid", wird anhand der Vorgabe aus der Textdatei gefüllt. Zusätzliche Attribute, wie ein vordefiniertes Passwort aus dem Textfile können einfach hinzugefügt werden. Die Datei *benutzer.txt* müssen Sie dazu um eine weitere Spalte ergänzen

```
Doerent,Peter,pdoerent,88453,
  {Passwort}
```

sowie den Befehl bei "tokens" und beim Parameter "-pwd" anpassen:

```
for /F "eol=; tokens=1,2,3,4,5
  delims=," %%i in (benutzer.txt) do
  dsadd user "cn=%%j
  %%i,OU=Users,OU=Sales,OU=
  Freiburg,DC=contoso,DC=com" -samid
  %%k -fn %%j -ln %%i -display "%%j
  %%i" -empid %%l -pwd %%m
```

Bekanntes wiederfinden

Oft ist nicht nur das Anlegen vieler Accounts ein Problem – das Editieren zahlreicher Konten oder Objekte im Verzeichnis kann zu einer mühseligen Kleinarbeit werden. Vor allem, wenn keine statische Liste vorliegt, sondern die Zielobjekte anhand ihrer aktuellen Eigenschaften geändert werden sollen. In diesem Beispiel sollen Benutzer gefunden werden, die sich seit mehr als fünf Wochen nicht eingeloggt haben und somit vermutlich für längere Zeit vom Netzwerk fern bleiben. Mit dem Kommando

```
dsquery user -inactive 5
```

werden sämtliche Benutzer ausgegeben, deren letzter erfolgreicher Logon an der Domäne fünf Wochen oder länger her sist. Um die Benutzer zur Sicherheit zu deaktiveren, nutzen Sie DSmod, das per

```
dsmod user {userDN} -disabled yes
```

die Benutzerkonten sperrt. Da der Befehl eine Eigendynamik erhalten soll und der Bediener nicht alle ausgegebenen Benutzer des DSquery-Befehls erneut eintippen soll, wird das Pipe-Symbol ("|") benutzt – es leitet die Ausgaben des ersten Befehls in den zweiten Befehl um:

```
dsquery user -inactive 5 | dsmod
  user -disabled yes
```

Die vom DSquery-Kommando gefundenen Ergebnisse werden per Pipe als Objekte für das zweite Kommando verwendet. Somit lassen sich mehrere Befehle aneinanderreihen, wodurch Sie Objekte dynamisch als Ergebnis einer Suche in weiteren Kommandos verarbeiten oder ändern. Ein ähnliches Kommando deaktiviert alte Computerkonten:

```
dsquery computer  -inactive 10 |
  dsmod computer-disabled yes
```

findet Computerkonten, die länger als zehn Wochen nicht aktiv waren und ihr

Bild 1: Das Verbinden mehrerer Befehle mit dem Pipe-Symbol erleichtert das Skripten komplexerer Aufgaben

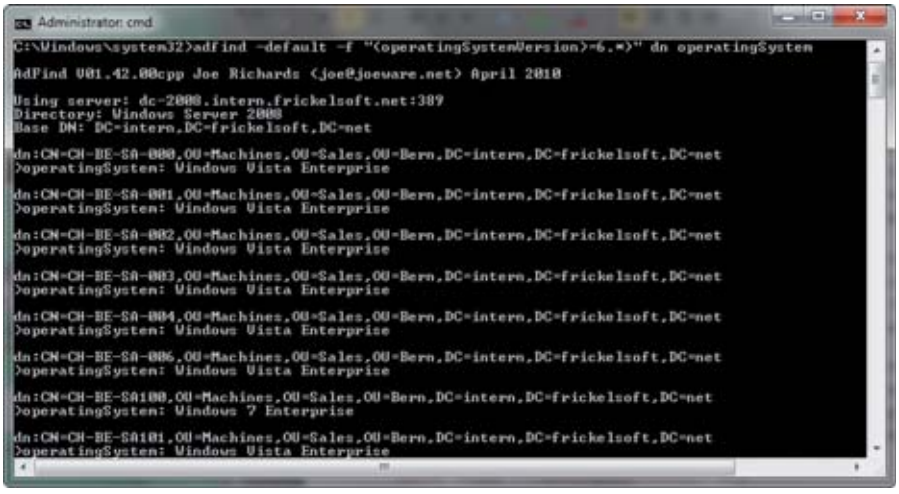


Bild 2: ADfind durchsucht das Verzeichnis nach gewünschten Ergebnissen – und gibt die gewünschten Attribute zu jedem Objekt aus

Passwort an der Domäne änderten – und sperrt sie anschließend. In einem zweiten Schritt, in dem Sie die Pipe von DSmod in DSrm ändern, können Sie sehr alte Computerkonten löschen:

```
dsquery computer -inactive 10 | dsrm
  -noprompt
```

Sind Attribute und Objekteigenschaften interessant, für die DSquery keinen Parameter liefert, hilft Ihnen nur die Erstellung eines LDAP-Filters weiter, den DSQuery mit auf die Suche schickt. Das folgende Beispiel listet alle Computer unterhalb des OU-Zweiges "Freiburg" auf, die mit Windows XP installiert wurden:

```
dsquery computer
  "OU=Freiburg,DC=contoso,DC=com"
  -filter "(operatingSystem=
  *Windows XP*)"
```

Mit dem Parameter "-filter" hängen Sie den LDAP-Suchfilter an. Das Attribut "operatingSystem" der Computerobjekte enthält eine textbasierte Beschreibung des Betriebssystems. Suchen nach mehreren Betriebssystemversionen oder Versionen wie "neuer als" führen Sie dagegen besser über das Attribut "operatingSystemVersion" durch:

```
dsquery * "OU=Machines,OU=Customer
  Support,OU=Freiburg,DC=contoso,DC=
  com" -filter "(operatingSystemVer-
  sion>=6.*)"
```

Die Betriebssystemversion ab 6.x liefert alle Windows-Versionen ab Vista, inklusive der Servervarianten. Erwarten Sie zahlreiche Ergebnisse im Rahmen einer Abfrage, ist es sinnvoll, den Schalter "-limit 0" anzufügen, der die Begrenzung der maximal zurück gelieferten Ergebnisse aufhebt – ohne "-limit 0" liefern Domänencontroller maximal 1.500 Objekte zurück, weitere werden nicht angezeigt.

Noch umfassender suchen und modifizieren

Die DS-Tools sind für alltägliche Aufgaben ausreichend, zeigen bei genauerer Betrachtung allerdings einige Unzulänglichkeiten, die ihre Verwendung in komplexen Szenarien einschränken. Ein Beispiel ist eine Kombination aus DSquery und DSmove mit der Pipe: Obwohl DSQuery die richtigen Objekte aus dem Verzeichnis liest, ist DSmove nicht in der Lage, die per Pipe zugewiesenen Objekte zu verschieben – der Versuch schlägt fehl.

Mächtigere Suchen erstellen Sie mit dem freien Gespann ADfind und ADMod von Joe Richards [1]. ADFind und ADmod sind ebenfalls kommandozeilenbasiert. Anders als die DS-Tools sind beide vollständig LDAP-basiert und in der Lage, Steuerelemente aus dem AD-LDAP-Server zu nutzen. Beide kennen eine Menge an Schaltern und Shortcuts, die wiederkehrende Abfragen und komplexe Suchen deutlich vereinfachen.

Um an ähnlicher Stelle mit den Beispielen der DS-Tools anzuknüpfen, dreht sich die erste Demonstration von ADFind in Kombination mit ADMod um das Verschieben von Computerobjekten bestimmter Eigenschaften in eine andere OU. Der LDAP-Filter für diese Operation ist bereits aus dem DSQuery-Exempel bekannt – gesucht werden Betriebssysteme in der Version Windows Vista oder neuer. Nach ADfind übersetzt, sieht die Abfrage so aus:

```
adfind -default -f
  "(operatingSystemVersion>=6.*)"
```

ADfind listet daraufhin alle mit Werten versehenen Attribute jedes gefundenen Objektes auf – eine ausführliche Ausgabe, die auf ein Minimum gekürzt werden kann. Mit der Nennung der interessanten Attribute am Ende des Kommandos beschränkt sich ADfind auf deren Ausgabe:

```
adfind -default -f
  "(operatingSystemVersion>=6.*)"
  dn operatingSystem
```

Sollen die gefundenen Konten in eine eigene OU verschoben werden, dient ADMod per Pipe-Anschluss als Umzugshelfer. Um nicht alle Computerkonten der Domäne mit Vista oder neuer umzuziehen, setzen Sie den Startzweig für die ADFind-Suche auf eine Unter-OU:

```
adfind -b "OU=customer
  Support,OU=Bern,DC=contoso,DC=com"
  -f "(operatingSystemVersion>=6.*)"
  -dsq | admod -move
  "OU=Test-Driving,DC=contoso,
  DC=com"
```

Alle Computerkonten, die sich in der OU "customer Support" oder einer ihrer Unterzweige befinden und eine neuere Windows-Version als 6 besitzen, werden korrekt

formatiert (-dsq) und anschließend per ADmod in die OU "Test-Driving" verschoben. Andere Massenänderungen können erfolgen, wenn Benutzer von einem Gebäude in ein anderes umziehen. Sind die Adressen im Active Directory gepflegt, kann eine Gruppenänderung mit ADfind und Admod die grobe Arbeit erledigen:

```
adfind -b OU=Management,
  OU=Freiburg,DC=contoso,DC=com -f
  "(&(objectClass=user)
  (objectCategory=person)
  (streetAddress=Goethestraße 3))"
  streetAddress -adcsv | admod
  "streetAddress::Brueckenstrasse
  9a" -upto 20
```

Das Kommando sucht die Mitarbeiter der Goethestraße 3 über das Attribut "streetAddress" aus der Management-OU und ändert die Adresse zu "Brueckenstrasse 9a". Befremdlich mag der Schalter "-upto" wirken, mit dem ADmod Administratoren aber vor sich selbst schützt. Der Schalter dient als Sicherheitsbarriere, um nicht aus Versehen zu viele Objekte zu modifizieren. Per Vorgabe ändert ADmod maximal zehn Objekte mit einem Befehl. Sind mehr Objekte von einer Änderung betroffen, verweigert ADmod nach zehn erfolgreichen Modifikationen seinen Dienst. Dann müssen Sie den Schalter "-upto", gefolgt von der Maximalanzahl der zu ändernden Objekte angeben. Die Anzahl "0" schaltet die Sicherheitsbarriere vollkommen ab.

Um ein Gefühl für die Anzahl der Zielobjekte zu erhalten, existiert der Schalter "-c" für "count". Anstelle der Suchergebnisse in Form von Objekten, spuckt ADfind lediglich die Anzahl gefundener Objekte aus:

```
adfind -b OU=Management,
  OU=Freiburg,DC=contoso,DC=com -f
  "(&(objectClass=user)
  (objectCategory=person)
  (streetAddress=Goethestraße 3))"
  streetAddress -c
```

Deaktivierte Benutzer finden oder sie gar automatisiert zu reaktivieren ist keine leichte Aufgabe. Wer sich bereits an einem Skript dafür versucht hat, kennt das Attribut "userAccountControl", das im Active Directory als Bitmaske abgelegt wird. Jedes Bit des Attributs steht hierbei für eine Funktion des Benutzerkontos, wobei der Wert 0 des Bits die Funktion deaktiviert, die 1 die Funktion einschaltet. Ob ein Benutzerkonto deaktiviert ist, bestimmt Bit Nummer 1, das im gesetzten Zustand dezimal "2" bedeutet. In Skripten wird dann mit dem logischen "UND" geprüft, ob das Bit gesetzt ist oder nicht – und aufgrund dieser Information erkannt, ob ein Account aktiviert ist. Logische Verknüpfungen werden mit LDAP zum Problem, da eigens Vergleichssteuerelemente zur Suchverarbeitung hinzugezogen werden müssen. ADFind abstrahiert komplizierte Suchlogiken und LDAP-Steuerelemente, indem es mit einfach zu merkenden Schlagworten arbeitet:

```
adfind -bit -default -f
  (useraccountcontrol:AND:=2) -dsq |
  admod -move "OU=disabled,
  DC=contoso,DC=com"
```

Deaktivierte Konten, sowohl für Benutzer als auch für Computer, verschiebt ADMod in die OU "disabled", wo sie zur Beobachtung oder weiterer Verarbeitung abgelegt werden. Die Bitmaske wird mit dem Dezimalwert 2 verglichen, der ein deaktiviertes Bit Nummer 1 erfordert. Einige Anfragen beschleunigt ADFind mit Hilfe von Shortcuts, die in dem Werkzeug hinterlegt sind. Der Kommandozeilenhilfe oder der Hilfe-Webseite [2] können Sie die Abkürzungen entnehmen:

```
adfind -sc computers_inactive
```

listet Computerkonten auf, die in den letzten 90 Tage keine Verbindung zu einem Domänencontroller aufgenommen haben. Das Kommando

```
adfind -sc users_disabled
```

listet alle deaktivierten Benutzer auf. Für deaktivierte Computer wird "users_disabled" durch "computers_disabled" ersetzt. Auch Exchange-Funktionen werden mit Shortcuts geliefert, so zählt etwa das Kommando

```
adfind -sc adobjcnt:mailbox
```

alle in der Domäne befindlichen Exchange-Mailboxen auf.

Fazit

AD-Kommandozeilen machen sowohl alltägliche als auch wiederkehrende Arbeiten am Verzeichnisdienst möglich. Ein gut ausgestattetes Textfile mit Beispielkommandos für das Auffinden von gesperrten Benutzern oder das Verschieben von Computer-Accounts bestimmter Eigenschaften sollte jedes Administrators Begleiter sein. Nicht jeder kann ein VBScript, das diese Aufgaben erledigt, aus dem Stehgreif zaubern. Umso besser, wenn es Werkzeuge gibt, die per Kommando und entsprechenden Parametern dazu bewogen werden können, diese Aufgaben zu bewältigen. *(dr)*

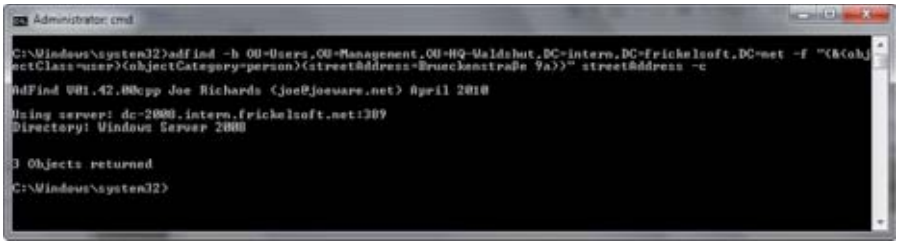


Bild 3: Die Ergebnisanzahl gibt ADfind mit dem Schalter "-c" aus

Links

[1] ADFind und ADMod
www.joeware.net/freetools/index.htm

[2] ADFind Usage
http://joeware.net/freetools/tools/adfind/usage.htm

Read-Only Domain Controller unter Windows 2008

Durchsichtiger Tresor

Quelle: otomo, Fotolia.com

Alte Hasen der IT erinnern sich noch an vergangene Zeiten, als es zur Windows NT4-Ära im Domänenumfeld zwei Kategorien von Domänencontrollern gab: Primäre Domänencontroller und Backupdomänencontroller. Auf dem PDC wurden alle Änderungen geschrieben, und da es nur einen geben durfte, konnten auch keine Konflikte entstehen. BDCs übernahmen damals die Authentifizierung von Clients und wurden für alles verwendet, wo Lesezugriffe ausreichten. Im Fehlerfall konnten sie zum PDC heraufgestuft werden und diesen ersetzen. Windows 2000 löste mit dem Active Directory dieses Konzept ab – und machte alle DCs zu gleichberechtigten Partnern im Domänenbund. Nun scheint es, dass Microsoft mit dem "Schreibgeschützten Domänencontroller" in Windows Server 2008 das PDC/BDC-Konzept wieder einzuführen versucht, weniger wichtige DCs als Nur-Lese-Speicher einsetzt und alte Zeiten aufleben lässt. Dieser Workshop führt in die Funktionsweise des RODC und dessen Administration ein.

Schreibgeschützte Domänencontroller (Read-Only Domain Controller, RODC) sind weder die Reinkarnation des NT4-Domänenmodells, noch stellen sie eine Verschiebung der Architektur des Active Directory dar. Vielmehr ist über die Jahre das Bewusstsein gestiegen, dass Domänencontroller geschützt werden müssen. Kommt der Server abhanden, oder auch nur eine der komfortablerweise redundant gespiegelten Festplatten, die per Hot-Swap schnell gewechselt werden können, muss der Administrator alle Kennworte des Unternehmens ändern: Benutzerkonten, Servicekonten, Administratorkonten, Trusts, Computerkonten oder auch zusätzlich gespeicherte Credentials und so weiter. Andere Unternehmen wollten DCs vermehrt in DMZs einsetzen oder sogar ins Internet stellen. Daher entstand die Notwendigkeit, eine DC-Rolle zu entwerfen, die deutlich mehr Sicherheit bietet.

Funktionsweise des RODC

RODCs ermöglichen es Administratoren, flexibel und effizient auf sicherheitskritische Anforderungen an DCs zu reagieren. Primäre Einsatzgebiete für RODCs sieht Microsoft an Standorten, die keinen hohen Sicherheitsstandards entsprechen, wo kein geschultes Personal zur Administration verfügbar ist oder wo ein erhöhtes Sicherheitsrisiko durch vermehrten Zugriff von außerhalb des Firmennetzwerkes möglich ist.

RODCs werden per se als "angegriffen" betrachtet und sind, basierend auf dieser Annahme, entworfen worden. Der größte Vorteil dabei ist, dass Passwörter standardmäßig nicht auf diesen DCs gespeichert werden – daher muss der RODC die Authentifizierung über einen vollwertigen DC laufen lassen. Setzen sie den RODC aber in einer Außenstelle ein und möchten, dass sich die Anwender dort auch authentifizieren können, wenn die Netzwerkverbindung zur Zentrale mal nicht da ist, können die Passwörter dieser Anwender (sowie deren Computer) auch zwischengespeichert werden.

Wie der Namen schon erahnen lässt, kann der RODC selbst keine AD-Daten schreiben. Angreifern ist es nicht möglich, Daten zu manipulieren oder sich durch das Erschleichen oder Verändern von Gruppenmitgliedschaften Zugriff zu verschaffen. Selbst wenn Änderungen an der AD-Datenbank eines RODCs durchgeführt würden (was ausschließlich mit Hacker-Methoden gelingt): Ein RODC wird diese Änderungen nicht replizieren – es existieren nämlich keine ausgehenden Replikationsverbindungen zu schreibfähigen DCs. Ein RODC repliziert lediglich durchgeführte Änderungen anderer DCs zu sich und übernimmt sie in seine lokale AD-Datenbank. Er führt keine relevanten Schreibaktionen an der Datenbank durch.

Auch das Sicherheitsmodell unterscheidet sich bei RODCs von beschreibbaren Domänencontrollern. Lokale Administratoren von RODCs haben keinen schreibenden Zugriff auf das Active Directory – das ist von Vorteil, wenn dem Wartungspersonal für Patchinstallationen oder Eingriffe auf Betriebssystemebene Rechte vergeben werden, das AD aber unberührt

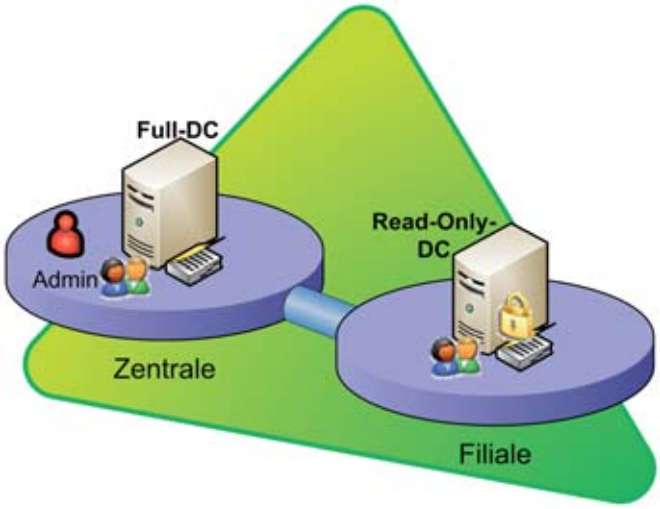


Bild 1: RODCs werden dort eingesetzt wo die Sicherheit von Domänencontrollern nicht gewährleistet werden kann, wie in Außenstellen …

bleiben soll. RODC-Admins müssen keine Domänen- oder Serveradministratoren sein. Die Erteilung lokaler Administratorberechtigungen genügt.

Im Falle des Diebstahls eines RODCs lässt sich Schadensbegrenzung betreiben: Das Active Directory merkt sich die zwischengespeicherten Passwörter der Benutzer und Computer, die sich über einen RODC angemeldet haben. Nach einem Diebstahl bietet das AD dann direkt das Sperren beziehungsweise Rücksetzen der Passwörter oder einen Export der betroffenen Konten an. Der Diebstahl eines schreibbaren DCs wäre ungleich schlimmer: dort sind alle Accounts in Gefahr und müssten zurückgesetzt und mit einem neuen Passwort versehen werden.

Einsatzgebiete von RODCs

Aufgrund der Annahme, dass RODCs nicht vertraut werden kann, ist ihr Einsatz an kritischen Standorten möglich. Plausibel wird dies beim Einsatz in kleinen Standorten, an denen keine ausreichende Sicherheitsvorkehrungen wie zugriffsbeschränkte Serverräume herrschen oder aber viele Mitarbeiter, inklusive Kunden oder dem unbeaufsichtigten Reinigungspersonal, Zutritt zum Serverraum haben. Da RODCs keine Änderungen in das produktive AD replizieren, besteht kein Grund zur Sorge vor einer Übernahme des RODC oder der Manipulation von AD-Daten. Selbst bei Erfolg wären die Auswirkungen stets nur lokal zu spüren und nicht an Hauptstandorten oder an Diensten außerhalb des lokalen Standortes. Sind Standorte zu klein für eine umfangreiche, physikalische Sicherung eines vollen DCs, ist ein RODC eine gute Alternative.

Ein weiterer Grund für RODCs wären Standorte mit geringer Bandbreite. Sollen sich Benutzer und Computer lokal authentifizieren, weil die Bandbreite zwischen Standort und Zentrale zu gering ist, um diesen Datenverkehr zu erlauben und Benutzer nur lokale Dienste in Anspruch nehmen, kann der RODC hilfreich sein. Das Speichern von Anmeldeinformationen auf den RODC hilft dabei, die Belastung der Verbindung so gering wie möglich zu halten und bietet den Mitarbeitern dennoch die Möglichkeit, alle Dienste ihres Standortes mit der gewohnten AD-Anmeldung zu nutzen.

Microsoft unterstützt mittlerweile auch den Einsatz von RODCs in der Demilitarisierten Zone (DMZ) – dem Perimeternetzwerk, das zwischen dem internen LAN und dem Internet liegt. Vielerorts wird die DMZ eingesetzt, um Webserver oder Dienste für Kunden und Mitarbeiter anzubieten. Wird hierfür eine Form von Authentifizierung benötigt, aber die direkte Kommunikation zu internen DCs ist nicht gestattet oder das Risiko ist zu groß, können RODCs hierfür eingesetzt werden.

Der Einsatz von RODCs ist erst ab der Schemaerweiterung für Windows Server 2008-DCs möglich – ADprep muss mit dem Schalter "rodcprep" erfolgreich ausgeführt worden sein und im Hauptstandort, mit dem sich DMZ oder der Nebenstandort verbinden, muss ein schreibbarer Windows Server 2008-DC stehen.

Trotzdem Schreibzugriff

Es bestehen weiterhin Situationen, in denen Clients aus dem Perimeternetzwerk

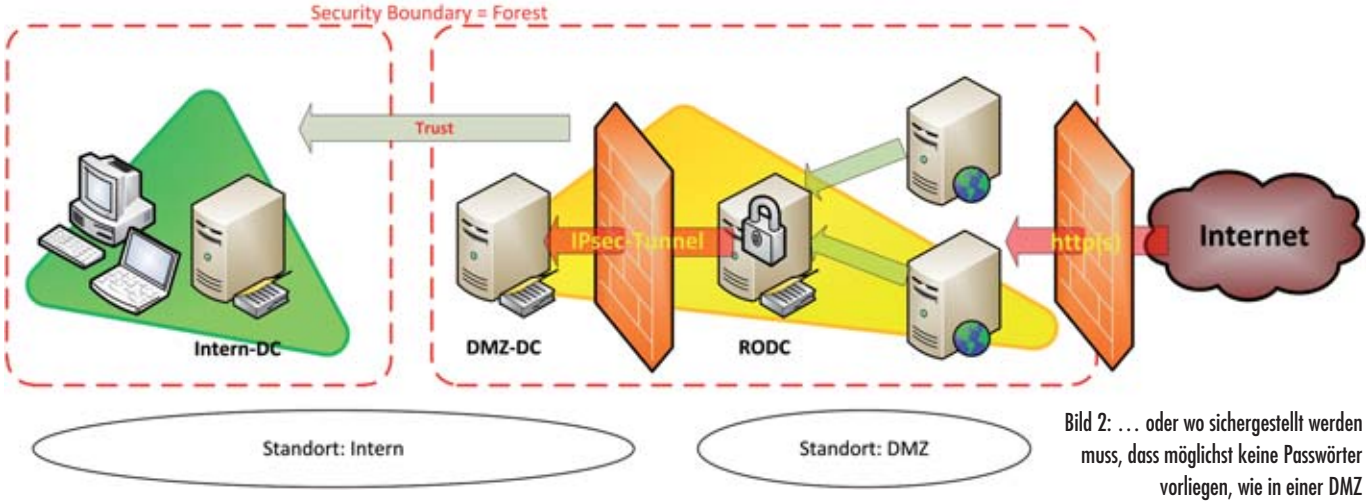


Bild 2: … oder wo sichergestellt werden muss, dass möglichst keine Passwörter vorliegen, wie in einer DMZ

oder in einer Außenstelle schreibend auf das Verzeichnis zugreifen müssen. Gerade, wenn Benutzer ihre Passworte ändern wollen oder Computer ihre DNS-Einträge beim DNS-Server aktualisieren, muss die Änderung am Verzeichnis von einem DC aufgenommen und verarbeitet werden. Für Clients ist der RODC in erster Linie nicht als "nur lesend" erkennbar – sie kontaktieren ihn aus diesem Grund für Änderungen am Verzeichnis.

Hier müssen wir zwischen den Mechanismen unterscheiden: Wenn ein Client oder eine Applikation schreibend auf den Domänencontroller via LDAP zugreifen will, erhält sie vom RODC einen LDAP-Referral – also einen Hinweis, dass die Verzeichnisdienstinstanz nicht beschreibbar ist und an welchen Server sich die Applikation wenden kann. Dies ist ein "voller DC" normalerweise in der Zentrale (Replikationspartner des RODC). Diese LDAP-Referrals sind Standard und sollten von allen wichtigen LDAP-APIs automatisch unterstützt werden. Die zuständige Komponente auf dem Clientsystem, die die Schreibänderung durchsetzen wollte, erkennt anhand des LDAP-Referrals, dass es einen geeigneteren DC für diese Änderung gibt und wendet sich, gemäß des Referrals, an einen dritten, schreibbaren DC im Hauptstandort. Der Client wird somit "freundlich" zum RWDC umgeleitet, wo sein Schreibwunsch bearbeitet wird. Der RODC erfährt zunächst nichts von dieser Änderung. Erst wenn die eigentliche Replikation eines schreibbaren DCs zum RODC stattfindet, werden die geänderten Daten zum RODC repliziert.

Möchte ein Client seinen DNS-Eintrag aktualisieren, ist die Prozedur eine andere. Standardmäßig muss ein DNS-Client, der einen Schreibzugriff durchführen will, zunächst nach einem schreibbaren DNS-Server suchen. Nachdem im klassischen DNS auch das Prinzip einer primären Kopie der Zone und mehreren sekundären herrscht, fragt der Client den DNS-Server zunächst nach dem "Start-of-Authority (SOA)"-Eintrag. Dieser gibt an, welcher Server schreibend für die Zone zuständig ist. Im SOA steht standardmäßig nur ein Server – wie gesagt verfügt im klassischen DNS nur einer über Schreibberechtigungen. Diejenigen Windows DNS-Server, die eine schreibbare Kopie der Zone haben (weil AD-integriert und die Konflikte dort behandelt werden), geben sich selber als SOA wieder. Nicht so der RODC, dieser gibt seinen Replikationspartner, einen vollwertigen DC, als SOA wieder. Der DNS-Client folgt weiterhin seinem Standardprozess und kontaktiert den Server, der im SOA stand, um das Update zu schreiben. Der RODC merkt sich jedoch, dass sich der Client gerade nach einem schreibbaren Server erkundigt hat, und fragt kurz darauf den vollwertigen DC an, ob er den DNS-Eintrag des Clients replizieren kann (über einen sogenannten "Replicate_Single_Object Request"). Daher ist der RODC dann für den Client in seinem Wirkungskreis aktuell.

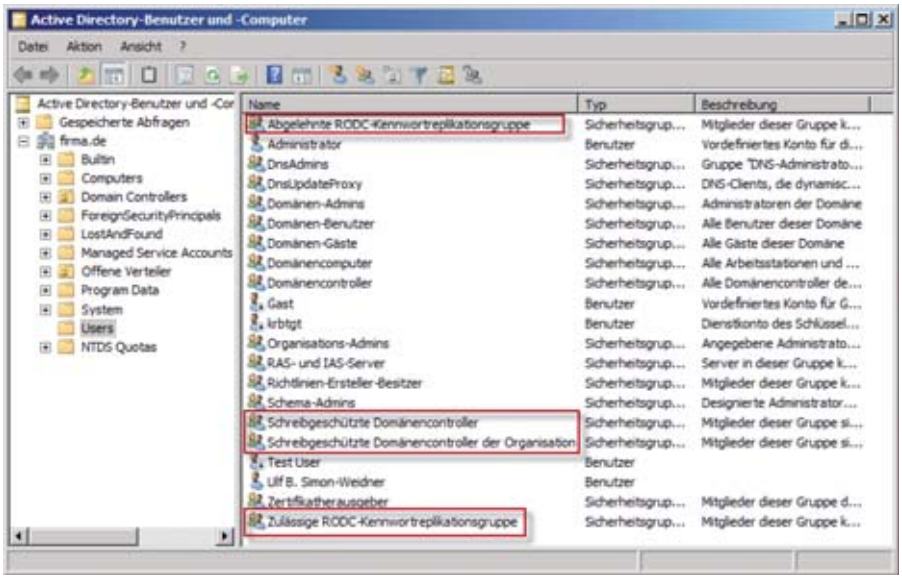


Bild 3: Die Administration von RODCs erfolgt über Windows-Gruppen

RODC-Authentifizierung administrieren

Um größtmögliche Sicherheit an Standorten und der DMZ zu gewährleisten, verhält sich ein RODC signifikant anders bei Anmeldeversuchen von Computern und Benutzer, als es schreibbare DCs tun. RODCs replizieren zwar alle Active Directory-Daten, aber keine Passwörter. Dies ist ihnen standardmäßig nicht erlaubt. Sie müssen RODCs explizit erlauben, Passworte von Computern und Benutzern zu cachen. Die Erlaubnis erteilt die Password Replication Policy (PRP). Sie gibt über eine Positiv- und eine Negativliste vor, welche Accounts für die Zwischenspeicherung erlaubt sind. Ist ein Account nicht in der Positivliste, werden die Anmeldeinformationen nicht gespeichert, es sei denn, er ist zusätzlich in der Negativliste.

Der Anmeldevorgang an einem RODC sieht wie folgt aus: Ein Benutzer versucht, sich mit seinem Benutzernamen und Passwort in einer Außenstelle anzumelden. Die Anmeldung wird von einem RODC bearbeitet, der zunächst prüft, ob die Anmeldeinformationen in seinem lokalen Zwischenspeicher liegen. Ist dies der Fall, wird der Benutzer direkt vom RODC authentifiziert. Sind sie nicht gegenwärtig, leitet der RODC selbst die Anfrage an einen schreibbaren Domänencontroller mit mindestens Windows Server 2008 im Hauptstandort weiter. Der DC prüft die Informationen und authentifiziert den Benutzer – der Austausch der Kerberos-Meldungen erfolgt und der Benutzer ist authentifiziert.

Bei Beendigung der Authentifizierung versucht der RODC per "Single Object

Replication", das Passwort des Accounts vom Hauptstandort-DC zu replizieren. Dieser prüft, ob genau diesem RODC die Zwischenspeicherung per Password Replication Policy (PRP) gestattet ist. Falls ja, wird das "Geheimnis" des Clients zum RODC repliziert. Falls nicht, rückt der schreibbare DC die Informationen nicht heraus und der nächste Anmeldevorgang läuft ebenso ab. Ist der betreffende Account in der PRP enthalten und der RODC konnte die Informationen speichern, kann er die nächste Anmeldung dieses Accounts lokal abwickeln und muss nicht den DC am Hauptstandort kontaktieren.

Password Replication Policy verwalten

Die Password Replication Policy ist ein wichtiger Bestandteil bei der Administration von RODCs. Um die Last auf der Verbindung der Standorte zu verringern, lässt sich die PRP einfach konfigurieren. Die eigentliche Administration der PRP erfolgt über die Active Directory-Gruppen, die bei der Installation des ersten Windows Server 2008 erstellt werden. Es werden standardmäßig zwei Gruppen im AD erzeugt, in die Sie Benutzer und Computeraccounts hinzufügen müssen: "Zulässige RODC-Kennwortreplikationsgruppe" und die "Abgelehnte RODC-Kennwortreplikationsgruppe". Mitglieder der "Zulässigen RODC-Kennwortreplikationsgruppe" dürfen auf dem RODC zwischengespeichert werden, wenn sie sich über diesen anmelden, Mitglieder der "Abgelehnt"-Gruppe dürfen RODCs niemals zwischenspeichern – auch nicht bei erfolgreichen Anmeldungen in der Außenstelle und gleichzeitiger Mitgliedschaft in der Erlaubt-Gruppe. So wird das grundlegende PRP-Verhalten gesteuert.

Die PRP besteht – im Detail betrachtet – nur aus Attributen, die dem RODC im Active Directory zugeordnet sind. Die dazugehörigen Attribute, in denen die Gruppen gespeichert sind, heißen "msDS-NeverRevealGroup" und "msDS-RevealOnDemandGroup". Daher können Sie die Liste, auch über die Gruppen hinaus, erweitern.

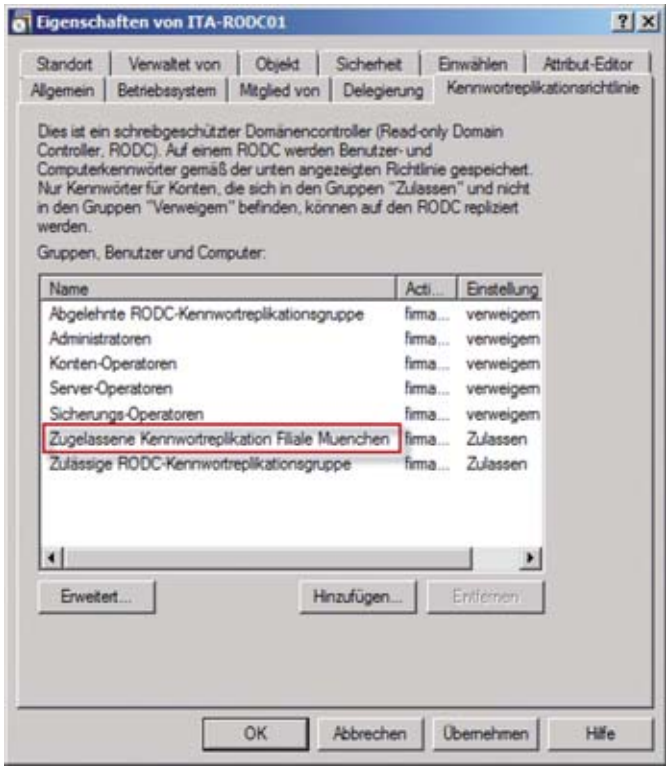


Bild 4: Best-Practice: Für jede Filiale liegt eine eigene "Erlaubt"-Liste für die Passwort-Replikation vor

Versorgen Sie mehrere Standorte mit RODCs, so lautet die Best Practice, nicht die standardmäßige Erlaubt-Liste zu verwenden. Für die Erlaubt-Liste empfiehlt es sich, eine Gruppe pro Standort zu verwenden, für die "Verboten"-Liste eine globale Gruppe. In dieser sind standardmäßig schon die kritischsten Accounts, wie Domänen-Admins, DCs, Schema-Admins et cetera vorhanden. Erweitern Sie die Verboten-Liste um zum Beispiel die zentralen Dienstekonten, Ihre Administrativen Gruppen, die höhere Rechte haben und weitere kritische Konten. In die Erlaubt-Liste für jeden Standort einzeln gehören diejenigen Anwender, die sich an diesem Standort befinden, und deren Passwörter auch für den Fall des WAN-Ausfalls gespeichert werden sollen. Mit dieser Strategie halten Sie die Anzahl von Accounts, die im Schadenfall gesperrt werden müssen oder deren Kennwörter Sie ändern müssen so niedrig wie möglich, während Sie nebenbei sicherstellen, dass keiner der kritischen Accounts auf einem RODC landet.

Hierfür erstellen Sie eine Gruppe (Domänenlokal) für die "Zugelassene Kennwortreplikation Filiale xyz" und konfigurieren Sie im Reiter "Kennwortreplikationsrichtlinie" des RODC in "Active Directory-Benutzer und -Computer" als "Zugelassene Gruppe".

Wie können Sie jedoch herausfinden, welche Accounts denn nun auf RODCs zwischengespeichert werden müssen, etwa weil sie sich bereits einmal dort angemeldet hatten? Die Antwort liegt in der Zwischenspeicherung der AD-Anmeldungen am RODC. Active Directory führt Buch über die erfolgreichen Anmeldungen von Benutzern an RODCs. Diese Buchführung hilft Administratoren zu erkennen, ob bestimmte Accounts für die Zwischenspeicherung auf RODCs freigegeben werden sollten, etwa um die Anmeldung bei WAN-Link-Ausfällen zu gewährleisten.

Das AD merkt sich ebenfalls, welche Accounts auf einem RODC zwischengespeichert wurden. Eine hilfreiche Information, falls der RODC gestohlen oder kompromittiert wurde, um die betreffenden Accounts zurücksetzen zu können. Die entsprechenden Funktionen befinden sich in den Eigenschaften des RODC-Computeraccounts in "Active Directory-Benutzer und -Computer" in der Domänencontroller-OU. Im Reiter "Kennwortreplikationsrichtlinie" unter der Schaltfläche "Erweitert" finden Sie

die entsprechenden Konten. Wenn Sie einen RODC löschen wollen, erhalten Sie eine Abfrage wie Sie mit den Konten verfahren wollen, die zwischengespeichert wurden.

Die Schaltfläche "Exportieren" ist ebenfalls vorhanden, um die Liste der betroffenen Konten jederzeit in eine Textdatei zu exportieren. Die Liste "Konten, die von diesem Read-Only Domänencontroller authentifiziert wurden" gibt Auskunft darüber, welche Accounts im Standort des RODC waren und sich bereits zumindest einmal angemeldet hatten. Die Chance ist groß, dass sich diese Accounts in naher Zukunft erneut dort anmelden werden, womit die Liste ein guter Ausgangspunkt für die "Zulässige RODC Kennwortreplikationsgruppe" darstellt. Bleibt die "Zulässige RODC Kennwortreplikationsgruppe" beziehungsweise deren selbsterstellte Pendants leer, benötigt der RODC für jeden Anmeldeversuch die Hilfe eines Server 2008 (R2)-DCs am Hauptstandort.

Um die Anmeldung von Konten bei häufigen Ausfallzeiten des WAN von Anfang an zu erlauben und nicht die erste Anmeldung jedes Anwenders abzuwarten, gibt es auch die Möglichkeit, die Passwörter einzelner erlaubter Konten auf den RODC zu pushen. Beim "Präpopulieren", das im Deutschen unter "Erweitert" und dort unter der Schaltfläche "Kennwörter auffüllen" zu finden ist, statten Sie einen RODC mit den gewünschten Passwörtern aus, so dass sich Benutzer und Computer am RODC ohne WAN-Verbindung zum Hauptstandort anmelden können – selbst wenn sie sich noch nie zuvor am RODC angemeldet haben. Ein entscheidender Vorteil: die Anmeldung neuer Benutzer funktioniert in jedem Fall, da der RODC keine Bestätigung eines schreibbaren DCs aus der Zentrale benötigt. Ein Nachteil ist hingegen, dass die Accountinformationen auf dem RODC gespeichert sind, obwohl sich der Nutzer möglicherweise niemals dort anmelden wird.

Das Präpopulieren mit Passwörtern ist an zwei Orten des Betriebssystems möglich: über die "Active Directory-Benutzer und Computer"-MMC und über die Kommandozeile. Über den Reiter "Kennwortreplikationsrichtlinie" der Eigenschaften eines RODC-Computerkontos gelangen Sie über die Schaltfläche "Erweitert" und "Kennwörter auffüllen" zur entsprechenden Oberfläche. Über diesen wählen Sie die gewünschten Konten und bestätigen diese anschließend. Die Passworte werden daraufhin zum RODC repliziert.

Per Kommandozeile, etwa wenn Sie die automatische Ausstattung der RODCs anhand einer Liste oder andere Abfragen durchführen, werden Passworte mit "repadmin" an den RODC repliziert. Der korrekte Befehl für die Durchführung lautet:

```
repadmin /rodcpwdrepl {rodc} {2008-
  dc} "CN=Thomas
  Neuenreuther,OU=Stuttgart,
  OU=Deutschland,DC=contoso,DC=com"
```

Mit dem Befehl geben Sie den betreffenden RODC, den beschreibbaren 2008-DC in der Zentrale sowie den LDAP-Pfadnamen des betreffenden Accounts an. Im Beispiel handelt es sich um einen Benutzer aus Stuttgart – Computerkonten sind jedoch ebenfalls möglich.

Was Sie auf keinen Fall vergessen sollten sind eben diese: Benutzer können sich nur anmelden, wenn sich das Computerkonto zuvor an der Domäne authentifizieren konnte. Daher sollte Sie auch alle Computerkonten einer Außenstelle in die zugelassene Kennwortreplikationsgruppe aufnehmen und gegebenenfalls ebenso auffüllen.

Passwortwechsel

Am Ende der Konfiguration sind die gewünschten Konten auf dem RODC zwischengespeichert und sollten, falls die Verbindungsstrecke zwischen Zentrale und Nebenstandort ausfällt, in der Lage sein, lokale Anmeldungen durchzuführen. Um ein vollständiges Bild von RODCs zu erhalten, ist das Verständnis zweier weiterer Szenarien notwendig: Was passiert, wenn das Passwort eines Accounts geändert wird oder es abläuft? In beiden Fällen erhält der RODC die entsprechende Meldung per Replikation aus der Zentrale. Sofort im Anschluss setzt er die Passwortinformationen des betreffenden Kontos auf "nicht gegenwärtig" – als hätte die Information nie vorgelegen.

Für neue Anmeldungen muss der RODC daraufhin die Authentifizierungsanfrage an einen schreibbaren DC weiterleiten und das Passwort, sollte ihm das erneute Zwischenspeichern per PRP erlaubt sein, wieder cachen. Für präpopulierte Accounts gibt es keinen automatischen Abgleich, der den RODC auf den neuesten Stand bringt: Die Anmeldeinformationen müssen erneut auf den RODC übertragen werden, sollten sie sich zwischenzeitlich ändern.

Das zweite Szenario beschäftigt sich mit der Frage, welche Accounts denn in der zugelassenen Kennwortreplikationsgruppe benötigt werden. Viele Benutzer wechseln Standorte oder scheiden aus und Computer werden ersetzt oder aussortiert. Die "Zwischenspeichern erlauben"-Liste wächst dabei stetig weiter und wird unübersichtlich. Leider nicht im Windows-Server enthalten, dafür aber für Scripting-Füchse umsetzbar, existiert eine Logik, die Ihnen genau diese Fälle aufzeigt. Das Active Directory speichert von RODCs weitergeleitete Anmeldungen an schreibbaren Zentralen-DCs in einem Attribut namens "msDS-AuthenticatedToAccountList" am Computerkonto des RODCs.

Das Attribut wird stets mit Benutzer- und Computerkonten gefüllt, wenn der RODCs eine Anmeldeanfrage an einen anderen DC weiterleiten muss. Leeren Sie diese Liste regelmäßig und vergleichen Sie sie mit der Liste der erfolgreich zwischengespeicherten Konten des

RODCs – das zugehörige Attribut heißt "msDS-RevealedUsers" – und der "Zugelassenen RODC Kennwortreplikationsgruppe" (idealerweise der des Standorts), lässt sich ein klares Muster erkennen: Denn Konten, die über längere Phasen nicht in der msDS-AuthenticatedToAccountList auftauchen und deren Passwort auch nicht auf dem RODC zwischengespeichert wurde, melden sich auch nicht am RODC an. Sie können diese demnach aus der "Zwischenspeichern erlauben"-Gruppe entfernen.

RODCs effizient einsetzen

Abschließend gibt es einige wenige Besonderheiten im Umgang mit RODCs, auf die beim ihrem Einsatz geachtet werden sollte. Mehrere RODCs in einer Außenstelle erhöhen die Ausfallsicherheit und Performanz nicht. Im Gegenteil: mehrere RODCs an einem Standort können zu Problemen führen, da unter den RODCs keine AD-Replikation erfolgt. Zwischengespeicherte Passwörter auf RODC-1 werden nicht zum RODC-2 übertragen. Meldet sich ein Benutzer per RODC-1 am AD an und seine Informationen werden auf dem RODC-1 gespeichert, können Probleme auftreten, wenn der WAN-Link gestört wird und bei der nächsten Anmeldung RODC-2 der authentifizierende DC ist. RODC-2 müsste, um die Authentifizierung durchführen zu können, einen schreibbaren DC kontaktieren, obwohl RODC-1 die Informationen zwischengespeichert hat.

Zudem erhöhen mehrere RODCs an einem Standort den Administrationsaufwand, da Passworte stets mehrfach präpopuliert werden müssten. Eine Lösung hierfür wäre wiederum ein Skript zu entwickeln, das die Konten, die sich an einem der RODCs authentifiziert haben, regelmäßig an den anderen RODC präpopuliert.

Für das Szenario RODC in der DMZ ist es aber valide, mehrere RODC in der DMZ für erhöhte Ausfallsicherheit anzusiedeln. Hier können Sie gewöhnlicherweise gute Verbindungen erwarten und sollten auch auf keinen Fall Passwörter zwischenspeichern, so dass der genannte Effekt keine Relevanz hat.

Eingesetzte Anwendungen, die AD-Zugriff benötigen, sollten Sie auf ihre Funktion mit RODCs hin überprüfen. Obwohl die Schreibweiterleitung und das Lesen im Zusammenhang mit RODCs nahezu transparent funktioniert, vorausgesetzt die Anwendung kann mit einem LDAP-Write-Referral umgehen, kann es Probleme bei zu schnellen Schreib- und anschließenden Leseversuchen geben.

Exchange ist eine der großen Anwendungen, die nicht mit einem RODC funktionieren. Betreiben Sie jedoch einen Exchange-Server in einer Außenstelle, sollten Sie dies nur tun, wenn Sie auch die physikalische Sicherheit des Servers gewährleisten können. Denn es wäre sicher nicht in Ihrem Sinn, wenn E-Maildaten in falsche Hände geraten. Sobald dies gegeben ist, spricht auch nichts dagegen einen vollwertigen DC in den Standort zu stellen. Prinzipiell zentralisieren Unternehmen Exchange zunehmend, und der Einsatz von RODCs sollte dies unterstützen.

Da der RODC Schreibzugriffe an einen schreibbaren DC weiterleitet und die geschriebenen Änderungen erst per Replikation aus der Zentrale übernimmt, entsteht eine Verzögerung, mit der die Information zum RODC zurückkommt. Anwendungen, die Daten schreiben und sie umgehend vom Verzeichnis lesen wollen, müssen sich – wie bei replizierten Datenspeichern üblich – merken, wo sie die Daten geschrieben haben und den gleichen DC verwenden.

Zusätzlich werden neben Passwörtern einige "gefilterte" Attribute nicht an RODCs repliziert. Objektattribute des Verzeichnisses, die dem "Filtered Attribute Set" angehören, werden nicht auf RODCs gespeichert, da sie von der Replikation ausgenommen sind. Windows 2008-DCs im Hauptstandort bieten diese RODCs schlicht nicht zur Replikation an und verschweigen sie. Diese Attribute sind vom RODC aus nicht lesbar und müssen, ohne dass hier ein automatischer Referral durchgeführt wird, von einem schreibbaren DC entnommen werden. Der RODC verhält sich der Anwendung gegenüber so, als wäre der Wert leer. Standardmäßig sind es aber nur Attribute die normalerweise nicht benötigt werden, wie die Bitlocker-Schlüssel für die Rücksetzung, die von Microsoft als kritisch genug betrachtet wurden, um nicht auf einen RODC repliziert zu werden.

Ein letztes Kriterium, das Sie bei RODCs beachten sollten, sind Vertrauensstellungen: Ein RODC kennt die Passwörter auch nicht für die Vertrauensstellungen, und kann somit keine Konten über eine Vertrauensstellung hinweg authentifizieren. Sollte also das klassische Master-Ressource-Model zum Einsatz kommen, wo sich die Computerkonten in einer anderen Domäne verhalten wie die Benutzerkonten, können RODCs die Authentifizierung in der Außenstelle nicht durchführen, selbst wenn die Passwörter beider Konten zwischengespeichert sind. Die leiten die Authentifizierung jeweils an den vollwertigen DC weiter, der dann auch die Authentifizierung über die Vertrauensstellung übernimmt. Das Szenario funktioniert also nur, solange die WAN-Leitungen verfügbar sind.

Fazit

RODCs sind eine interessante Technologie für DMZs und Außenstellen, die keine physische Sicherheit für Domänencontroller gewährleisten können. Sie können Anmeldungen "zwischenspeichern" und selbst bei Konten, in denen die Passwörter nicht zwischengespeichert sind, läuft die Authentifizierung schneller, da alle Daten bis auf das Kennwort vor Ort liegen. Dies betrifft vor allem auch die Gruppenrichtlinien, die maßgeblich sind für die Geschwindigkeit von Anmeldungen. Trotzdem ist es notwendig, dass der Administrator RODCs und deren Spezialeffekte versteht. *(jp)*


Quelle: pixelio.de

Built In-Gruppen schützen

Gruppenbildung

Bei der Installation des Active Directory legt die Installationsroutine nicht nur grundlegende Objekte wie das Schema und die Konfiguration in den jeweiligen Partitionen an, sondern auch einen Satz von Gruppen, die Administratoren zur Delegation von Aufgaben dient. Diese Built In-Gruppen werden im "Builtin"-Container der Domäne angelegt und besitzen durch die in den Standard-Gruppenrichtlinien vorgegebenen Einstellungen teils weitreichende Berechtigungen für die lokale Domäne. Dieser Workshop erklärt, über welche Berechtigungen diese Gruppen verfügen und zeigt deren mögliche Auswirkungen in der Praxis. Darüber hinaus erfahren Sie, wie Sie Rechte dieser Gruppen delegieren.

Per Vorgabe sind nur wenige Gruppen mit Benutzern gefüllt. Es steht Administratoren frei, die vordefinierten Gruppen nach Belieben zu nutzen und beispielsweise Mitarbeiter des Helpdesks oder Administratoren anderer Standorte als Mitglieder hinzuzufügen. Die Tabelle "Built In-Gruppen" listet die Gruppen und die besondere Berechtigungen auf. Zusätzlich zu den im "Builtin"-Container erstellten Gruppen verfügt eine Domäne über Gruppen im "Users"-Container (Tabelle: Gruppen im Users-Container). Weitere Informationen zu den Berechtigungen, liefert ein Technet Whitepaper [1].

Nutzung privilegierter Built In-Gruppen

Von den drei im Users-Container genannten administrativen Gruppen wird die Schema-Admin-Gruppe häufig unterschätzt. Obwohl Mitglieder dieser Gruppe keine Daten in der Domänenpartition manipulieren können, sind sie dennoch in der Lage, Schaden am Verzeichnis anzurichten. Das Schema in der Schemapartition ist die Definition aller Objekte, die im Verzeichnis existieren und neu im Verzeichnis erstellt werden. Änderungen am Schema können dazu führen, dass das Active Directory (AD) nicht mehr ordnungsgemäß funktioniert, so dass das Erstellen neuer Objekte oder die Replikation von Daten zwischen Domänencontrollern (DC) nicht mehr funktioniert. Da das Schema für die Gesamtstruktur gültig ist und nicht nur domänenweit, sind alle Domänen von Änderungen und Fehlern betroffen. Weil Schemaänderungen keine alltägliche administrative Aufgabe darstellen, empfiehlt Microsoft, diese Gruppe stets leer zu lassen und nur bei geplanten Modifikationen am Schema Mitglieder in die Gruppe aufzunehmen. Der Schutz vor ungeplanten Änderungen, versehentlich oder nicht, ist somit gewährleistet.

Auch bei der Verwendung der anderen Built In-Gruppen im Active Directory gilt die Empfehlung, Vorsicht bei der Erteilung administrativer Privilegien walten zu lassen. Wie aus der Beschreibung der beiden Gruppen der Organisations-Admins und Domänen-Admins zu erkennen ist, besitzen sie weitreichende Berechtigungen zur Administration der Domäne oder der Gesamtstruktur. Es ist wichtig zu verstehen, dass die Domänen-Admins in der Lage sind, in ih-

Built In-Gruppen		
Gruppe	**Bemerkungen**	**Rechte**
Administratoren		Administratoren haben Vollzugriff auf Domänencontroller der Domäne. Die Administratorengruppe hat "Organisations-Admins" und "Domänen-Admins" als Mitglieder.
Benutzer	Alle neu erstellten Accounts sind (indirekte) Mitglieder der Gruppe "Benutzer".	Benutzer sind in der Lage, den lokalen Computer zu bedienen. Sie können Applikationen starten, den Computer herunterfahren und persönliche Einstellungen vornehmen. "Authentifizierte Benutzer" und das Prinzipal "Interaktiv" sind Mitglieder dieser Gruppe.
Sicherungs-Operatoren	Die Gruppe hat per Vorgabe keine Mitglieder.	Sicherungsoperatoren dürfen sich an Domänencontrollern lokal anmelden und alle Ordner und Dateien sichern und wiederherstellen. Sie dürfen außerdem das System herunterfahren.
Konten-Operatoren	Die Gruppe hat per Vorgabe keine Mitglieder.	Konten-Operatoren dürfen sich an Domänencontrollern lokal anmelden und – falls gewünscht – herunterfahren. Sie können Benutzer- und Computerkonten sowie Gruppen in Containern und OUs der Domäne erstellen, ändern und löschen (gilt nicht für administrative Gruppen und Konten und die OU "Domänencontroller").
Erstellung eingehender Gesamtstrukturvertrauensstellungen	Die Gruppe hat per Vorgabe keine Mitglieder und steht nur in der Forest-Root-Domäne zur Verfügung.	Mitglieder der Gruppe können eingehende Einweg-Vertrauensstellungen für die Gesamtstruktur erstellen und verwalten.
Netzwerkkonfigurations-Operatoren	Die Gruppe hat per Vorgabe keine Mitglieder.	Netzwerkkonfigurations-Operatoren können die TCP/IP-Einstellungen an Domänencontrollern verändern.
Systemmonitorbenutzer	Die Gruppe hat per Vorgabe keine Mitglieder.	Mitglieder dieser Gruppe können Leistungsindikatoren von Domänencontrollern ansehen und auswerten (auch von Remote).
Leistungsprotokoll-benutzer	Die Gruppe hat per Vorgabe keine Mitglieder.	Mitglieder dieser Gruppe können Leistungsindikatoren auf Domänencontrollern erstellen (auch von Remote).
Prä-Windows 2000-kompatibler Zugriff		Diese Gruppe existiert für die Abwärtskompatibilität mit Windows NT4-Computern.
Druck-Operatoren	Die Gruppe hat per Vorgabe keine Mitglieder.	Druck-Operatoren können an Domänencontroller angeschlossene Drucker verwalten. Sie sind außerdem in der Lage, AD-Druckerobjekte zu erstellen, zu verwalten und zu löschen. Sie dürfen sich an Domänencontrollern anmelden und DCs herunterfahren.
Remotedesktopbenutzer	Die Gruppe hat per Vorgabe keine Mitglieder.	Remote Desktop-Benutzer können sich remote auf Domänencontrollern anmelden.
Replikationsoperator	Die Gruppe hat per Vorgabe keine Mitglieder.	Diese Gruppe darf Replikationsfunktionen von Domänencontrollern kontrollieren. Sie wird vom File Replication Service (FRS) genutzt.
Server-Operatoren	Die Gruppe hat per Vorgabe keine Mitglieder.	Server-Operatoren dürfen sich an Domänencontrollern interaktiv anmelden und sind in der Lage, Backups zu erstellen und sie zurückzuspielen, Festplatten neu zu formatieren, Freigaben zu erstellen, Dienste zu starten und zu stoppen und Betriebssystemkonfigurationen vorzunehmen.

Gruppen im Users-Container		
Gruppe	**Bemerkungen**	**Rechte**
Organisations-Admins	Diese Gruppe steht nur in der Forest-Root-Domäne zur Verfügung. Sie enthält per Vorgabe keine Mitglieder außer dem Administrator.	Organisations-Admins haben weitreichende Berechtigungen im ganzen Forest. Sie sind Mitglied jeder "Administratoren"-Gruppe jeder Domäne der Gesamtstruktur. Organisations-Admins können somit die Gesamtstruktur kontrollieren.
Domänen-Admins	Diese Gruppe enthält per Vorgabe keine Mitglieder außer dem Administrator.	Domänen-Admins haben Vollzugriff auf alle Domänencontroller der Domäne sowie Administrator-Berechtigungen auf allen Mitgliedsrechnern der Domäne. Domänen-Admins sind Mitglied der Gruppe "Administratoren" ihrer Domäne.
Schema-Admins	Diese Gruppe steht nur in der Forest-Root-Domäne zur Verfügung. Sie enthält per Vorgabe keine Mitglieder außer dem Administrator.	Mitglieder dieser Gruppe sind in der Lage, das Active Directory-Schema zu verändern.

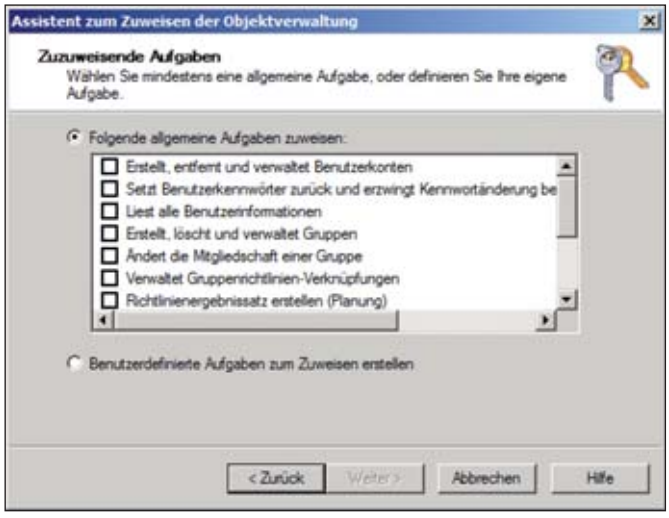


Bild 1: Der Delegationsassistent bietet Administratoren eine Vorauswahl von Aufgaben

rer Domäne alle Mitgliedsserver und Clientcomputer zu administrieren. Da sie beim Domänenbeitritt eines Computers zur lokalen Gruppe der "Administratoren" hinzugefügt werden, besitzen sie die Fähigkeit, alle Server, Computer und deren Dienste zu verwalten.

Ähnlich ist es mit den Organisations-Admins, die in jeder Domäne der Gesamtstruktur in der "Administratoren"-Gruppe Mitglied sind. Es ist ein Leichtes für sie, ebenfalls zu Domänen-Admins in anderen Domänen zu werden und dort ebenfalls Server und Clients zu verwalten. Nur Personen, die diese Berechtigungen für ihre tägliche Arbeit benötigen, sollten Mitglieder beider Gruppen sein. Hier gilt es als Empfehlung, mit Hilfe von Objektdelegation eigene Gruppen und Tätigkeiten zu erstellen, die auf das gewünschte Szenario passen.

Bei näherer Betrachtung anderer Built In-Gruppen, lässt sich feststellen, dass auch sie eine ganze Reihe von Berechtigungen besitzen, die für alltägliche Verwaltungsaufgaben sehr hoch gegriffen sind. Nicht in jeder Umgebung ist es gewünscht, dass Druckeradministratoren Domänencontroller herunterfahren dürfen oder Mitarbeiter mit Backupverantwortlichkeit Domänencontroller ausschalten und Backups ohne Rücksprache zurückspielen können. Die Nutzung der Vorgabegruppen ist demnach mit einer ähnlichen Vorsicht zu genießen wie die der Admin-Gruppen. Meist benötigen Helpdesk-Mitarbeiter zwar Rechte, Benutzerkonten zu editieren, jedoch sollten sie in der Regel nicht in der Lage sein, sich lokal an DCs anzumelden oder gar alle Benutzerkonten des Verzeichnisses zu verwalten. Sollen Helpdesk oder Abteilungsadministratoren Rechte im Active Directory erhalten, ihnen jedoch keine Möglichkeit des Eingriffs in den Laufbetrieb des Verzeichnisses gegeben werden, drängt sich die Lösung der Rechtedelegation im Active Directory auf.

Rechte delegieren

Das AD bietet ein tiefgreifendes Delegationsmodell, mit dem Sie Benutzern und Gruppen bis auf Attribut-Ebene Berechtigungen zu AD-Objekten erteilen. AD-Objekte und ihre Attribute besitzen, ähnlich wie Dateien und Ordner im Dateisystem, eine Access Control List (ACL), die Zugriffe steuert und regelt. Bei Anpassung dieser Berechtigungen lässt sich nahezu jede Verwaltungsaufgabe delegieren. Die ACLs ändern Sie auf unterschiedliche Weisen:

- Mit "Active Directory-Benutzer und -Computer": Unter "Ansicht" aktivieren Sie die "Erweiterten Optionen". Anschließend befindet sich im Eigenschaftendialog jeder OU der "Sicherheit"-Tab.
- ADSIEdit: Im Eigenschaftendialog einer OU im Reiter "Sicherheit"
- Mit dem "Delegationsassistenten" in "Active Directory-Benutzer und -Computer", der im Kontextmenü beim Rechtsklick auf eine OU erscheint.

Den einfachsten Einstieg bietet sicher der Delegationsassistent, da er bereits vordefinierte Tätigkeitsfelder zur Auswahl bereithält. Administratoren können so anderen Gruppen per Knopfdruck notwendige Berechtigungen für bekannte Aufgaben delegieren.

Um einer AD-Gruppe Rechte für das Accountmanagement beispielsweise der OU "Stuttgart" zu gewähren, müssen Sie per Rechtsklick auf die Stuttgart-OU klicken und den Kontextmenüeintrag "Objektverwaltung zuweisen" auswählen. Der "Assistent zum Zuweisen der Objektverwaltung" öffnet sich somit. Der zweite Schritt des Assistenten, "Benutzer oder Gruppen", fordert Sie zur Auswahl der Ziel-Gruppe auf – im Beispiel die Helpdesk-Gruppe, die zusätzliche Rechte für diese OU erhalten soll. Der Assistent hat somit die zu delegierende OU und die Gruppe identifiziert – was fehlt, sind die Berechtigungen, die er erteilen soll. Im nächsten Schritt, "Zuzuweisende Aufgaben" geschieht genau dies: in diesem Schritt stehen Ihnen sowohl Standardtätigkeiten als auch die Möglichkeit, benutzerdefinierte Aufgaben zu erstellen, zur Auswahl. Die meisten zu delegierenden Tätigkeiten können Sie mit den im Dialog gezeigten Vorlagen erledigen, so dass eine eigene Aufgabendefinition selten notwendig sein sollte.

Reichen die vorgegebenen Aufgaben für die gewünschten Ziele nicht aus, erlaubt es Ihnen der Assistent, benutzerdefinierte Berechtigungen anzulegen. Bis auf Attributebene hinab können Sie mit dieser Methode Rechte für Objekte in der Ziel-OU definieren. Die Kenntnis der gewünschten Attributnamen, die Gegenstand der Delegation werden sollen, ist hier von Vorteil. Zudem ist es Voraussetzung, vor der Aufgabendelegation die "Erweiterte Features" in "Active Directory-Benutzer und -Computer" zu aktivieren. Erst dann lässt der Assistent es zu, einzelnen Attributen auf Zielobjekten Zugriff zu delegieren.

Nun starten Sie den Objektverwaltungsassistent erneut und geben wiederum die Zielgruppe für den Zugriff an. Im Schritt "Zuzuweisende Aufgaben" wählen Sie anschließend "Benutzerdefinierte Aufgaben zum Zuweisen erstellen" aus. Per Klick auf

"Weiter" lässt der Assistent die Auswahl des Zugriffsbereichs zu. Der Klick auf "Diesem Ordner, bestehenden Objekten in diesem Ordner und neuen Objekten in diesem Ordner" berechtigt die Zielgruppe zur Verwaltung aller Objekttypen in der Ziel-OU. Sollen Mitarbeiter nur bestimmte Objekte verwalten dürfen, ist "folgende Objekten im Ordner" die richtige Option. Hier wählen Sie die AD-Objekttypen aus, die die Zielgruppe administrieren soll. Die im Folgenden erteilten Rechte finden dann nur auf den markierten Objekttypen Anwendung. Der Schritt "Berechtigungen" listet die möglichen Rechte auf, die der Zielgruppe erteilt werden können. Beim Klick auf "Allgemein", "Eigenschaftenspezifisch" und "Erstellen/Löschen der Berechtigungen von bestimmten untergeordneten Objekten" blendet der Assistent spezifische Berechtigungen ein- oder aus.

Ein weiteres Beispiel – diesmal für die Human Resource-Abteilung – zeigt, dass die Rechtevergabe mit dem Assistenten sehr einfach Schritt für Schritt erfolgen kann. Möchten Sie, dass die HR-Mitarbeiter Kontaktattribute wie Telefonnummer, Privatadresse, Faxnummer oder die Angestellten-ID von Mitarbeitern verwalten dürfen, die Sperrung der Benutzer oder das Zurücksetzen von Passworten jedoch weiterhin Aufgabe der Helpdesk-Mitarbeiter ist, müssen Sie eine eigene Objektdelegation anlegen. Der Gruppe HR-Mitarbeiter gestatten Sie folglich "Lesen"- und "Schreiben"-Berechtigung auf die Attribute "telephoneNumber", "streetAddress", "facsimileTelephoneNumber" und "employeeID".

Schutz für administrative Konten und Admin-Gruppen

Nachdem wir uns die Delegation von Rechten im vorherigen Abschnitt in Detail angeschaut haben, ist es jetzt notwendig, uns ein interessantes Szenario genauer anzusehen: Nehmen wir an, dass ein Benutzer namens "Peter" Mitglied der Gruppen "Server-Operatoren" und "Backup-Operatoren" ist und somit viel Verantwortung in der Domäne trägt. Peters Benutzerkonto ist in der OU Stuttgart, auf die die Helpdesk-Gruppe Rechte besitzt, um Benutzer- und Computerkonten zu verwalten. Mitarbeitern des Helpdesks ist es gestattet, Änderungen an Benutzerkonten vorzunehmen und Passwörter, sollten Benutzer sie vergessen, zurückzusetzen. Durch diese Konfiguration entsteht eine Situation, in der sich Helpdesk-Mitarbeiter über die "Passwort zurücksetzen"-Funktion Zugriff auf Peters Benutzerkonto verschaffen können und so Server und Backups kontrollieren und Schaden an Domänencontrollern oder Mitgliedsservern anrichten können.

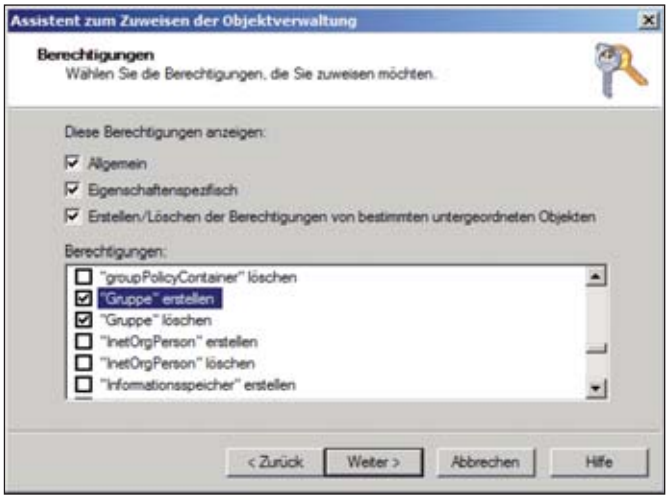


Bild 2: Eigene Berechtigungen erstellen und delegieren Sie mit der Auswahl von Attributen

Um diesem und ähnlichen Problemen entgegenzuwirken, besitzt das Active Directory einen Aufräumprozess, der für die Sicherheit privilegierter Gruppen und ihrer Mitglieder sorgt: der AdminSDHolder-Prozess. Der Prozess besitzt diesen Namen, weil er auf einem AD-Objekt beruht, dem AdminSDHolder-Objekt der Domänenpartition CN=AdminSDHolder,CN=System, DC=contoso, DC=com. Der Prozess ist simpel: In einem Zyklus von 60 Minuten wird auf dem PDC-Emulator-Domänencontroller ein Dienst gestartet, der für jede zu schützende Gruppe alle Gruppenmitgliedschaften rekursiv durchläuft und die Mitgliedskonten – seien es Benutzer, Computer oder Gruppen – auf die gesetzten Berechtigungen prüft. Mit "rekursiv" ist gemeint, dass der Prozess nicht nur direkte, sondern auch indirekte Mitgliedschaften durch ineinander verschachtelte Gruppen durchsucht. Dabei prüft er sowohl Sicherheits- als auch Verteilergruppen.

Findet der Prozess Objekte, deren gesetzte Berechtigungen nicht den vorgeschriebenen Sicherheitsberechtigungen entsprechen, modifiziert er sie wie folgt:

- Der Prozess setzt die Sicherheitsberechtigungen (ACL) zurück und gleicht die ACL der des AdminSDHolder-Objektes im "System"-Container der Domäne an. Die AdminSDHolder-ACL wird kopiert. Das Objekt besitzt anschließend die gleichen ACLs wie das AdminSDHolder-Objekt.
- Die Vererbung der Sicherheitsberechtigungen übergeordneter Objekte wird deaktiviert.
- Das Attribut "adminCount" des Objektes wird mit dem Wert "1" versehen.

Mit dem Deaktivieren der Vererbung und dem Setzen restriktiver Berechtigungen schützt das AD privilegierte Benutzer. Die Helpdesk-Mitarbeiter haben demzufolge maximal 60 Minuten Zeit, nämlich bis zum nächsten Durchlauf des AminSDHolder-Prozesses, um Schabernack mit Peters Benutzerkonto zu treiben. Danach wird die Berechtigung angepasst, so dass sie keinen Zugriff mehr darauf haben.

Bekanntschaft mit dem AdminSDHolder machen viele Administratoren erst, wenn auf wundersame Weise die Berechtigungen und Anpassungen an Accounts verschwinden – auch nach mehrmaligem Konfigurieren. Auch dies ist die Kennzeichnung des AdminSDHolder-Prozesses, obwohl sein Verhalten an dieser Stelle nicht gewünscht ist. Erkennbar ist der Pro-

zess am adminCount-Attribut, das er bei den betroffenen Konten auf "1" setzt.

Zur Anzeige und Überprüfung der vom AdminSDHolder geschützten Benutzer und Gruppen verwenden Sie folgendes Kommando, das die entsprechende Objekte anzeigt, die den adminCount mit Wert "1" besitzen (die Tabelle "Durch AdminsSDHolder geschützte Gruppen" zeigt Ihnen, welche Gruppen per Default geschützt werden):

```
dsquery * -filter "&(|(object
  Category=user)(objectCategory=
  group))(adminCount=1)"
```

Entfernen die AD-Verwalter Peter zu einem späteren Zeitpunkt aus den beiden geschützten Gruppen, wird auch der Aufräumprozess aufhören, Berechtigungen an seinem Benutzerobjekt anzupassen. Da der AdminSDHolder-Prozess sich jedoch nicht merkt, welche Objekte er bei jedem Lauf ändert, kann er seine Änderungen nachträglich nicht zurückspielen. Aus diesem Grund werden Helpdesk-Mitarbeiter auch weiterhin keine administrativen Tätigkeiten an Peters Benutzerobjekt durchführen können, obwohl er nicht mehr in einer geschützten Gruppe Mitglied ist. Die Vererbung der Berechtigungen von übergeordneten Objekten müssen Sie manuell wieder aktivieren.

Durch AdminsSDHolder geschützte Gruppen

Windows 2000 bis SP4	Windows 2000 SP4 Windows Server 2003	Windows Server 2003 ab SP1	Windows Server 2008 und neuer
Administratoren	Administratoren	Administratoren	
Domänen-Admins	Administrator	Administrator	Administrator
Organisations-Admins	Konten-Operatoren	Konten-Operatoren	Konten-Operatoren
Schema-Admins	Sicherungsoperatoren	Sicherungsoperatoren	Sicherungsoperatoren
	Zertifikats-Veröffentlicher	Domänen-Admins	Domänen-Admins
	Domänen-Admins	Domänencontroller	Domänencontroller
	Domänencontroller	Organisations-Admins	Organisations-Admins
	Organisations-Admins	Krbtgt	Krbtgt
	Krbtgt	Druck-Operatoren	Druck-Operatoren
	Druck-Operatoren	Schema-Admins	Schema-Admins
	Schema-Admins	Server-Operatoren	Server-Operatoren
			Read-Only Domänencontroller

Gruppenmitgliedschaft in verwaltenden Gruppen schützen

Neben dem AD-eigenen Aufräummechanismus gibt es weitere Möglichkeiten für Administratoren, Verwaltungsgruppen zu schützen. Die Gruppenrichtlinien-Einstellungen der "Eingeschränkten Gruppen", die Administratoren zur Verwaltung von lokalen Gruppen auf Ziel-Clients nutzen, können Sie auch für den Schutz von Domänengruppen verwenden. Obwohl diese Variante nicht sehr weit verbreitet ist, ist sie ebenso effektiv wie das Kontrollieren von Client-Gruppen. Domänencontroller verarbeiten Gruppenrichtlinien per Vorgabe alle fünf Minuten, so dass geänderte Gruppenmitgliedschaften schnell vom System rückgängig gemacht werden. Änderungen an Domänengruppen, wie etwa den "Domänen-Admins", lassen sich mit den eingeschränkten Gruppen verhindern, wenn ein Standard-Mitgliedschaftssatz per Gruppenrichtlinie definiert wird.

Hierzu verknüpfen Sie eine neue Gruppenrichtlinie wird mit der "Domänencontroller"-OU. Bei der Bearbeitung der GPO wählen Sie die Funktion "Eingeschränkte Gruppen" in "Computerkonfiguration / (Richtlinien) / Windows-Einstellungen / Sicherheitseinstellungen/ Eingeschränkte Gruppen" aus. Nach einem Rechtsklick und anschließender Auswahl von "Gruppe hinzufügen" fordert der Gruppenrichtlinien-Editor Sie zunächst auf, die Zielgruppe einzugeben. In diesem Schritt wählen Sie die zu schützende Domänengruppe "Domänen-Admins" oder "Server-Operatoren" aus. Im nächsten Schritt, "Domänenname / Gruppe Eigenschaften" müssen Sie die neuen Vorgabemitglieder der Gruppe definieren. Der korrekte Abschnitt hierfür ist "Mitglieder dieser Gruppe", in den der Editor per "Hinzufügen" neue Mitglieder einpflegt.

Es empfiehlt sich, die aktuellen Mitglieder der Domänengruppe zu studieren und eventuelle Standardmitglieder wie den Administrator oder die "Administratoren"-Gruppe ebenfalls in diesem Dialog hinzuzufügen. Die in den eingeschränkten Gruppen konfigurierte Liste von Mitgliedern wird aktuelle Mitglieder ersetzen. Nur die per GPO konfigurierte Benutzer, Computer und Gruppen werden in der Domänengruppe bleiben.

Es sei angemerkt, dass Microsoft diese Vorgehensweise nicht unterstützt. Das Forcieren der eingeschränkten Gruppen funktioniert nämlich auf jedem DC lokal und hat eine Replikationsschleife zur Folge. Wenn DC-1 die eingeschränkten Gruppen übernimmt, wird die Gruppenänderung an die anderen DCs repliziert, die daraufhin ebenfalls die Änderung der Gruppen anwendet. Anschließend werden weitere DCs die eingeschränkten Gruppen übernehmen, was erneut zu einem Replikationsaufkommen führt. Da Domänencontroller alle fünf Minuten eine GP-Aktualisierung durchführen, sind sie in größeren Netzwerken stets damit beschäftigt, die Mitgliedschaften zu aktualisieren – ein unnötiges Übel. Was bleibt, ist die Empfehlung, diese Konfiguration in kleinen Infrastrukturen durchzuführen und, falls möglich, die Gruppenrichtlinie der eingeschränkten Gruppen so per GP-Sicherheitsfilterung einzuschränken, dass nur ein DC die Änderungen übernimmt und nicht die gesamte "Domänencontroller"-OU. *(jp)*

Sicherheit und Delegation im Active Directory

Neue Machtverhältnisse

Die meisten Unternehmensnetze basieren auf einer Windows-Infrastruktur mit einer oder mehreren Active Directory-Domänen. Die mächtigsten Verwalter im Active Directory sind die Enterprise- und Domänenadministratoren. Obwohl es noch weitere vordefinierte Verwaltungsrollen gibt, empfiehlt es sich in Unternehmen, eigenen Rollen je nach Aufgabenbereich zu definieren und einzurichten. Zum Beispiel lässt sich die Pflege von Telefonnummern dem Administrator der Telefonanlage übertragen, ohne ihm weitere Rechte zu geben. Zur Umsetzung der Delegation bietet das Active Directory umfangreiche Möglichkeiten. In diesem Workshop ermitteln wir zunächst, welche Berechtigungen delegiert werden sollten und setzen die Neuverteilung der Rechte – nach intensivem Test – praktisch um.

Quelle: AKS – Fotolia.com

Anstatt allein das gesamte Netzwerk zu administrieren, sollte der IT-Verantwortlich die Last auf viele Schultern verteilen

Zunächst müssen wir uns mit einigen Grundlagen bezüglich des Sicherheitsmodells von Windows auseinandersetzen. Wenn wir die Delegation im Active Directory betrachten, wollen wir im Allgemeinen einem "normalen Benutzerkonto" zusätzliche administrative Rechte einzuräumen. Dazu ist wichtig zu verstehen, wie ein Benutzerkonto seine Berechtigungen erhält und wie der Zugriff auf Ressourcen (wie Active Directory-Objekte, Dateien, Drucker et cetera) funktioniert.

Das Windows-Sicherheitsmodell

Alles beginnt mit der Anmeldung des Benutzers. Gibt der Benutzer den Namen seines Benutzerkontos und sein Passwort in die Anmeldemaske ein, wird beides an einen Domänencontroller (DC) übermittelt. Der DC überprüft nicht nur, ob die Benutzernamen/Passwort-Kombination stimmt, sondern stellt auch einen "Token" für den Benutzer zusammen. Dieser Token enthält die Security-Identifier (SIDs) des Benutzers, SIDs bisheriger Benutzerkonten (nach Migrationen) sowie die SIDs aller Sicherheitsgruppen, in denen der Benutzer direkt oder indirekt Mitglied ist. Sie können sich diese Liste mit dem Befehl *whoami /all* anzeigen lassen. Dieser Token wird dem Benutzer während der Anmeldung übermittelt, und im Folgenden bei jedem Ressourcenzugriff dem Zielsystem präsentiert.

Auf der anderen Seite wird Ressourcen wie Dateien oder Ordnern im NTFS-Dateisystem, Registrierungsschlüsseln und auch Objekten im Active Directory Berechtigungen zugeordnet. Dies geschieht über die Registerkarte "Sicherheit" die Sie in den Eigenschaften eines Objektes sehen (in "Active Directory-Benutzer und -Computer" nachdem Sie im Menü "Ansicht" die "Erweiterte Ansicht" eingeschaltet haben). Auf jeder Ressource wird die Liste mit den Berechtigungen gespeichert, die sogenannte Zugriffskontrollliste (Access Control List, ACL). Einfach gesagt ist es nur eine Tabelle mit SIDs von Benutzerkonten oder Gruppen sowie deren Zugriffsrechten.

Bei einem Zugriff auf eine Ressource vergleicht das Betriebssystem den Token des Benutzers mit der Zugriffskontrollliste. Das System vergleicht einfach die Liste der SIDs, die dem Benutzer zugeordnet sind (aus dem Token) mit der Liste der SIDs, die Berechtigungen auf der Ressource haben. Bei einer Übereinstimmung wird der definierte Zugriff gestattet oder verweigert.

Ursprung der Berechtigungen

Nehmen wir an, wir erstellen als Administrator ein neues Benutzerkonto. Zunächst gibt es im Schema des AD eine Beschreibung, welche Werte so ein Benutzerkonto haben muss (zum Beispiel Benutzernamen) und welche Werte es haben kann (etwa E-Mailadresse, Telefonnummer). Zusätzlich ist im Schema aber auch definiert, wie die standardmäßige Sicherheit auf einem Benutzerobjekt aussehen soll. Dies ist im Schema unter dem Attribut "defaultSecurityDescriptor" hinterlegt – das Format ist eine SDDL-Zeichenkette (Security Descriptor Definition Language [1]). Zu-

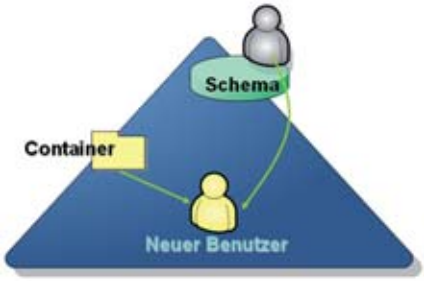


Bild 1: Die Berechtigungen eines neuen Objekts setzen sich aus den standardmäßigen Rechten, aus dem Schema sowie vererbten und expliziten Rechten zusammen

sätzlich wird das Benutzerkonto in einem Container (wie cn=Users,dc=..) oder einer Organisatorischen Einheit (Organizational Unit, OU) angelegt. Das Benutzerkonto erhält nicht nur die standardmäßigen Sicherheitseinstellungen aus dem Schema, sondern erbt auch die Berechtigungen von allen übergeordneten Containern, OUs oder dem Domänenobjekt auf oberster Ebene. Und zuletzt können nach dem Erstellen des Benutzerobjektes noch individuelle Sicherheitseinstellungen auf dem Objekt selber vergeben werden. Das neue Benutzerkonto umfasst also standardmäßige Sicherheitseinstellungen, vererbte Sicherheitseinstellungen und außerdem explizit gesetzte Einstellungen.

Um die umfangreichen Möglichkeiten der Delegation zu verstehen, müssen wir uns auch damit auseinandersetzen, wie die Sicherheitseinstellungen aufgebaut sind.

Struktur der Sicherheitseinstellungen

Die Sicherheitseinstellungen werden intern im so genannten "ntSecurityDescriptor" des Objektes (in unserem Beispiel des Benutzerkontos) gespeichert. Beim Erstellen eines neuen Objektes wird also der Inhalt des defaultSecurityDescriptors aus dem Schema in den ntSecurityDescriptor kopiert, und weitere vererbbare Berechtigungen angewendet. Der ntSecurityDescriptor enthält einige Werte, die in diesem Kontext relevant sind:

- Owner: Der Besitzer des Objektes wird über seine SID gespeichert.
- Primary Group: Die primäre Gruppe des Besitzers wird mit ihrer SID gespeichert.
- Control: Dieser Wert gibt an, welche weiteren Optionen gesetzt sind und welche weiteren Eigenschaften existieren. Aus diesem Wert ist ersichtlich, ob DACL und/oder SACL (siehe unten) existiert, und ob die DACL oder SACL vor Vererbung von oben geschützt ist (also keine vererbten Berechtigungen übernimmt).

Die Discretionary Access Control List (DACL) und System Access Control List (SACL) sind weitere Strukturen, die in einem ntSecurityDescriptor enthalten sein können. Die DACL enthält die Berechtigungseinstellungen bezüglich der Berechtigungen auf einem Objekt (was jemand mit diesem Objekt machen darf), die SACL enthält die Überwachungseinstellungen (ob zum Beispiel eine Änderung eines bestimmten Wertes in der Sicherheits-Ereignisanzeige protokolliert werden soll). Im Weiteren beschäftigen wir uns vor allem mit der DACL, die SACL sieht aber im Prinzip genauso aus. Wie wir weiter oben gesehen haben, enthält der Wert "Control" im ntSecurityDescriptor die Information, ob eine DACL oder SACL existiert beziehungsweise ob diese von oben vererbte Sicherheitseinstellungen akzeptieren darf.

In der Datenstruktur der DACL sehen wir eigentlich nur die Anzahl der Access Control Entries (ACEs) im Wert "ACECount", sowie die einzelnen ACEs. Ein ACE ist eine weitere Datenstruktur, die die Berechtigung auf das Objekt selber festlegt. Wenn Sie nun auf der Registerkarte "Sicherheit" auf die Schaltfläche "Erweitert" klicken, sehen Sie die Berechtigungseinstellungen auf der Registerkarte "Berechtigung" und alle Eigenschaften der DACL. Die Berechtigungseinträge entsprechen den ACEs. Jeder Berechtigungseintrag setzt sich aus den folgenden Werten zusammen:

- Trustee: Definiert, für wen (SID) die Berechtigung festgelegt wird.
- ACEType: Wird ein Berechtigungseintrag für "Zulassen" oder "Verweigern" definiert, also der Zugriff erlaubt oder explizit verboten?
- ACEFlags: Legt fest, ob die ACE auf alle Objekte unterhalb in der Hierarchie vererbt oder nur auf direkt darunter liegende Berechtigungen oder nur auf das Objekt selber angewendet wird, beziehunsgweise ob ACE geerbt wurde.
- AccessMask: Definiert die in der ACE vergebenen Berechtigungen, wie Löschen oder Hinzufügen von darunterliegenden Objekten, standardmäßiger Lesezugriff, Vollzugriff, Schreibzugriff, Schreibzugriff auf bestimmte Eigenschaften und so weiter.
- Flags: Beschreibt, welche weiteren Werte existieren – ObjectType und/oder InheritedObjectType.
- ObjectType: Wenn das Recht vergeben wurde, Objekte hinzuzufügen oder zu löschen, oder nur bestimmte Eigenschaften zu lesen oder zu schreiben, enthält ObjectType den Global Unique Identifier (GUID) des Objektes oder Attributes im Active Directo-

Bild 2: Die Struktur der Sicherheitseinstellungen

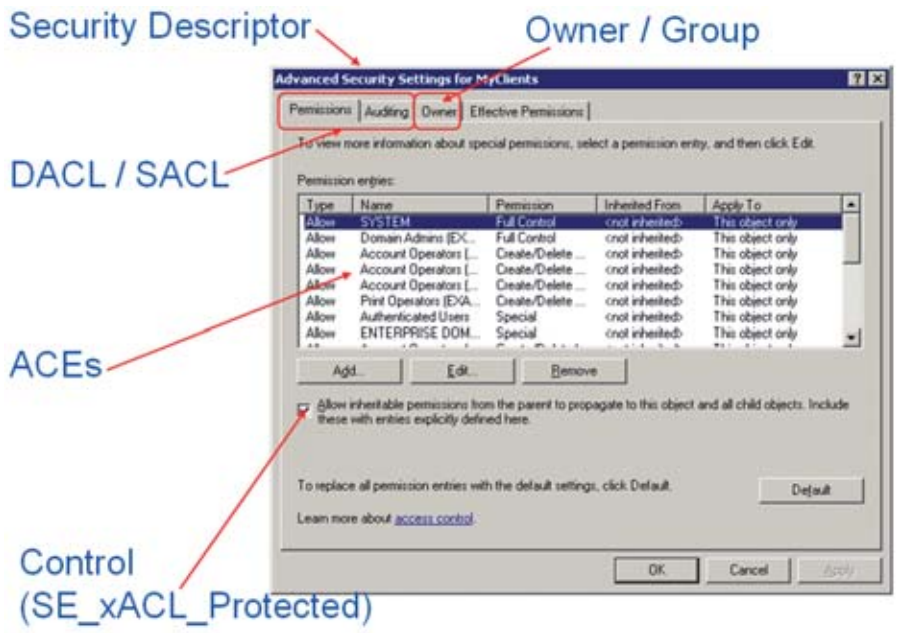


Bild 3: Die Registerkarte "Berechtigungen" enspricht der DACL ...

ry (Eigenschaft "schema-ID-GUID" im Schema).

- InheritedObjectType: Wenn die Vererbung nur für bestimmte Objekttypen eingestellt ist (zum Beispiel Benutzerkonten), enthält InheritedObjectType die GUID des Objektes.

Diese ganzen Werte klingen zunächst recht trocken, aber wenn wir uns damit auseinandersetzen, stellen wir fest, dass sowohl die Sicherheitsdialog- wie auch Kommandozeilen-Tools diese Werte wiedergeben. Sehen wir uns einmal ein Beispiel an: Wenn wir auf einer OU der Gruppe "Helpdesk" die Berechtigung geben möchten, die Mitgliedschaften aller darunter liegenden Gruppen zu ändern, werden einige Werte geändert und hinzugefügt:

- Owner, Primary Group bleibt bestehen.
- Control enthält den Wert, dass eine DACL existiert. Innerhalb der DACL wird eine neue ACE (Zugriffskontrolleintrag) erstellt. Diese erhält die SID der Gruppe Helpdesk als "Trustee".
- Im ACEType definieren wir eine Allow-ACE, also den Zugriff zulassen.
- In ACEFlags wird festgelegt, dass die Berechtigung auf alle darunterliegenden Objekte vererbt werden soll.
- Als nächstes kommt die AccessMask – diese wird den Wert "WRITE_PROPERTY" annehmen, was bedeutet, dass ein bestimmtes Attribut geschrieben werden soll.
- Und Flags legt fest, dass sowohl ObjectType wie auch InheritedObjectType gesetzt werden. ObjectType wird hierbei auf die GUID des Attributes "Member" gesetzt, da wir einen Schreibzugriff auf dieses Attribut zulassen wollen. InheritedObjectType wird auf die GUID des Objektes "Gruppe" gesetzt.

Damit sind schon alle Werte gesetzt und wir haben Schreibzugriff auf Member-Attribute von allen Gruppen unterhalb der OU für die Gruppe Helpdesk definiert.

Rollenbasierte Administration planen

Rollenbasierte Administration ist nicht nur ein "Hypewort" der letzten Jahre, sondern sollte tatsächlich in allen Unternehmen implementiert werden. Sowohl die steigende Komplexität der Systeme, Anforderungen nach Revisions- und Überwachungsrichtlinien, sowie Sicherheitsanforderungen erfordern, dass Administratoren, Mitarbeiter von Benutzerhelpdesks und vor allem Servicekonten mit den geringsten Rechten ausgestattet sind, die für ihre jeweiligen Aufgaben notwendig sind.

Viele Unternehmen haben wesentlich mehr Domänenadministratoren als notwendig. Manche Unternehmen setzen dann die Sicherheitsgruppe Kontenoperatoren (Account Operators) ein, aber auch diese hat ein deutliches Manko: Sie erhält (per Definition im Schema) die Rechte zum Erstellen, Löschen und Verändern von Benutzerkonten, Gruppen,

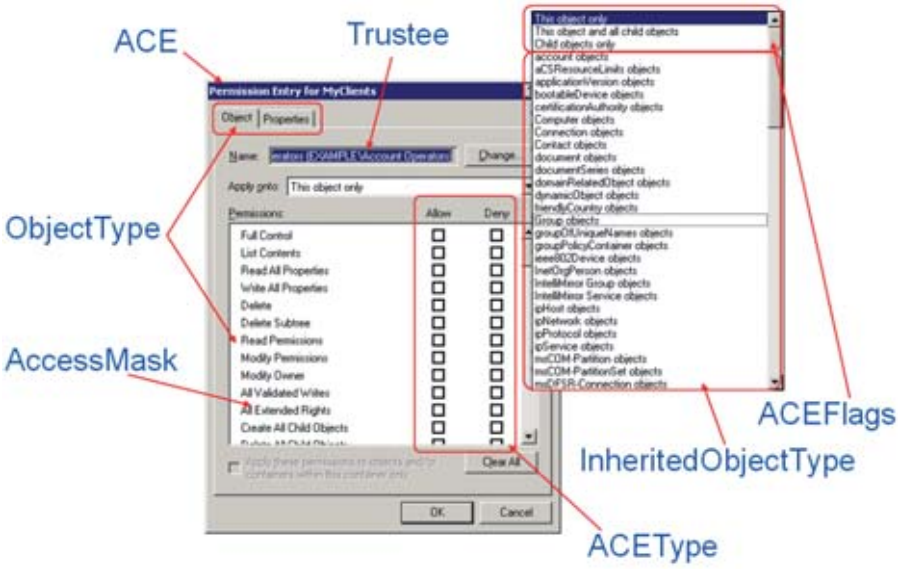


Bild 4: ... die "Berechtigungseinträge" den Access Control Entries (ACEs)

Bild 5: Selbst die Kontenoperatoren sollten nicht verwendet werden, da sie zu viele Berechtigungen haben …

Bild 6: … besser ist es, eigene Kontenoperatoren zu erstellen

Computern und iNetOrgPerson-Objekten, und das auf jeder OU. Häufig erstellen die Unternehmen aber ein OU-Modell, das primär die administrative Struktur reflektiert und sekundär zum Verlinken von Gruppenrichtlinien verwendet werden sollte. Meistens – und das ist auch sehr gut so – stehen dann Benutzerkonten und Computerkonten in verschiedenen OUs. Ein Kontenadministrator könnte aber, aus Versehen oder absichtlich, neue Objekte dort erstellen, wo sie per Definition gar nicht sein sollten (zum Beispiel ein Benutzer in der Computer-OU und umgekehrt – Gruppenrichtlinien sind damit dann ausgehebelt). Sollte es eine Support-Gruppe im Unternehmen geben, die sowohl Benutzer-, Gruppen- wie auch Computerkonten verwaltet, ist es besser, eine eigene Berechtigungsgruppe hierfür zu erstellen und dieser die Rechte auf den entsprechenden OUs zu geben: Erstellen, Löschen und Vollzugriff auf Benutzerobjekte und gleiches für Gruppen und Computer.

Des Weiteren empfiehlt es sich, eine OU vorzuhalten, in der keine Delegation passiert. Hierunter legen Sie dann die Objekte an, die nur von Domänenadministratoren verwaltet werden sollen und nicht von delegierten Administratoren, wie zum Beispiel die Berechtigungsgruppen für die AD-Delegation.

Ein Weg um festzustellen, wie viele Konten in Ihrem Unternehmen durch standardmäßige Gruppen wie Domänenadmins oder Konten-Operatoren hohe Rechte erhalten, ist der folgende Befehl:

```
dsquery * domainroot -filter "
  (&(objectCategory=Person)(object
  Class=User)(adminCount>=1))" |
  find /c /I "dc="
```

Damit erhalten Sie die Anzahl von Accounts, die über eine der standardmäßigen Gruppen administrative Rechte erhalten. Grundsätzlich sind dies nur zwei Accounts, der lokale Administrator und der KRBTGT-Account. Sollte hier eine ungewöhnlich hohe Anzahl an Konten stehen, dann sollten Sie über eine delegierte Administration nachdenken, da die Default-Gruppen für viele Aufgaben zu hohe Berechtigungen haben.

Administratoren in Unternehmen, die über die Einführung rollenbasierter Administration nachdenken, haben häufig Angst, dass ihnen Rechte genommen werden. Jedoch ist es meistens so, dass für viele Aufgaben keine Domänenadministrator-Rechte benötigt werden. Und die Rolle des Domänenadministrators bringt eine Menge Verantwortung mit sich: Fehler können fatale Folgen für das Unternehmen haben; wenn beim Internet-Surfen oder beim Lesen von E-Mails das Domänenadministrator-Konto verwendet wird, können Viren, Trojaner und Würmer wesentlich leichter in das Unternehmen eindringen. Wenn darüber hinaus unsichere und zu kurze Passwörter verwendet werden, sind diese Konten unsicher und schnell zu knacken. Idealerweise sollten Mitarbeiter immer normale Benutzerkonten für die Anmeldung und Kommunikation nutzen, und die administrativen Konten nur zum Aufruf der Administrationswerkzeuge oder zum Einloggen an den Servern über Remote Desktop verwenden. Damit unterstreicht die Verantwortung von Domänenadministratoren die Implementierung administrativer Rollen. Aber welche Rechte muss der Mitarbeiter einer bestimmten Abteilung wirklich haben? Und welche Rechte braucht ein Dienstekonto?

Wenn es um die Rechte von administrativen Gruppen geht, hilft es, zunächst die Verantwortungen für die administrativen Aufgaben im Unternehmen zu klären und zu dokumentieren. Hierbei werden alle anfallenden Aufgaben gesammelt und dann festgelegt, welche Abteilung für diese verantwortlich ist. Dies geschieht zunächst unabhängig von der technischen Realisierbarkeit. Ist hierzu ein gemeinsamer Konsens gefunden, können Sie sich an die Arbeit machen und herausfinden, welche Rechte notwendig sind, um die Rollen zu implementieren. Hierbei hilft zum Beispiel das Dokument "Best Practices for Delegating Active Directory Administration" und dessen Anhang, oder eine Referenz, welche Felder in den Eigenschaften des Benutzerobjektes in "Active Directory-Benutzer und -Computer" welchen Attributen entsprechen [2,3,4].

Sie können aber auch mit anderen Mitteln herausfinden, welche Rechte Sie delegieren müssen. Erstellen Sie zum Beispiel einen Testbenutzer (am besten in einer Testumgebung) und führen dann die folgenden Kommandos aus (wobei "%server%" der Servername ist und "%dn%" der DistinguishedName des Objektes). Das erste Kommando gibt Ihnen alle Attributwerte eines Objektes zurück:

```
ldifde -s %server% -d %dn% -f
  file1.log
```

```
whenCreated: 20061115105030.0Z
whenChanged: 20061116100140.20115344.0Z
displayName: Joe Doe
uSNCreated: 16468
memberOf: CN=BCN-Users,OU=Barcelona,OU=Branch,OU=MyGroups,DC=example,DC=com
uSNChanged: 20622037
name: Joe Doe
objectGUID:: v1j94hNyvkahJ03Io0s7MQ==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 128084972042249648
lastLogoff: 0
lastLogon: 0
pwdLastSet: 128080614310475920
primaryGroupID: 513
userParameters::
 bTogICAgICAgICAgICAgICAgICAgIGQCTD1BbCAgICAgICAgICAgICAgICAgICAg
objectSid:: AQUAAAAAAAUVAAAAhRD1AIUQ5QCFEOUAUgQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: jdoe
sAMAccountType: 805306368
userPrincipalName: jdoe@example.com
lockoutTime: 128084972042249648
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
msNPAllowDialin: FALSE
```

Bild 7: Mit einem einfachen Skript und einer Software zum Vergleichen von Dateien zeigt die Schnittmenge aus Änderungen und Replikation, was delegiert werden muss

Dieses Kommando zeigt uns die Replikations-Metainformationen eines Objektes:

```
repadmin /showobjmeta %server% %dn%
  /nocache /linked > file1.log
```

Hiermit ermitteln Sie alle Berechtigungen auf einem Objekt:

```
dsacls \\%server%\%dn% > file1.log
```

Beachten Sie, dass Sie alle Kommandos gegen den gleichen Server ausführen, um sicherzugehen, dass Sie konsistente Daten erhalten. Danach ändern Sie den Testbenutzer und führen die Kommandos noch einmal aus, leiten die Ergebnisse jedoch in eine andere Datei. Jetzt haben Sie zwei Textdateien, in denen jeweils die Attribute des Objektes und deren Werte stehen, die Replikationsinformationen sowie die Berechtigungen. Vergleichen Sie jetzt die zwei Textdateien – zum Beispiel mit CSDiff von Componentsoftware [5] – können Sie feststellen, was Sie delegieren müssen. Dies sind normalerweise die Attribute, die sich geändert haben und repliziert werden (es gibt auch Attribute, die lokal vom Domänenkontroller verwaltet werden, wie zum Beispiel "whenChanged"). Liegen Änderungen im letzten Teil (dsacls) vor, müssen Sie hierfür zusätzlich Berechtigungen vergeben, die erlauben, die Berechtigungen zu ändern.

Setzen von Berechtigungen

Betrachten wir zunächst einmal die Möglichkeiten, Berechtigungen zu vergeben, die sicherlich jeder IT-Administrator kennt: direkt über die grafische Benutzeroberfläche. Berechtigungen für Delegation im Active Directory können Sie direkt über "Active Directory-Benutzer und -Computer" setzen. Schalten Sie zunächst die Anzeige der "Erweiterten Funktionen" (im Menü "Ansicht") ein. Jetzt können Sie mit der rechten Maustaste auf eine OU klicken, unter der Sie Berechtigungen delegieren wollen, und den Menüpunkt "Objektverwaltung zuweisen" wählen. In diesem Assistenten wählen Sie zunächst die Gruppe aus, der Sie Berechtigungen geben wollen. Auf der nächsten Seite des Assistenten können Sie allgemeine Aufgaben (Tasks) wie das Verwalten von Benutzerkonten delegieren, oder alternativ "Benutzerdefinierte Tasks" erstellen. Bei "Benutzerdefinierten Tasks" werden Sie dann noch gefragt, welche Objekttypen Sie delegieren wollen und anschließend, welche Attribute. Daher lassen sich bereits hier sehr detailliert Berechtigungen vergeben, zum Beispiel nur die Pflege der Mitglieder von Gruppenobjekten ("member"-Attribut schreiben).

Was vielen oft aber unklar ist: Der Menüpunkt "Objektzugriff verwalten" ist lediglich ein Assistent für den Sicherheits-Dialog in den Objekteigenschaften. Im Assistenten sehen Sie daher nicht, was bereits delegiert wurde. Allerdings sollten Sie sowieso den Sicherheits-Dialog bevorzugen. Hier können Sie sowohl die Berechtigungen einsehen als auch ändern. Gewöhnen Sie sich vor allem an den "Erweiterten Dialog", der sehr hilfreich ist, um den ntSecurityDescriptor zu verstehen.

Natürlich lassen sich Berechtigungen auch scripten. Am einfachsten geht das über das Kommandozeilentool *dsacls*, womit Sie Berechtigungen lesen oder setzen. Hier einige Beispiele (weitere Hilfe erhalten Sie mit dem Befehl *dsacls /?*). Das folgende Kommando liest alle Berechtigungen auf der OU "MyUsers":

```
dsacls "ou=MyUsers,dc=firma,dc=de"
```

Mit dem nächsten Kommando geben wir der Gruppe Helpdesk das Recht, Benutzerkonten unterhalb der OU "MyUsers" zu entsperren, wenn diese Ihr Passwort zu häufig eingegeben haben:

```
dsacls "ou=MyUsers,dc=firma,dc=de"
  /G
  firma\Helpdesk:WP;lockoutTime;user
  /I:S
```

Und mit dem folgenden Befehl geben wir der Gruppe Helpdesk das Recht, Gruppenmitgliedschaften unterhalb von "MyGroups" zu pflegen:

```
dsacls "ou=MyGroups,dc=firma,dc=de"
  /G firma\Helpdesk:WP;member;group
  /I:S
```

Hierbei bedeutet der Parameter "/G", dass Berechtigungen zum "Zulassen" gesetzt

werden. Die Parameter danach definieren im Format "gruppe:berechtigung;attribut;objekt", was genau berechtigt werden soll. Gruppe (kann auch ein Benutzerkonto sein) stellt dar, für wen die Berechtigung gelten soll (Trustee), danach steht die Berechtigung. In dem vorliegenden Beispiel steht "WP;lockouttime" für Schreibzugriff auf dem Attribut lockouttime. Und am Schluss steht noch der Objekttyp, auf den die Berechtigung gilt beziehungsweise vererbt werden soll. Für die Vererbung ist noch der Parameter "/I:S" notwendig, der festlegt, dass die Berechtigung nur auf darunterliegenden Objekte und nicht auf die OU selber angewendet wird (eine OU kann sich ja schlecht aussperren).

Dies waren zwei Beispiele für die Pflege von Attributen in Objekten. Natürlich können Sie mit *dsacls* auch das Erstellen und Löschen von Objekten delegieren, zum Beispiel über den folgenden Befehl:

```
dsacls "ou=MyUsers,dc=firma,dc=de"
  /G firma\Helpdesk:CCDC;;user /I:T
```

Hier vergeben wir das Recht, Benutzerobjekte zu erstellen und zu löschen (Create Child, Delete Child; es sind keine Attribute angegeben, aber der Objekttype "user"). Die Vererbung ist hier angegeben auf "Dem Objekt selber und darunter liegenden Objekten".

Wenn Sie einmal Berechtigungen zurück setzen möchten, verwenden Sie die Parameter "/S" und gegebenenfalls "/T" (für mehrere Objekte). Auch interessant ist es, einen Teil der Objektverwaltung durch die Benutzer selber erledigen zu lassen. Wenn Sie ein Recht für die Gruppe "Self" auf einem Benutzer- oder Computerobjekt delegieren, kann der Benutzer bestimmte Eigenschaften selber ändern.

Rollenbasierte Administration testen und implementieren

Wenn Ihnen klar ist, welche Rollen Sie im Unternehmen implementieren wollen, welche Rechte Sie dafür benötigen und wie Sie diese Rechte delegieren, können Sie sich an das Testen und Implementieren machen. Zunächst sollten Sie ein Skript mit den Berechtigungen für jede Rolle entwerfen, dies setzt sich einfach aus den dsacls-Kommandos des vorigen Abschnittes zusammen. Als nächstes müssen Sie diese Berechtigungen testen. Dies erfolgt am besten in einer Testumgebung, die die gleiche OU-Struktur aufweist wie die Produktion. Hierfür können Sie zum Beispiel Skripte verwenden, die in der Gruppenrichtlinienverwaltungskonsole (GPMC) enthalten sind. Diese sind seit Windows Server 2008 ausgelagert in das Scriptcenter [6].

Und es gibt einen weiteren Aspekt, warum Sie die Delegation testen müssen: So müssen Sie nach dem Entwerfen der Rollen nicht nur überprüfen, ob Sie die angeforderten Berechtigungen setzen können, sondern auch, ob die Administrationsoberflächen mit den delegierten Berechtigungen zurechtkommen. Bei manchen Eigenschaften, die zwar von "Active Directory-Benutzer und -Computer" geschrieben werden können, hat die Oberfläche mit den delegierten Berechtigungen Probleme. Diese Werte können Sie dann nur über *ADSIEdit.msc*, *LDP.exe* oder andere Tools ändern. Hier ein Lichtblick: Mit der Verwaltungskonsole "Active Directory-Benutzer und -Computer" seit Windows Server 2008 ist der "Attribut Editor" aus *ADSIEdit* auch Bestandteil dieser Konsole – Sie müssen hierfür lediglich die "Erweiterten Eigenschaften" in der Ansicht einschalten. Eine weitere Methode besteht darin, eigene Skripte für dieses Aufgaben zu entwerfen.

Daher ist die Testphase so wichtig. Implementieren Sie zunächst die Rollen, testen Sie Ihre Delegationsskripte und überprüfen Sie dann, ob diese mit einem Benutzer mit den limitierten Berechtigungen tatsächlich auch die Aufgaben wahrnehmen können, die delegiert wurden. Achten Sie auf Ihre OU-Struktur – mischen Sie nicht administrative und nicht-administrative Konten in den gleichen OUs. Ansonsten müssen Sie damit rechnen, dass die administrativen Konten die delegierten Berechtigungen wieder verlieren [7].

Fazit

Das Implementieren rollenbasierter Administration ist ein wichtiges Thema, das in jedem Unternehmen ernst genommen werden muss. Zum einen sollten nur so wenig Administratoren wie notwendig über höhere Rechte wie etwa die Domänenadministratoren verfügen, zum anderen ist es wichtig, dass besonders Dienstkonten nur mit den notwendigen Rechten arbeiten. Zudem müssen die Rollen zunächst geplant, die Realisierbarkeit erprobt und vor allem die Implementierung und die administrativen Benutzeroberflächen getestet werden. Und denken Sie daran, die Änderungen an den Systemen zu dokumentieren. Aber gut geplante und implementierte Berechtigungen sind eine Erleichterung für jeden administrativen Mitarbeiter, da klar ist, wer welche Eigenschaften ändern kann und welche Gruppen für welche Änderungen verantwortlich sind. *(jp)*

[1] **Security Descriptor Definition Language**
http://msdn.microsoft.com/library/en-us/secauthz/security/security_descriptor_definition_language.asp

[2] **Best Practices for Delegating Active Directory Administration**
www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3

[3] **Best Practices for Delegating Active Directory Administration Appendices**
www.microsoft.com/downloads/details.aspx?FamilyID=29dbae88-a216-45f9-9739-cb1fb22a0642

[4] **User Interface Mappings in Active Directory Domain Services**
http://msdn.microsoft.com/library/en-us/ad/ad/user_interface_mappings_in_active_directory_domain_services.asp

[5] **CSDiff von Componentsoftware**
www.componentsoftware.com/products/CSDiff/index.htm

[6] **VBS-Scripting-Beispiel für Berechtigungen**
www.windowsserverfaq.de/faq/CompACLs.asp

[7] **Informationen zum AdminSDHolder**
http://msmvps.com/blogs/ulfbsimonweidner/archive/2005/05/29/49659.aspx

Links

Managed Service Accounts

Dienstekonten autonom

Dienstekonten werden in allen Unternehmen eingesetzt und besitzen häufig höhere Rechte als andere Konten. Trotzdem fehlen vielerorts die Prozesse, um deren Passwörter regelmäßig zu ändern. Windows Server 2008 R2 geht mit den "Managed Service Accounts" einen neuen Weg, um die Infrastruktur sicherer zu gestalten.

Ob Datensicherung, gespeicherte Aufgaben, Softwareverteilung, Monitoring-Agenten, Webserver-Applikationspools oder Datenbankserver – jedes Unternehmen nutzt zahlreiche Anwendungen, sei es zur Verwaltung und dem Schutz der Infrastruktur oder Anwendungen für das eigentliche Geschäft. Häufig kommen dabei Dienstekonten zum Einsatz, damit die Server systemübergreifend kommunizieren können. Und häufig benötigen diese Dienstekonten erhöhte Rechte für Vollzugriffe auf Datenbanken oder zur Sicherung von Daten. Dieses Konzept ist jedoch nicht auf die Serverwelt und das sichere Rechenzentrum beschränkt, sondern findet mitunter auch auf Clients Anwendung.

Quelle: pmphoto – Fotolia.com

Da Dienstekonten häufig höhere Rechte besitzen, sollten sie auch besser geschützt werden als normale Benutzerkonten. Dies bedeutet dann auch, dass Sie möglichst sichere Passwörter verwenden sollten sowie die Prozesse zum wechseln dieser Passwörter im Unternehmen definieren und regelmäßig anwenden. Leider ist dies nicht immer ganz einfach: Während Sie als Administrator die Auswirkung von Passwortänderungen eines Benutzerkontos absehen können, gestaltet sich dies bei Servicekonten umso schwieriger, desto häufiger sie zum Einsatz kommen. Wer möchte schon, dass die Datenbankreplikation eines kritischen SQL-Servers, ein hochverfügbarer Cluster-Dienst oder Exchange nicht mehr funktioniert, nur weil das Servicekonto-Passwort nicht im richtigen Ablauf geändert wurde? Daher ist gerade bei dieser Thematik die altbekannte Devise "Never touch a running System" zu beobachten.

Häufig werden auch bekannte oder berechenbare Passwörter eingesetzt – sei es, dass alle Dienstekonten das gleiche Kennwort besitzen oder, dass ein Konto namens "srv_Backup" dann das Passwort "srv_Backup01!" erhält und das gleiche Schema über sämtliche Dienstekonten hinweg zum Einsatz kommt.

Häufig sind Dienstekonten auch mehreren Administratoren bekannt und werden manchmal sogar für die Administration missbraucht. Um hier für mehr Sicherheit zu sorgen, sollten Sie zumindest zufällig generierte, ausreichend lange Passwörter verwenden und diese in einem Password-Safe wie KeyPass oder eWallet speichern. Microsoft bietet mit Windows 7 und Windows Server 2008 R2 nun eine Lösung für derartige Problematiken an: Managed Service Accounts (kurz MSA).

Bild 1: Ein Managed Service Account wird in drei Schritten erstellt, zugewiesen und der Dienst eingerichtet

Managed Service Accounts

Die Managed Service Accounts verwalten ihre Passwörter selbst. Dies ist vergleichbar mit einem Computerkonto, das auch über ein Passwort verfügt und dieses schon in den Betriebssystemen der vergangenen Jahre (solange es das Domänen-Konzept gibt) eigenständig verwaltet. Hierbei werden sehr lange Passwörter verwendet, die zufällig generiert und in regelmäßigen Abständen (spätestens alle 30 Tage) geändert werden. Beim Managed Service Account verwaltet der Computer, auf dem der dazugehörige Service eingerichtet ist, das Konto parallel zu seinem Computerkonto. Hierbei ändert er nicht nur das Passwort in der Domäne, sondern aktualisiert auch den Dienst, der dieses verwendet. Daher müssen Sie einige Punkte berücksichtigen, wenn Sie Managed Service Accounts verwenden:

- Zwischen dem MSA und dem Computer (Client oder Mitgliedsserver), der diesen verwaltet, besteht eine 1:1-Beziehung.
- Ein Managed Service Account kann nur einem einzigen Computer zugeordnet werden und nicht über mehrere Computer hinweg verwendet werden.
- Möchten Sie ein Servicekonto über mehrere Computer hinweg nutzen, ziehen Sie in Betracht, einen MSA pro Computer zu erstellen und diese dann in einer Gruppe zusammenzufassen.
- Dienste mit besonderen Berechtigungen müssen bekannt sein, um diese dann in einen MSA umzuwandeln.

Wann immer möglich, sollten Sie Managed Service Accounts gegenüber den traditionellen, manuell angelegten Dienstekonten bevorzugen. Prinzipiell sind MSAs auch nur reguläre Benutzerkonten, wie auch die klassischen Dienstekonten. Jedoch müssen Sie einen MSA einem bestimmten Domänenmitglied (oder auch DC) zuordnen, der den Account in Zukunft verwalten soll. Dies muss der Server sein, auf dem ein Dienst oder Webserver-Application Pool läuft, der den MSA verwenden soll. Es ist nicht möglich, MSAs einzusetzen, wenn der Service auf mehreren Systemen unter dem gleichen Konto laufen soll. Der Grund hierfür ist, dass der MSA ähnlich einem Computerkonto verwaltet wird: Meldet sich der Computer an der Domäne an, überprüft der Netlogon-Prozess, ob das Passwort des Computerkontos aufgrund seines Alters geändert werden sollte. Ist dies der Fall, fragt das Domänenmitglied bei seinem Domänencontroller an, ob die Änderung gerade gelegen käme oder ob dieser zu sehr unter Last steht. Da dies nur selten der Fall sein dürfte, wird er dann das Passwort ändern – genauso wie ein Benutzer ein Passwort manuell ändern würde. Hierbei erstellt er ein zufällig generiertes Passwort mit 127 Stellen, ändert das Domänenkonto des Computers und vermerkt in der lokalen Sicherheitsautorität das neue Passwort. Das System meldet sich daraufhin mit dem neuen Passwort an. Genau über den gleichen Prozess werden Managed Service Accounts geändert. Der Netlogon-Prozess überprüft lediglich zusätzlich, für welche MSAs er zuständig ist und ändert deren Passwörter mit. Außerdem überprüft er die lokalen Dienste und Application Pools, die dieses Konto verwenden und ändert das Passwort auch an dieser Stelle. Damit wird deutlich, warum MSAs nicht über un-

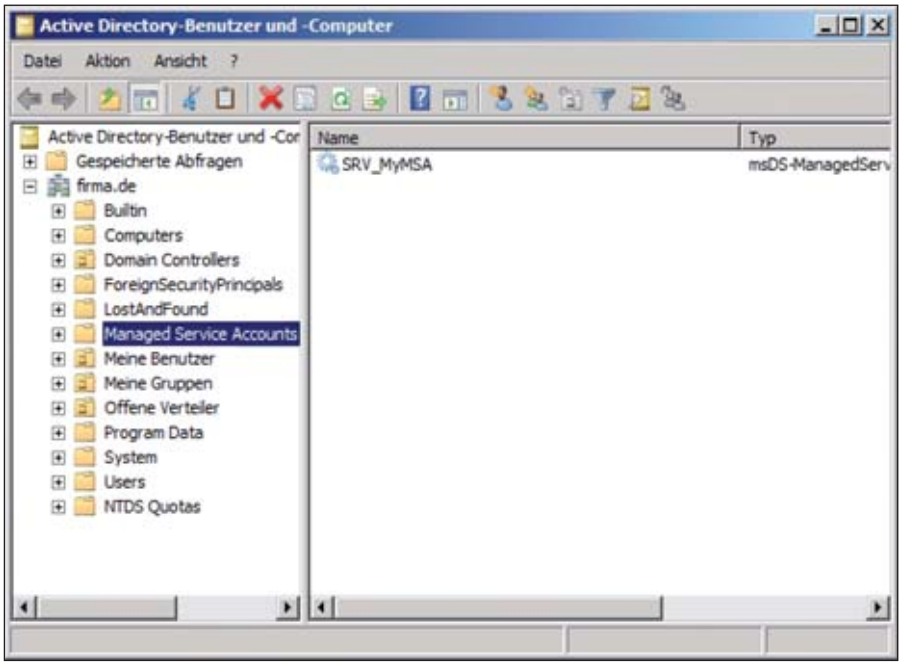


Bild 2: Nachdem Sie die MSAs mit der PowerShell erstellt haben, erscheinen diese in der Managed Service Accounts-OU im Active Directory

terschiedliche Domänenmitglieder hinweg verwendet werden können. Allerdings sollte dies auch nicht allzu häufig notwendig sein.

Voraussetzungen

Als Admin mögen Sie nun denken, dass Sie Managed Service Konten erst verwenden können, wenn alle Domänencontroller einen bestimmten Betriebssystemstand besitzen. Aber tatsächlich lassen sich MSAs auch ohne einen Windows Server 2008 R2-Domänencontroller nutzen. Sie sind nämlich ein Feature, das bis auf eine Ausnahme lediglich ausschlaggebend von der Version des Betriebssystems des Domänenmitgliedes abhängt, das den MSA verwenden soll. Auch dies ist ein Vorteil der clientseitigen Steuerung von MSAs. Damit können Sie MSAs verwenden, sobald folgende Kriterien erfüllt sind:

- Ein Domänencontroller mit mindestens Windows Server 2003, idealerweise 2008 R2 zum Einrichten des MSAs.
- Das Domänenmitglied, das den MSA verwalten soll, muss Windows 7 oder Windows Server 2008 R2 als Betriebssystem nutzen.
- Wird die Gesamtstruktur im "Windows Server 2008 R2 Funktionalitätslevel" betrieben und laufen damit alle DCs auf dem Betriebssystem, können MSAs automatisch auch ihren Service Principal Name verwalten. Dies ist besonders interessant, wenn sich einmal der Name des Servers ändern sollte oder weitere Namen hinzugefügt werden.

Sollten Sie noch keinen Windows Server 2008 R2-Domänencontroller in Ihrer Domäne nutzen, in der Sie den Managed Service Account einsetzen möchten, müssen Sie auf einem Windows Server 2003 oder 2008 das "Active Directory Management Gateway" installieren. Das Active Directory-Schema muss zudem für Windows Server 2008 R2 vorbereitet sein.

Des Weiteren benötigen Sie ein Rechner unter Windows 7 oder Windows Server 2008 R2 als Domänenmitglied, auf dem die "Remote Server Administration für Active Directory" als Feature installiert ist. Nutzen Sie dagegen einen Windows Server 2008 R2-Domänencontroller, lassen sich auf diesem alle notwendigen Schritte zur MSA-Nutzung durchführen.

Einrichten eines Managed Service Accounts

Um einen Managed Service Account zu erstellen und automatisch zu verwalten, müssen Sie zunächst den MSA einrichten. Wie so häufig unter Windows Server 2008 R2 geht dies über die PowerShell. Nachdem Sie die PowerShell entweder in der Kommandozeilenversion oder in der Integrierten Scripting-Oberfläche (Integrated Scripting Environment, ISE) gestartet haben, laden Sie als nächstes das Active Directory-Modul für die PowerShell mit

```
import-module ActiveDirectory
```

Nun kann Sie den Managed Service Account mit dem New-ADServiceAccount-Cmdlet erstellen:

```
New-ADServiceAccount -Name
  {SRV_IhrMSA}
```

Als Nächstes weisen Sie den Managed Service Account einem Computer unter Windows 7 oder Windows Server 2008 R2 zu, der diesen verwalten soll beziehungsweise, auf dem der Dienst läuft, der den MSA verwenden soll:

```
Install-ADServiceAccount -identity
  {SRV_IhrMSA}
```

Das Erstellen des MSA können Sie dann wieder in der Verwaltungskonsole "Active Directory-Benutzer und -Computer" überprüfen.

Als nächstes weisen Sie den Managed Service Account dem Dienst zu, der unter diesem Konto laufen soll. Microsoft SQL und die geplanten Aufgaben werden hierfür derzeit nicht unterstützt, dafür jedoch normale Dienste wie Exchange, IIS Web-Application Pools und Active Directory Lightweight Domain Services (AD-LDS). Hierbei kann es sein, dass für einzelne Dienste weitere Berechtigungen zu setzen sind, vergleichbar zur Nutzung eigens erstellter Servicekonten. Diese Berechtigungen können im Da-

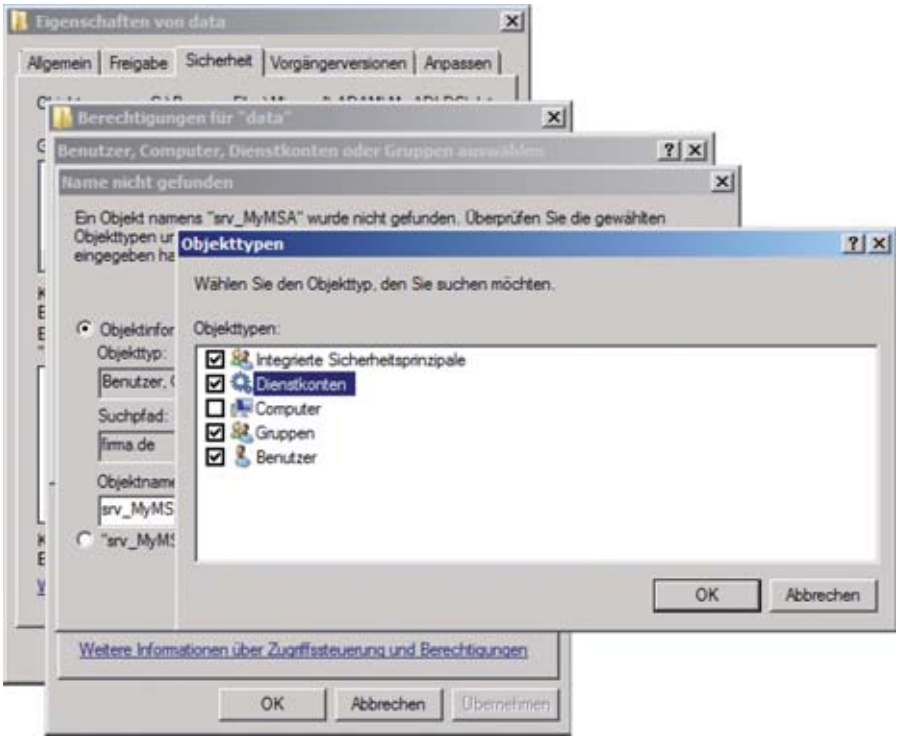


Bild 3: Es ist wichtig, dass beim Zuweisen von Berechtigungen die "Dienstekonten" mit durchsucht werden

teisystem, in der Registrierungsdatenbank, im Active Directory oder sonstigen Applikationen notwendig sein. Meist ist vom Hersteller eine Dokumentation darüber verfügbar, welche Rechte gesetzt werden müssen, wenn Sie eigene Servicekonten verwenden.

Beim Zuweisen der Berechtigungen müssen Sie darauf achten, dass die Dienstekonten als Objekttypen mit überprüft werden. Ansonsten meldet die Konsole, dass das Konto nicht gefunden werden kann. Um einen Dienst oder Application Pool für die Nutzung eines MSAs einzurichten, müssen Sie zudem auf zwei Punkte achten:

- Der MSA muss in der Form "domäne\MSA-Name$", also mit einem $-Zeichen am Ende, angegeben werden. Dies hat den Hintergrund, dass auch Computerkonten ein $-Zeichen am Ende des SAM-Accountnamens haben. Dieser wird jedoch von den meisten Konsolen nicht angezeigt.
- Das Passwort muss leer bleiben.

Häufig unterstützen die Installationsassistenten noch nicht die Verwendung eines MSAs während der Installation eines Dienstes. Hier installieren Sie den Dienst zunächst mit Standardberechtigungen (Lokales System, Netzwerkservice), dann weisen Sie dem Managed Service Account die notwendigen Rechte zu. Öffnen Sie nun die Dienste-Verwaltungskonsole und stoppen Sie den Dienst, ändern das Konto ab und starten den Dienst erneut.

Beseitigen alter MSAs

Werden Managed Service-Konten nicht mehr benötigt, sollten sie, wie alle Konten, entfernt werden. Hierfür konfigurieren Sie zunächst den Dienst, der das Konto verwendet hat, um, so dass dieser ein anderes Konto verwendet – oder Sie entfernen den Dienst mittels Deinstallation ganz. Danach starten Sie die PowerShell mit dem geladenen Modul Active Directory und führen anschließend die folgenden Cmdlets aus:

```
Uninstall-ADServiceAccount -identity
  {SRV_IhrMSA}

Remove-ADServiceAccount -identity
  {SRV_IhrMSA}
```

Der Managed Service Account wird hiermit von dem entsprechenden Computer nicht mehr verwaltet und danach mit dem Befehl Remove-ADServiceAccount aus der Domäne entfernt. Den Befehl *Uninstall-ADServiceAccount* müssen Sie natürlich auf dem Computer ausführen, der den MSA verwaltet. Mittels des Uninstall- und Install-Befehls können Sie den Account erhalten, aber die Verwaltung des Kontos von einem Domänenmitglied auf ein anderes verlegen. Achten Sie hierbei darauf, die Applikationsrechte auch auf der neuen Maschine zu ändern.

Ist einmal nicht mehr bekannt, welcher Computer einen MSA verwaltet, finden Sie dies über den folgenden Befehl heraus:

```
Get-ADServiceAccount -filter *
  -Properties Hostcomputers
```

Wie zu Beginn erläutert, besteht zwischen Managed Service Account und Hostcomputer eine 1:1-Beziehung. Verwaltet ein Computer einen MSA, kümmert sich dieser um das Ändern der Passwörter des Kontos. Nach einer Änderung des Kennwortes können alle anderen Computer, die dieses Konto verwenden, dieses nicht mehr nutzen. Doch wie können Sie damit umgehen, wenn Sie mehrere Computer nutzen, die das gleiche Dienstkonto verwenden?

Nutzung mit mehreren Servern

Ein Beispiel für dieses Szenario ist eine WebServerfarm, die aus mehreren WebServern besteht, etwa aus Performance- und Redundanzgründen. Diese greift auf

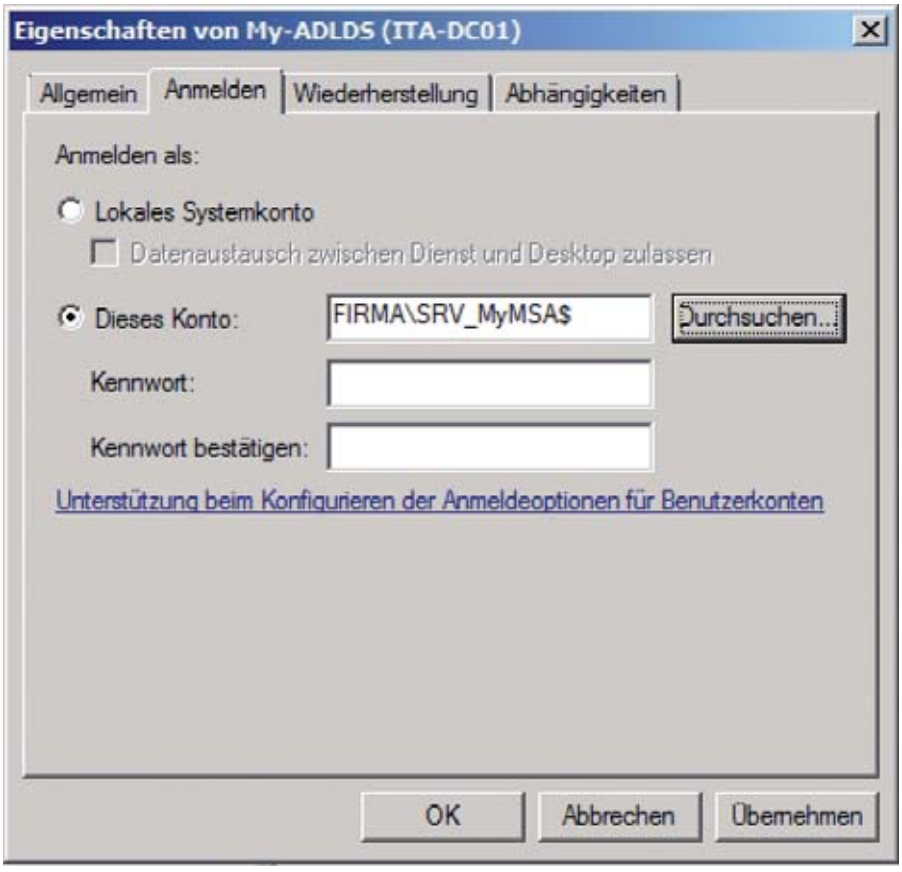


Bild 4: In der Diensteverwaltungskonsole weist der Administrator den Managed Service Account dem entsprechenden Dienst zu

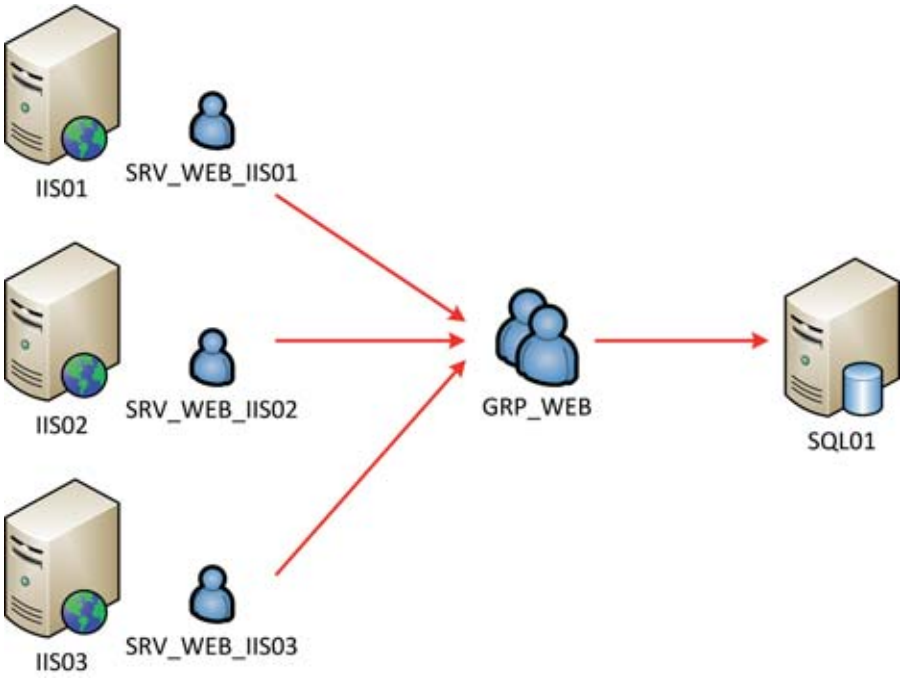


Bild 5: Managed Service Konten können manchmal verwendet werden, obwohl in der Vergangenheit mit einem einzelnen Dienstekonto über mehrere Systeme hinweg gearbeitet wurde.

eine Datenbank im Backend zu. Kann diese Serverfarm MSAs verwenden? Die Antwort ist denkbar einfach: Während wir es bei Benutzerkonten gewohnt sind, diese in Strukturen zu verwalten, werden Dienstekonten häufig direkt auf Ressourcen berechtigt. Sollten sie höhere Rechte erfordern, werden sie manchmal noch in die eingebauten Gruppen Server-Operatoren, Administratoren oder Backup-Operatoren mit aufgenommen. Hier müssen Sie nun umdenken:

- Es wird ein MSA für jeden WebServer erstellt und auf diesem installiert.
- All diese MSAs kommen in eine gemeinsame Gruppe.
- Die Gruppe wird auf dem SQL-Server (oder Cluster) in der Datenbank berechtigt.

Dies bietet nicht nur den Vorteil, dass Sie MSAs benutzen können, sondern vor allem auch, dass nicht alle Systeme gleichzeitig dasselbe Konto verwenden. Das Troubleshooting im Fehlerfall wird so erleichtert, da Sie das Dienstekonto klar einer Maschine zuordnen können.

Bei Applikationen, die sich mit dem Dienstekonto lokal anmelden, dieses aber gleichzeitig für die Replikation mit anderen Maschinen nutzen, lässt sich diese Vorgehensweise vielleicht nicht immer anwenden. Hier überprüfen Sie zunächst, ob entweder eine Trennung der Aufgaben möglich ist oder ob Sie die Berechtigung zur eingehenden Replikation auch an eine Gruppe vergeben können. Ist dies der Fall, lassen sich MSAs wieder verwenden. Greifen Sie hierfür auf das Dateisystem zurück, kann dies einfach sein. Kommt allerdings eigener Code, gegebenenfalls unter Zuhilfenahme von RPC zum Einsatz, gestaltet sich das Unterfangen schwieriger und Sie sollten den Hersteller auf den Wunsch, in Zukunft mit MSAs arbeiten zu können, hinweisen.

Fazit

Managed Service Konten sind eine sehr gute Möglichkeit, um die Problematiken von Dienstekonten mit höheren Berechtigungen in den Griff zu bekommen: Die Passwörter werden automatisch und zufällig vergeben, ändern sich regelmäßig, und der Administrator muss sich nicht mehr darum kümmern, die Passwörter zu speichern und vor allem regelmäßig zu ändern. Doch leider lassen sie sich nicht in allen Fällen anwenden. Es gibt Applikationen, die diese Form der Konten einfach (noch) nicht unterstützen, etwa weil sie bei der Installation die Kombination Benutzername und Passwort überprüften möchten, oder weil sie über mehrere Systeme hinweg das gleiche Konto benötigen. Einigen Diensten kann dann nachgeholfen werden, indem Sie den Dienst nach der Installation auf ein Managed Service Konto migrieren, oder indem Sie unterschiedlichen Servern unterschiedliche Konten zuweisen, diese dann aber in einer Gruppe zusammenfassen, auf die Sie die benötigten Rechte vergeben.

Für Applikationen, die Managed Service Accounts überhaupt nicht unterstützen, müssen Sie weiterhin auf klassische Dienstekonten zurückgreifen. Hierbei ist es aber wichtig, dass Sie einen Prozess für die sichere Verwaltung der Passwörter nutzen, diese Konten nicht für administrative Aufgaben verwenden, und vor allem, dass Sie sich an Regeln halten, die ein regelmäßiges Wechseln der Passwörter ermöglichen. Ist bekannt, wie die Passwörter der Dienstekonten möglichst unterbrechungsfrei geändert werden können, bietet sich auch Folgendes an: Beim Erstellen des Dienstkontos generieren Sie ein zufälliges und sehr langes Passwort, das Sie in die Zwischenablage laden. Dann tragen Sie das Kennwort in dem Dienst ein, indem Sie es aus der Zwischenablage einfügen. Das Passwort können Sie nun getrost vergessen. Benötigen Sie das Passwort wieder oder steht ein Passwortwechsel an, gehen Sie genauso vor, um das Passwort wieder neu zu generieren und zu ändern. Diese Vorgehensweise ist fast ebenso sicher, wenn auch nicht so komfortabel, wie Managed Service Konten zu verwenden. Sie hat aber einen großen Vorteil: Sie funktioniert auch systemübergreifend und mit Diensten wie den geplanten Aufgaben. *(dr)*


Quelle: de.wikipedia.org

Passwortrichtlinien in Unternehmen

sl(h3re_p4ssWörT3r

Passwörter gehören in jede Infrastruktur und legen den Grundstein aller Sicherheit in Unternehmen. Sie schützen Konten und Daten vor ungewolltem Zugriff und kommen quasi überall zum EInsatz. Dieser Workshop zeigt auf, wie Passwörter in Windows-Systemen über die Gruppenrichtlinien gesteuert werden, wie diese im Active Directory verarbeitet und geprüft werden und welche Drittanbietertools für stärkere Passwörter sorgen.

In Domänen bis Windows Server 2003 lässt sich pro Domäne eine bestimmende Passwortrichtlinie definieren: die Domänen-Passwortrichtlinie. Sie ist eine Gruppenrichtlinie, die die sogenannten "Passworteinstellungen" in "Computerkonfiguration / Windows-Einstellungen / Sicherheitseinstellungen / Kennwortrichtlinien" definiert.

Entgegen vieler falsch lautender Tech-Net- oder Webseiten-Artikel müssen die Passworteinstellungen für die Richtlinie nicht in der "Default Domain Policy" hinterlegt sein. In der Tat kann es jede beliebige, gern auch selbst erstellte Gruppenrichtlinie sein, die mit dem Domänenobjekt verknüpft ist. Nur mit dem Domänenobjekt verlinkt wirkt die Passwortrichtlinie auch auf Domänenkonten. Gruppenrichtlinien, die Passwortrichtlinien definieren und mit OUs verknüpft werden, haben keinen Einfluss auf Domänenkonten, die sich an Computern in der OU einloggen. Stattdessen wirkt die Passwortrichtlinie auf OU-Ebene nur auf lokale Benutzerkonten der Zielrechner in der OU.

Bearbeitungsreihenfolge entscheidet über Passwort

Ein Problem bei der Erstellung von eigenen Passwortrichtlinien und der Verlinkung mit dem Domänenobjekt ist für viele Administratoren die Reihenfolge der GPO-Abarbeitung. Bei den Passwortrichtlinien verhält es sich wie mit unsterblichen Schotten in New York: Es kann nur eine geben. Passwortrichtlinien werden nicht zusammengeführt – sind mehrere GPOs mit Passwortrichtlinien am Domänenobjekt verlinkt, gewinnt die zuletzt verarbeitete.

Die Abarbeitungsreihenfolge der Gruppenrichtlinien ist bekanntermaßen "L-S-D-OU", wobei zunächst die lokalen Richtlinien an einer Maschine, danach die standortbezogenen, anschließend die Domänenrichtlinie und danach der OU-Baum bis zum Zielobjekt im Verzeichnis abgearbeitet werden. Richtlinien auf einer Ebene haben ebenfalls eine Ordnung, in der sie nacheinander gelesen und verarbeitet werden. Geöffnet in der Gruppenrichtlinien-Management-Konsole, werden Gruppenrichtlinien derselben Ebene von unten nach oben abgearbeitet. Die letzte GPO der Liste zuerst, zum Schluss die ganz oben auf der Liste.

Übertragen wir diese Kenntnis auf den Domänenlevel, sollte eine selbst erstellte Passwortrichtlinie stets als erste Richtlinie in der Übersicht der GPMC verknüpft sein. Für die Sortierung lassen sich die Pfeiltasten der GPMC nutzen.

Richtlinien in Windows Server 2008-Domänen

Mit Windows Server 2008 erhörte Microsoft den Wunsch vieler Kunden, mehr als nur eine Passwortrichtlinie pro Domäne definieren zu können. In der Tat stößt genau diese Beschränkung vielen Unternehmen negativ auf, zumal unterschiedliche Jobrollen oder Abteilungen unterschiedlich starke Sicherheitsanforderungen an die Authentifizierung der Mitarbeiter und Sicherung der Daten legen. Die bisherige Empfehlung seitens Redmond war es, diese Geschäftszweige in eine eigene Domäne auszulagern und so eine neue Passwortrichtlinie zu definieren. So ein Vorgehen hat aber weitere, negative Effekte wie zusätzlichen Verwaltungsaufwand und Kosten für Hard- und Software.

Befindet sich eine Domäne im Domänenfunktionsmodus "Windows Server 2008", lässt das Active Directory (AD) Administratoren sogenannte "Password Setting Objects" (PSOs) erstellen. PSOs

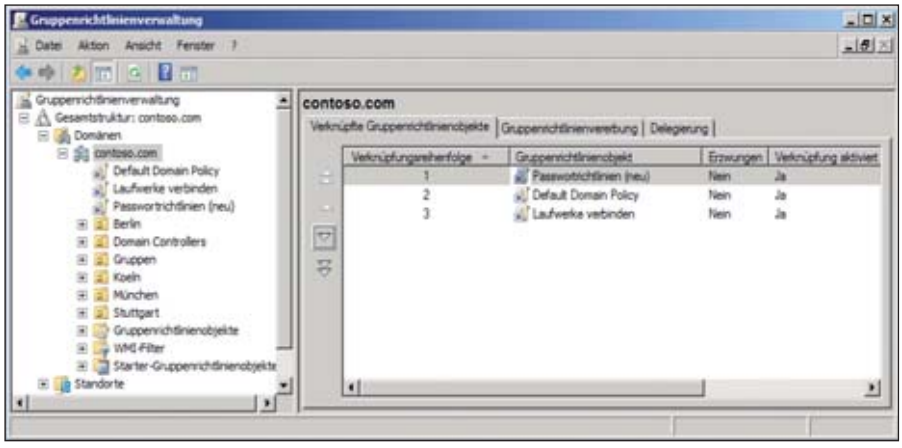


Bild 1: Die Liste der Gruppenrichtlinien wird stets von unten nach oben im Last-Writer-Wins-Prinzip abgearbeitet

sind AD-Objekte, mit denen granulare Passwortrichtlinien ("fine-grained password policies", FGPP) definiert werden. Sie werden im Container "CN=PasswordSettingsContainer,CN=System,DC=Domain,DC=tld" abgelegt und während ihrer Erstellung mit einem Benutzer, einer Sicherheitsgruppe oder einem InetOrgPerson-Objekt verknüpft. Über die Verknüpfung wird bei einer Passwortänderung dann die richtige Passwortrichtlinie geladen. Beim Einsatz von FGPPs ändert sich die Prüfung des zu ändernden Passwortes im Gegensatz zur herkömmlichen Passwortrichtlinie nicht – der Mechanismus ist identisch. Die zu prüfenden Optionen wie "maximale Kennwortlänge" bleiben erhalten.

Bevor Sie eine PSO erstellen, sollten Sie die Objekte, mit denen die PSO verknüpft wird, notieren und ihren LDAP-Pfad bereithalten. Während der PSO-Erstellung wird der "distinguishedName" der Zielobjekte verlangt, die Sie per *ADSIEdit* von den entsprechenden Gruppen oder Benutzern ablesen.

Erstellen lässt sich eine PSO mit reinen Windows-Bordmitteln über den AD-Editor ADSIEdit. Per Rechtsklick auf den Container "System" und Auswahl von "Neu" und "Objekt..." wird ein neues Passwortobjekt erstellt. Der "Objekt erstellen"-Dialog lässt nur die Auswahl des "msDS-PasswordSettings"-Objekts zu. Im Folgenden verlangt ADSIEdit Schritt für Schritt die Eingabe der für die Erstellung notwendigen Informationen für das PSO (siehe Tabelle "Erstellung eines PSO").

Im letzten Schritt der Objekterstellung zeigt ADSIEdit an, dass per Klick auf "Fertig stellen" das Objekt erstellt werden kann. In der Tat würde das Objekt zu diesem Zeitpunkt erfolgreich erstellt werden, was jedoch fehlt, ist der Bezug zu einer Gruppe, einem Benutzer oder einem iNetOrgPerson-Objekt. Es fehlt das optionale Attribut "msDS-PSOAppliesTo", das Sie mit einem Klick auf "Weitere Attribute" in "Anzuzeigende Eigenschaft" auswählen. Der Attributwert muss der "DN"-Syntax entsprechend, die dem LDAP-Pfad entspricht. Hier fügen Sie den kurz zuvor notierten "distinguishedName" des Zielobjektes ein.

Evaluation der Passwortrichtlinie

Bei der Zuweisung von PSOs an Zielobjekte kann es Überschneidungen geben. Das Active Directory führt keine Prüfung über die bereits verlinkten PSOs auf die Zielobjekte durch – im Gegenteil: Mehrere PSOs, die mit einem Zielobjekt verlinkt sind, sind völlig legitim.

Bei der Evaluation der Passwortrichtlinie wird ein besonderer Algorithmus herangezogen: Das AD prüft, ob dem im Fokus stehenden Objekt direkt eine PSO zugewiesen wurde. Falls ja, wird die PSO angewandt. Falls mehrere PSOs in Frage kommen, wird das Vergleichsverfahren angewandt. Ist kein Passwortobjekt mit dem Benutzerkonto verknüpft, werden die Gruppenmitgliedschaften des Benutzers in Betracht gezogen. Ist einer der Gruppen des Benutzers eine Richtlinie zugeordnet, wird diese angewandt – bei mehreren in Frage kommenden Richtlinien wird erneut das Vergleichsverfahren herangezogen. Landet das AD auch hier keinen Treffer, weil der Benutzer oder keine seiner Gruppen eine PSO verknüpft hat, nutzt der Verzeichnisdienst die Domänen-Passwortrichtlinie für die Prüfung der Validität des neuen Passworts.

Das Vergleichsverfahren, das bei mehreren in Frage kommenden PSOs angewandt wird, ist simpel: Zuerst werden die Preference-Werte der beteiligten PSOs verglichen. Die Richtlinie mit dem kleineren PSO-Wert gewinnt. Besitzen beide Richtlinien denselben Preference-Wert, wird die vom System vergebene Objekt-GUID verglichen. Die kleinere der eindeutigen Identifizierungsnummern gewinnt hier ebenfalls.

PSO-Erstellung mit PSOMgr

Joe Richards bietet auf seiner Webseite [1] ein kostenfreies Kommandozeilen-Programm für die Erstellung von PSOs an. Die Bedienung von "PSOMgr" ist etwas einfacher als die Nutzung von ADSIEdit. Per Kommandozeile kann PSOMgr aufgerufen werden. Das folgende Kommando erstellt ein PSO anhand der Beispieldaten der Tabelle "Erstellung eines PSO":

```
PSOMgr -add myPSO:meine
  PSO:20:75:8:10:10:90:20:3:
  TRUE:FALSE
```

Das Kommando enthält Parameter, die jeweils mit Doppelpunkten voneinander getrennt sind. Die Syntax lautet:

Erstellung eines PSO		
Attribut	**Beschreibung**	**Beispielwerte**
Cn (Common-Name)	Der Anzeigename der PSO.	"Passwortrichtlinie für Sales"
msDS-PasswordSettingsPrecedence	Die Gewichtung der PSO. Sind mehrere PSOs für ein Objekt definiert, gewinnt die PSO mit der niedrigsten Gewichtungswert.	Ganzzahl, etwa "20".
msDS-PasswordReversibleEncryptionEnabled	Ein boolscher Wert (wahr/falsch), ob Passworte in rückkehrbarer Verschlüsselung gespeichert werden sollen.	"FALSE"
msDS-PasswordHistoryLength	Die Anzahl der zu speichernden alten Passworte, auf die geprüft werden soll, wenn Benutzer neue Passworte wählen.	Ganzzahl, etwa "10".
msDS-PasswordComplexityEnabled	Ein boolscher Wert (wahr/falsch), ob die Passwortkomplexität aktiviert werden muss oder nicht.	"TRUE"
msDS-MinimumPasswordLength	Die Anzahl der Zeichen, die das Passwort mindestens lang sein sollte.	Ganzzahl, etwa "8"
msDS-MinimumPasswordAge	Die Dauer, die ein Passwort mindestens alt sein muss, bevor es erneut geändert werden darf.	Dauer nach der Syntax Tage:Stunden:Minuten:Sekunden im Format dd:hh:mm:ss.
msDS-MaximumPasswordAge	Die Dauer, die ein Passwort maximal alt sein darf, bevor es zwingend geändert werden muss.	Dauer nach der Syntax Tage:Stunden:Minuten:Sekunden im Format dd:hh:mm:ss.
msDS-LockoutThreshold	Die Anzahl der Fehlversuche, die ein Benutzer bei der Passworteingabe hat, bevor der Account gesperrt wird.	Ganzzahl von 0 bis 65535, wobei "0" die Sperrung deaktiviert. Beispiel: "10" für zehn Versuche
msDS-LockoutObservationWindow	Die Dauer, die sich das System fehlgeschlagene Authentifizierungsversuche merken soll, bevor es den "Fehlversuchszähler" auf null zurücksetzt.	Dauer nach der Syntax Tage:Stunden:Minuten:Sekunden im Format dd:hh:mm:ss.
msDS-LockoutDuration	Die Dauer, die ein Account nach Erreichen der maximalen Fehlversuche gesperrt wird.	Dauer nach der Syntax Tage:Stunden:Minuten:Sekunden im Format dd:hh:mm:ss.

```
PsoMgr -add name:displayname:
  precedence:maxpwdage:minpwdlength:
  pwdhistory:lockout count:lockout
  duration:lockout observation
  window:minpwdage:password
  complexity:reversible encryption
  enabled
```

Die Ausführung des Kommandos legt die PSO nicht automatisch an. Stattdessen zeigt das Werkzeug, was es tun würde, wenn es seine Arbeit verrichten würde. Um dem Tool die Erlaubnis zu erteilen, Änderungen am Verzeichnis vorzunehmen und eine PSO anzulegen, müssen Sie den Schalter "-forreal" am Ende des Kommandos anfügen. In einem zweiten Schritt weisen Sie die PSO dann einem Benutzer, einer Gruppe oder einem iNetOrgPerson-Objekt zu:

```
PSOMgr /applyTo Florian /pso
  Passwortrichtlinie
```

Ein großer Vorteil dieses Tools ist seine Reportingfunktion. Werden mehrere PSOs auf unterschiedliche Gruppen und Benutzer verlinkt, kann es schwierig sein, die angewendete PSO für einen bestimmten Benutzer zu bestimmen. PSOMgr hat hierfür eigens einen Schalter: *PSOMgr /effective {Benutzername}* sorgt dafür, dass die greifende PSO für den ausgewählten Benutzer, unter Nutzung des beschriebenen Vergleichsverfahrens, ausgegeben wird.

Prüfung der Passworte im System

Die Passwortprüfung in Windows hat Grenzen, derer Sie sich bewusst sein müssen, um ein Gefühl dafür zu bekommen, welche Arten von Passworten und welche Passwortänderungen vom System akzeptiert werden und welche nicht.

Eine nicht ganz einfach zu durchschauende Option ist die Komplexitätsprüfung, die Sie für Kennwortrichtlinien ein- oder ausschalten können. Kennworte können in einem Active Directory aus vier unterschiedlichen Zeichensätzen bestehen: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen. Die Prüfung der Zeichen beschränkt sich darauf zu testen, ob mindestens drei dieser vier Zeichensätze im Passwort enthalten sind – wie viele Zeichen zu jedem Zeichensatz verwendet wurden, spielt keine Rolle.

Die Prüfung schlägt dann fehl, wenn nur zwei Zeichensätze zum Einsatz kommen. Es ist aus diesem Grund nicht notwendig, Son-

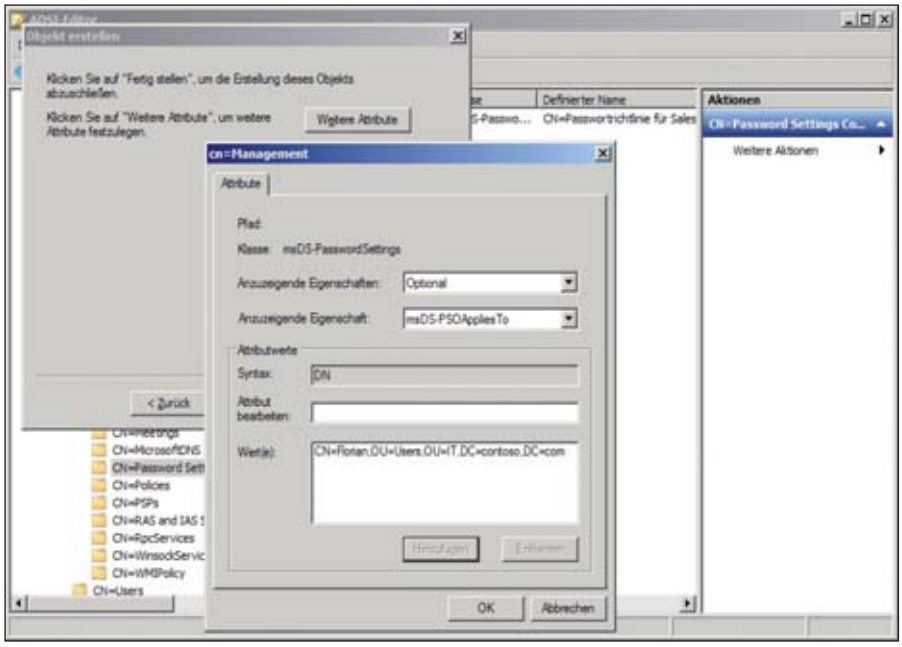


Bild 2: Zum Abschluss der Erstellung der PSO müssen die zu übernehmenden Objekte gewählt werden

derzeichen zu nutzen, wenn sowohl Groß- als auch Kleinbuchstaben und mindestens eine Zahl im Passwort verwendet wird. Benutzer haben somit die Wahl, ob sie beispielsweise Sonderzeichen verwenden möchten und dafür Großbuchstaben nicht verwenden oder Zahlen umgehen anstatt Sonderzeichen. Welche Zeichensätze zu nutzen sind, lässt sich nicht kontrollieren.

Die "Password History" ermöglicht, bereits genutzte Passworte zwischenzuspeichern und sie für eine erneute Nutzung zu verbieten. Die Prüfung der zuletzt genutzten Passworte schlägt dann an, wenn ein Passwort aus der Historie dem neuen Passwort gleicht. Eine Ähnlichkeitsprüfung findet an dieser Stelle nicht statt, nur vollkommen identische Passworte werden bemerkt. Manager, deren Lieblingspasswort "Golf" ist, können deshalb ungestört ihr Passwort herauf zählen und mit jedem Passwortwechsel eine Zahl im Kennwort erhöhen; etwa Golf1, Golf2 oder Golf3. Diese Zählfolge ist völlig legitim und wird vom System nicht zurückgewiesen.

Überblicken wir die zur Verfügung stehenden Optionen der Passwortrichtlinien, finden wir uns in einem überschaubarem Rahmen konfigurierbarer Einstellungen wieder. Während quantitative Merkmale der Passworte, wie maximale und minimale Länge oder Sperrdauern sehr flexibel konfiguriert werden können, fehlt es der qualitativen Prüfung der Passworte, nämlich der Syntax und Wortüberprüfung, an Flexibilität. Schnell stoßen Administratoren an Grenzen, wenn Passworte auf Ähnlichkeit zu vorherigen Passworten überprüft werden sollen oder eine "Blacklist" mit verbotenen Zeichenketten definiert werden soll, die niemals in Passworten vorkommen darf.

Drittanbietertools für stärkere Passwörter

Wenn Sie über Programmierkenntnisse verfügen, können Sie sich Ihren eigenen Passwortfilter bauen: Microsoft selbst nutzt bei der Überprüfung neuer Passworte die Passwortfilter-Komponente *passfilt.DLL* [2]. Sie wird zur Rate gezogen und durchlaufen, wenn Passworte evaluiert werden. Entwickler können eigene Passwort-Filter erstellen und sie zusätzlich registrieren [3]. Da der Passwortfilter an einer zentralen Stelle im System verwendet wird, ist Vorsicht geboten: Nicht jedes Unternehmen duldet in diesem sicherheitskritischem Bereich selbsterstellte Eingriffe in das System. Ausgiebiges Testen im Labor und die Prüfung der Komponente mit vielen Testpassworten ist ein Muss.

Mittlerweile existieren viele kommerzielle Drittanbieteranwendungen, die flexible und strenge Kontrollen neuer Passwörter erzwingen. Einige dieser Produkte umfassen konfigurierbare Schwarzlisten mit nicht erwünschten Zeichen oder ganzen Zeichenketten, das Erzwingen einer bestimmten Anzahl von Zeichen eines Zeichensatzes oder das Verbot von spezifischen Anfangs- oder Endzeichen in Passworten. Auch Ähnlichkeitsprüfungen bieten einige Produkte an. Tests einiger Produkte können Sie auf [4] einsehen. *(jp)*

Anixis – "Password Policy Enforcer"
http://anixis.com/products/ppe/default.htm

SpecOps – "SpecOps Password Policy"
www.specopssoft.com/web/specops-password-policy.aspx

nFront Security – "Password Filter"
http://nfrontsecurity.com/products/nfront-password-filter/

Quest – "Password Manager"
www.quest.com/password-manager/

Drittanbietertools zur Passwortkontrolle

[1] **Joeware.NET – PSOMgr**
www.joeware.net/freetools/tools/psomgr/index.htm

[3] **Password Filter Programming Considerations (Windows)**
http://msdn.microsoft.com/en-us/library/ms721884(VS.85).aspx

[2] **Password Filters (Windows)**
http://msdn.microsoft.com/en-us/library/ms721882(VS.85).aspx

[4] **Gruppenrichtlinien – Übersicht, FAQ und Tutorials**
www.gruppenrichtlinien.de

Links

SpecOps Password Policy Basic

Passwortrichtlinien fein verwaltet

Seit Windows Server 2008 können Administratoren unterschiedliche Passwortrichtlinien für Servicekonten, Administratoren oder andere Benutzergruppen einrichten. Leider fehlt aber das Werkzeug, um diese grafisch zu verwalten. Der Hersteller SpecOps hilft mit dem freien Tool Password Policy Basic aus.

Passwortrichtlinien sind eigentlich ein Thema in jedem Unternehmen. Was leider nicht häufig genug bewusst ist: Passwörter sind bei physikalischem Zugriff auf ein System relativ einfach zu knacken. Und wer die Kombination von Benutzernamen und Passwort besitzt und an die Infrastruktur des Unternehmens herankommt, tut sich häufig recht leicht damit, an weitere Daten zu gelangen. Besonders kritisch sind aber Konten mit höheren Berechtigungen, wie Administratoren- oder Dienstekonten. Ein zufällig generiertes Passwort mit zehn Zeichen, Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen hält nicht einmal zwei Tage stand, bis es geknackt ist. Dabei arbeitet die Hardware zusehens schneller. Ob Passwort-Lockouts eine sinnvolle Alternative bieten, darüber streiten sich Sicherheitsexperten. Stellen diese doch eine mögliche Denial of Service-Schwachstelle dar, indem ein Angreifer fremde Konten durch Ausprobieren von Passwörtern sperren kann.

Während in den bisherigen Versionen des Active Directory immer nur eine Passwort-Richtlinie für die Domäne gelten durfte, gibt es mit Windows Server 2008 die Möglichkeit, Benutzern oder Gruppen eigene Passwortrichtlinien zuzuordnen. Die Details hierfür finden Sie ab Seite 128. Für Dienstekonten sollten Sie, sofern Sie bereits Windows Server 2008 R2 oder Windows 7 einsetzen, lieber Managed Service Accounts verwenden (mehr dazu ab Seite 123). Wo dies aber nicht möglich ist, sollten die Dienstekonten auf alle Fälle eine sicherere Passwortrichtlinie wie auch "normale Anwender" erhalten.

Während Microsoft die Mechanismen hierfür mit Windows Server 2008 anbietet, stellt der Hersteller kein Tool bereit, um diese auch anwenderfreundlich zu administrieren. In Windows Server 2008 R2 gibt es zwar die Active Directory-Cmdlets für die PowerShell, aber eine grafische Benutzeroberfläche lässt dennoch auf sich warten.

Specops ist eine Softwarefirma, die mit Specops Password Policy [1] schon seit Jahren einen eigenen Passwortfilter vertreibt. Damit stellen Sie nicht nur die normalen Parameter wie Komplexität oder Länge ein, sondern richten auch in jeder unterstützten Version von Windows eine Passwortrichtlinie abhängig vom Benutzer oder der Gruppe ein. Diese Richtlinien können dabei mehr Vorgaben besitzen, zum Beispiel, dass bestimmte Worte aus einem Lexikon nicht erlaubt sind, die Kombination mit dem Benutzernamen geprüft wird und eine bestimmte Kombination von Zahlen, Sonderzeichen oder Buchstaben erforderlich ist.

Zudem bietet Specops auch denjenigen Administratoren eine Hilfe an, die nur die standardmäßigen Möglichkeiten von Windows Server 2008 nutzen wollen: Mit SpecOps Password Policy Basic [2] lassen sich die Windows Server-eigenen Passwortrichtlinien grafisch verwalten.

Einfache Installation

Die Installation verläuft schnell und problemlos. Die Vollversion installiert auch Cmdlets für die Verwaltung der Fine Grained Password Policies über die PowerShell. Benutzer von Windows Server 2008 R2 verwenden wahrscheinlich lieber die Standard-Cmdlets von Microsoft, aber für Windows Server 2008-Benutzer ohne Windows 7 oder Windows Server 2008

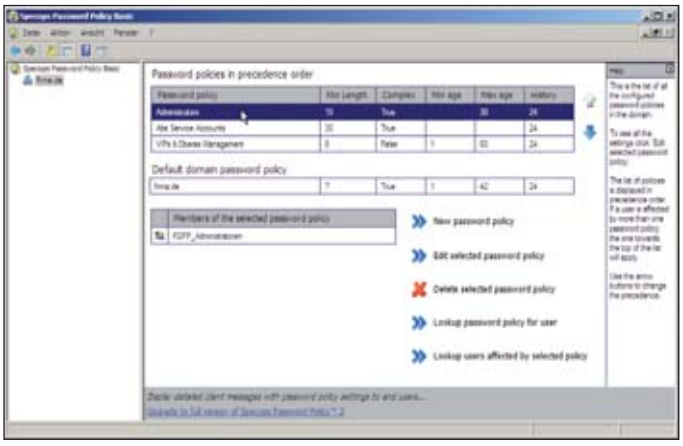


Bild 1: Die übersichtliche Oberfläche bietet alle Funktionen, die Sie im Alltag benötigen

R2 Administrationssysteme gibt es diese Möglichkeit ja nicht.

Was etwas eigenartig wirkt: Während der Installation öffnet sich kurz ein Kommandofenster, in dem Dateien im .NET Framework-Bereich eingerichtet werden. Es sieht so aus, als träten hier Fehler auf, allerdings funktioniert hinterher trotzdem alles. Nach der Installation führen Sie die Anwendung über das Startmenü aus. Leider registriert die Software sich nur unter "Alle Programme / Special Operations Software / Specops Password Policy Basic" und nicht unter "Verwalten". Da diese Konsole aber zum Umfang der Administrationstools gehören sollte, können Sie diese auch dort registrieren.

Erstellen von Passwortrichtlinien

Die Oberfläche stellt sich übersichtlich und zweckgemäß dar. Auf der Startseite erlaubt sie, mehrere Domänen für die Verwaltung hinzuzufügen. Sobald Sie auf der linken Seite die Domäne auswählen oder auf "Configure Selected Domain" gehen, erscheinen die Passwortrichtlinien, die im Password Settings Container gespeichert sind. Standardmäßig – wenn noch keine "Fine Grained Password Policies" erstellt wurden – finden Sie hier nur die Einstellung aus der Default Domain Policy.

Das Erstellen einer neuen Passwort-Richtlinie ist recht einfach, Sie sollten aber ein paar Punkte beachten:

- Überlegen Sie sich im Unternehmen eine Namenskonvention für die Password Settings-Objekte.
- Die Zuordnung von Passwortrichtlinien erfolgt über Benutzer oder Gruppen. Präferiert ist letzteres. Es wird empfohlen, eine Gruppe pro Passwortrichtlinie anzulegen, die Passwortrichtlinie auf diese zu Verknüpfen, und über Delegation festzulegen, wer die Passwortrichtlinie zuordnen darf. Die Gruppe hierfür muss eine Globale Gruppe sein.
- Das Delegationsmodell muss solide sein: Passwortrichtlinien sollten nicht von "normalen" Helpdesk-Mitarbeitern festgelegt werden dürfen.
- Helpdesk-Mitarbeiter benötigen trotzdem lesenden Zugriff auf die Konsole, um festzustellen, welche Richtlinie für den entsprechenden Benutzer gilt.

Neue Richtlinien lassen sich einfach über die Oberfläche erstellen. Hierfür wählen Sie einen Namen und anschließend, welche Parameter Sie für die neue Richtlinie konfigurieren möchten:

- Minimale Passwort Länge
- Passwort muss Komplexitätsanforderungen erfüllen
- Maximales Passwortalter
- Minimales Passwortalter (um mehrfache Änderungen zu verhindern)
- Passwort-Historie erzwingen (um zu verhindern, dass der Anwender eines der letzten Passwörter wieder verwendet)
- Passwort in zurückrechenbarer Verschlüsselung speichern (diese Einstellung sollte eigentlich nie getätigt werden, außer man ist sich absolut sicher).

Zusätzlich legen Sie die Kontensperrungsrichtlinien fest:

- Konto sperren nach einer Anzahl von fehlgeschlagenen Versuchen.
- Anzahl fehlgeschlagener Versuche nach x Minuten zurücksetzen.
- Konto automatisch nach x Minuten entsperren.

Zusätzlich lassen sich im Dialog noch die Mitglieder festlegen, für die die Passwortrichtlinie gelten soll. Hier sollten Sie wie erwähnt eine Globale Gruppe verwenden, deren Administration nicht oder nur geplant delegiert wurde. Diese Gruppe kommt dann zum Einsatz, um die Passwortrichtlinien auf die eigentlichen Benutzergruppen anzuwenden.

In der Übersicht der Passwortrichtlinien sehen Sie sowohl deren Einstellungen wie auch die Reihenfolge. Würden Sie die Passwortrichtlinien mit ADSIEdit verwalten, müssten Sie den Wert Precedence (=Vorrang) selbst mit einer beliebigen Zahl füllen. Gelten für einen Benutzer dann mehrere Passwortrichtlinien, kommt derjenigen mit der höchsten Precedence zum Einsatz. Specops Password Policy Basic verwaltet auch diesen Wert eigenständig – Sie können in der Oberfläche jedoch die Reihenfolge der Richtlinien angeben und ändern, wobei die Richtlinien eine höhere Priorität besitzen, desto weiter oben sie stehen. Daher sollten Sie sich auch beim Ordnen der Richtlinien Gedanken machen. Sinnvollerweise haben die Richtlinien Vorrang, die restriktiver / sicherer sind und weiter oben stehen.

Analyse

Das Werkzeug unterstützt Sie aber nicht nur beim Anlegen der Richtlinien, sondern kann auch dazu dienen, die Zuordnung von Passwortrichtlinien und Benutzer zu analysieren. Auch lassen sich alle Benutzer anzeigen, die über verschachtelte Gruppenmitgliedschaften von der Richtlinie betroffen sind. Hierzu wählen Sie einfach "Lookup password policy for user" und wählen den Benutzer. Dann erhalten Sie die Richtlinie, die für ihn gilt. Oder Sie wählen eine Passwortrichtlinie aus und klicken dann auf "Lookup users affected by selected policy". Damit erhalten Sie die Liste der betroffenen Benutzerkonten.

Fazit

Was Microsoft bisher versäumt hat anzubieten, stellt SpecOps mit Password Policy Basic unentgeltlich zur Verfügung: die einfache Verwaltung von individuellen Passwortrichtlinien in einer grafischen Administrationsoberfläche. Da ist es auch einmal erlaubt, dass in der Konsole etwas Werbung für die volle Version von Specops gemacht wird, die dann zahlreiche weitere Funktionen zur Verfügung stellt, die das Betriebssystem bisher nicht leisten kann. *(dr)*

[1] SpecOps Password Policy
www.specopssoft.com/web/specops-password-policy.aspx

[2] Download SpecOps Password Policy Basic
www.specopssoft.com/web/specops-password-policy-basic-download_1.aspx

Links

Quelle: robynmac – Fotolia.com

GGPHealth-Cmdlets für die PowerShell

Gruppenrichtlinien auf dem Prüfstand

Nicht nur Gruppenrichtlinien-Administratoren in sicherheitskritischen Umgebungen kennen das Problem, dass ausgerollte Gruppenrichtlinien kontrolliert und ihr Übernahmezustand protokolliert werden müssen. Auch GP-Administratoren anderer Industriebereiche sehen sich zunehmend vor der Herausforderung, einen Nachweis für die korrekte Übernahme und Wirkung von erzwungenen Einstellungen an Clientrechnern zu erbringen. Die Sicherheitseinstellungen sind dabei nur eine Komponente. Wie Sie mit der PowerShell diese Nachweise automatisiert erbringen, zeigt dieser Workshop.

Für den Administrator gibt es keine Möglichkeit zu prüfen, ob Clients eine Gruppenrichtlinie übernommen haben, nachdem sie mit der GPMC an die entsprechende OU verlinkt wurde. Es existiert kein "Report-Back"-System, das dem GP-Admin mitteilt, ob neu definierte Sicherheitseinstellungen an allen Computern Wirkung zeigen oder eine Registrierungseinstellung oder ein GP Preference-Item aufgrund einer fehlenden Datei oder falschen Pfadangabe nicht ausgeführt werden konnte. Zumindest geringfügig Abhilfe schaffen selbstgebaute Skripte oder Eventlog-Sammler, die die GP-Clients nach bekannten Gruppenrichtlinien-Fehlern im Eventlog durchforsten und bei Funden anschlagen, um Administratoren zu warnen. Schön und präzise sind diese Lösungen allerdings meist nicht.

Etwas eleganter geht dies mit dem Group Policy Health-Cmdlet von SDMSoftware, das unter [1] frei zum Download zur Verfügung steht. Das PowerShell-Cmdlet binden Sie per Import-Modul in die PowerShell-Session ein und rufen es per Get-SDMGPHealth-Kommando auf. Fokussiert werden mit dem Cmdlet stets einzelne Computer, die Sie aber problemlos auch in großer Anzahl per Pipe durchforsten können. Das Cmdlet nimmt dabei jeweils Kontakt mit dem Zielrechner auf, enumeriert alle Gruppenrichtlinien und ihre Client Side Extension und prüft, ob der letzte Lauf der Richtlinienverarbeitung korrekt und problemlos durchgeführt wurde. Das Skript gibt den Status nach den bekannten Ampelfarben Grün für gut und Rot für schlecht aus. Gelb für warnende Hinweise gibt es hier nicht. Der zu untersuchende Computer muss bei der Ausführung des Kommandos per Netzwerk erreichbar sein, sonst kann das Skript die Daten nicht korrekt sammeln.

Nach der Installation des zugehörigen Cmdlet-MSI-Files muss eine benötigte .NET-DLL-Datei für die Verwendung registriert werden. Hierfür wechseln Sie in das Systemverzeichnis des .NET-Ordners mit

```
cd C:\Windows\Microsoft.NET\Framework\v2.0.50727
```

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet> Get-SDMGPHeal
th -computer dell630


OverallStatus              : green
TimeLogged                 : 06.09.2010 09:57:25
HostName                   : dell630
Domain                     : intern.frickelsoft.net
OSVersion                  : Microsoft Windows 7 Ultimate ,
ComputerCoreStatus         : The operation completed successfully
UserCoreStatus             : The operation completed successfully
FastLogonEnabled           : False
ComputerSlowLinkDetected   : False
Loopback                   : None
DCUsed                     : \\DC-2008r2.intern.frickelsoft.net
ComputerElapsedTime        : 00:00:01
CurrentLoggedOnUser        : INTERN\florian
UserSlowLinkDetected       : False
UserElapsedTime            : 00:00:02
ComputerGPOsProcessed      : {Local Group Policy, Enable REmote Desktop, Certific
                             ate Policy, Default Domain Policy...}
UserGPOsProcessed          : {Local Group Policy, Enable REmote Desktop, Certific
                             ate Policy, Default Domain Policy...}
ComputerCSEsProcessed      : {Registry, Security}
UserCSEsProcessed          : {}


PS C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet> _
```

Bild 1: Die erfolgreiche Verarbeitung der Gruppenrichtlinien weist Get-SDMGPHealth im "OverallStatus" aus

und rufen dort das installutil auf, mit dem die Datei *GetSDMGpHealth.DLL* aus dem Installationsordner des Cmdlets startet:

```
installutil "c:\Program Files
  (x86)\SDM Software\Group Policy
  Health Cmdlet\GetSDMGPHealth.DLL
```

Anschließend starten Sie die PowerShell über das Startmenü unter "Programme / SDM Software / Launch PowerShell with …" neu. Für 64 Bit-Versionen von Windows, wie sie in Server 2008 R2 nur noch vorhanden sind, müssen Sie die 64 Bit-Version von *installutil* im Ordner Standardordner *C:\Windows\Microsoft.NET\Framework64\v2.0.50727* aufrufen. Der Basisaufruf des Cmdlets erfolgt per *Get-SDMGPHealth* – alle Parameter werden an den Befehl angehängt. Um einen Statusreport eines Computers namens "Dell630" einzuholen, geben Sie also *Get-SDMGPHealth -computer Dell630* ein. Der Computername wird dabei mit dem Switch "-computer" übergeben.

Dieser Befehl listet einige Informationen zur GP-Verarbeitung auf. Nicht nur den Gesamtstatus mit Ampelfarbe, sondern auch die benötigte Zeit zur Verarbeitung, den gerade eingeloggten Benutzer, die Liste aller Richtlinien, die bei der Verarbeitung berücksichtigt wurden und die Client Side Extensions, die bei der Verarbeitung aufgerufen wurden. Da die Listen der ComputerGPOsProcessed und UserGPOsProcessed zur Übersichtlichkeit abgeschnitten wurden, können Sie diese für eine nähere Betrachtung mit "select" vollständig angezeigen lassen:

```
Get-SDMGPHealth -computer dell630 |
  select -expand ComputerGPOs
  Processed
```

Sind diejenigen Richtlinien für den gerade betrachteten Rechner interessant, die Sicherheitseinstellungen beinhalten, dann kann das Expandieren und anschließende Filtern nach "Security" des Objektes "ComputerCSEsProcessed" ein Weg sein:

```
Get-SDMGPHealth -computer dell630 |
  select -expand ComputerCSEsProces-
  sed | ? {$_.ExtensionName
  -contains "Security" }
```

Für die Massenprüfung von Clients ist eine Einzelverarbeitung aber alles andere als ein Patentrezept. Mit dem Schalter "-OU" lassen sich mehrere Clientcomputer prüfen, die in derselben OU liegen – hier im Beispiel die Domain Controller-OU:

```
Get-SDMGPHealth -OU "OU=Domain
  Controllers,DC=intern,DC=frickel-
  soft,DC=net"
```

Enthält die OU Leerzeichen, müssen Sie diese CMD-typisch mit Anführungszeichen umschließen, damit sie vom Kommando als zusammenhängender Parameter erkannt wird. Um die Ausgabe etwas übersichtlicher zu gestalten, können Ergebnisse gekürzt und in Listenform per "ft" für "Format-Table" umgeformt werden:

```
Get-SDMGPHealth -OU "OU=Domain
  Controllers,DC=intern,DC=frickel-
  soft,DC=net" | ft Hostname,
  OverallStatus
```

Wie bereits erwähnt, kann das Cmdlet auch mehrere Computer nacheinander verarbeiten, wenn die Pipe entsprechend eingesetzt wird. Bereiten Sie eine Textdatei vor, in der die zu suchenden Computernamen bereits enthalten sind. Die Liste sollte pro Zeile einen Computernamen enthalten und wird wie folgt in das Skript gepipet:

```
Get-Content C:\Group Policy
  Reports\computer.txt |
  %{Get-SDMGPHealth -computer $_} |
  ft Hostname, Overallstatus
```

Ergebnisse einzelner Rechner gibt das Skript sehr detailliert im XML-Format aus, wenn Sie den Schalter "-OutputByXML" verwenden. Dann nämlich wandelt das Skript all seine Ausgaben in ein XML-Objekt um, das dann per Save-Methode in der PowerShell beliebig weggespeichert oder weiterverarbeitet werden kann:

```
(Get-SDMGPHealth -ComputerName
  dell630
  -OutputByXML).Save("C:\Group
  Policy Reports\output.xml")
```

Die Klammern um den eigentlichen Befehl ermöglichen es, die Save-Methode für XML-Objekte aufzurufen, der dann der Pfad zur Speicherung des Ergebnisses mitgeteilt wird. *(dr)*

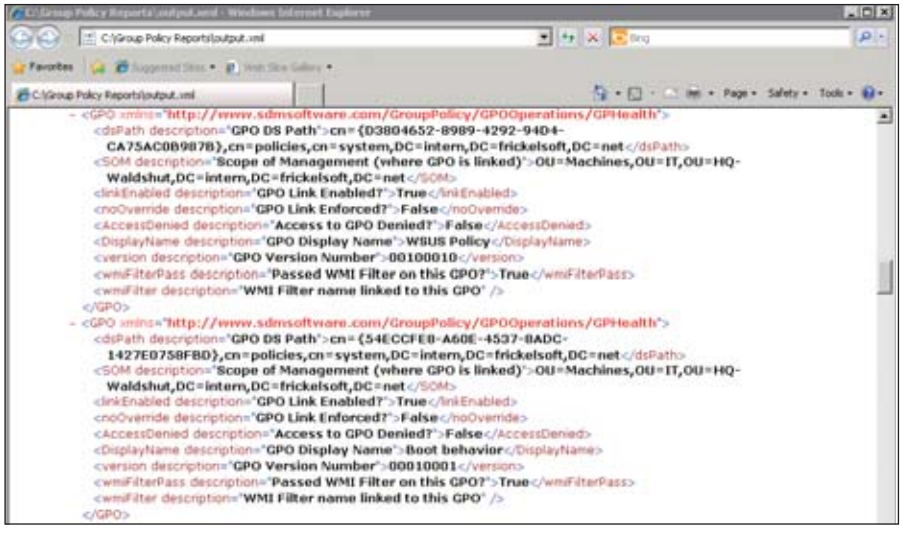


Bild 2: Per XML-Datei erhalten Sie die Ergebnisse Ihres Skriptes

[1] SDM Software Group Policy Freeware
www.sdmsoftware.com/freeware.php

Links

Quests Spotlight on Active Directory

AD-Überwachung in Echtzeit

Das Active Directory gestaltet sich sehr komplex, ist für den Verzeichnisdienst doch ein Zusammenspielen unterschiedlichstern Komponenten notwendig. Mit "Spotlight on Active Directory" von Quest können Sie den Zustand des Active Directory und der Domänencontroller in Echtzeit überwachen und Diagnosen durchführen.

Zeitsynchronisation, Namensauflösung über DNS, Firewalls im Netzwerk, Dateireplikation, sowie die Replikation, Kerberos und LDAP-Komponenten des Verzeichnisdienstes: Das Active Directory (AD) funktioniert nur dann richtig, wenn eine ganze Menge Komponenten zusammenspielen. Dies erschwert jedoch auch die Überwachung und Diagnose. Empfehlenswert bei der Performance-Überwachung ist, dass Sie sich die für den Server wichtigsten Werte zusammensuchen und eine Überwachung durchführen, wenn das System normal funktioniert. Nur dann wissen Sie, welche Werte abweichen, wenn Sie auch im Fehlerfall die Performance betrachten müssen. In der Realität ist dies allerdings nur selten machbar, so dass eine Messung nur dann durchgeführt wird, wenn ein Problem aufgetreten ist. Quest bietet mit Spotlight on Active Directory ein Werkzeug für das "Live-Monitoring" sowie die Diagnose des Verzeichnisdienstes.

Lieferumfang

Quest liefert in der Suite "Spotlight on Active Directory Pack 1.2" neben Spotlight on AD auch die ehemaligen Netpro-Werkzeuge "Directory Analyzer" und "Directory Troubleshooter" mit. Die Tools sind teilweise redundant, bieten Ihnen aber den größtmöglichen Funktionsumfang. Es ist zu erwarten, dass das Softwarehaus die Werkzeuge mit der Zeit zusammenführt.

Das Spotlight on Active Directory, das wir in diesem Artikel besonders betrachten wollen, kommt mit unterschiedlichen Komponenten daher: Der "Spotlight on Active Directory Topology Viewer" erlaubt Ihnen, die Standort- und Replikationsinfrastruktur zu betrachten, liefert in Farben einen "Gesundheitsstatus" der unterschiedlichen Komponenten und bietet unterschiedliche Diagnosemöglichkeiten. Sie können an jeder Stelle mit dem "Drill-Down" mehr Details erfahren. Eines dieser Details ist mit "Spotlight on Active Directory" der detaillierte Gesundheitszustand jedes DCs, sowie mit der darin ebenso enthaltenen Komponente "Spotlight on Windows" der Systemzustand des selbigen.

Die Suite von Quest ist kostenpflichtig, die Lizenzierung basiert auf der Anzahl an Domänencontrollern im Unternehmen. Allerdings ist der endgültige Preis häufig Verhandlungssache. Eine vollständige Testversion steht unter [1] zur Verfügung, die Anforderung eines Lizenzschlüssels hierfür ist unkompliziert. Betrachten wir aber zunächst einmal die Installation.

Installation

Da das Highlight des Werkzeugs die grafische Darstellung der Zustände der unterschiedlichen Komponenten der Replikationstopologie, des Active Directory sowie des Systemzustandes auf jedem Domänencontroller ist, empfiehlt es sich, das Tool auf einem separaten System laufen zu lassen. Bei Unternehmen, bei denen es sich im Einsatz befindet, ist häufig ein großer Monitor zentral aufgestellt, der die Konsole anzeigt. Je nachdem ob die "Web Reports" installiert werden, müssen auf dem "Monitoring-System" die Internet Information Service vorhanden sein. Des Weiteren ist eine Datenbank nötig. Hier bieten sich entweder die konstenfreie Version "SQL-Express" oder ein vollwertiger SQL-Server an. Ab 51 Domänencontrollern empfiehlt Quest die Enterprise-Version des SQL-Servers.

Die Installation mit einem Assistenten lässt sich unkompliziert durchführen, allerdings muss der SQL-Server vorher installiert sein und während der Installation angegeben werden. Hierbei ist zu beachten, dass die Express-Version sich mit der In-

Bild 1: "Rot" bedeutet Gefahr: Hier sollten Sie die Directory-Replikation überprüfen. Spotlight zeigt den Fehler vielleicht sogar, bevor es die Benutzer oder andere Admins merken.

stanz "SQLExpress" installiert. Als Server wählen Sie daher die Form "SQL-Computername\SQLExpress". Die Software ist dann schnell aufgesetzt und kann sofort, auch ohne Neustart, verwendet werden. Auf den Domänencontrollern wird nichts installiert, je nach Konfiguration kann es sein, dass zusätzliche Performancecounter für das AD aktiviert werden.

Schlauer Topology Viewer

Nach der Installation starten Sie den "Spotlight on Active Directory Topology Viewer" und führen am besten zunächst ein "Discovery" durch – also ein Entdecken der Infrastruktur. Dann werden die einzelnen Standorte, Replikationsverbindungen und Server angezeigt. Quest benutzt über alle Komponenten hinweg ein einfaches Farbschema: wenn etwas grün ist, ist alles in Ordnung, gelb bedeutet erhöhte Last ist oder einen wahrscheinlich (noch) unkritischen Fehler, bei Rot sollten Sie ganz genau hinsehen. Im linken Navigationsbereich können Sie zwischen verschiedenen Ansichten wählen: Topologie, die Testergebnisse von Analysen, Ergebnisse von Verwaltungsaufgaben (Management Action Results) oder erstellte Web-Reports.

Im Aktionsbereich auf der rechten Seite lassen sich verschiedene Test durchführen, Standard-Verwaltungskonsolen wie "Active Directory-Benutzer und -Computer" aufrufen, oder Replikationsfehlern auf den Grund gehen. Die Assistenten bieten die am meisten genutzten Funktionen einfach an, müssen aber je nach Bedarf auch einmal angepasst werden. Zum Beispiel achtet die FSMO Best Practice Analyse nicht darauf, ob es sich um eine einzelne Domäne handelt oder jeder Server Globaler Katalog ist – wenn der Infrastrukture Master auf einem GC läuft, zeigt das Tool trotzdem einen "roten" Status an. Daher sollten Sie in diesem Fall auswählen, genau diese Best-Practice nicht zu prüfen, was aber gleich zu Beginn des Assistenten abgefragt wird.

Die Diagnosen lassen sich zwar anpassen, bieten aber bereits standardmäßig eine sehr sinnvolle Konfiguration für die meisten Szenarien. Dabei werden echte Diagnosen durchgeführt, so zum Beispiel berechnet das Werkzeug bei DNS-Einträgen, welche existieren sollten. Das mit dem Betriebssystem gelieferte DcDiag überprüft hingegen nur, ob die Einträge, die in der Datei *netlogon.dns* stehen, auch eingetragen wurden, nicht ob diese schlüssig sind. Die im Spotlight durchgeführten Tests sind gründlich, zum Beispiel wird für die Replikationsanalyse ein Objekt erstellt und dann überprüft, wie dieses über die verschiedenen Domänencontroller hinweg repliziert.

Beim Dateireplikationstest lassen sich auch einzelne Dateien dahingehend überprüfen, ob diese auf den Replikationspartnern identisch sind. Außerdem wird der Status von Gruppenrichtlinien daraufhin überprüft, ob die GPOs identisch zu denen auf dem PDC sind. Dies ist sehr nützlich und hilft darüber hinweg, dass die Analyse zur Dateireplikation nur NTFRS, nicht aber DFS-R unterstützt. Aber da die meisten Infrastrukturen heute noch NTFRS verwenden, sei dem Hersteller hierfür auch noch etwas Zeit gegönnt.

Auch auf den unterschiedlichen Servern lassen sich mit der rechten Maustaste das Discovery, die Diagnosen und die Assistenten zum Lösen von Problemen direkt aufrufen. In den Eigenschaften werden die Stati unterschiedlicher Komponten angezeigt. Wählen Sie im Kontextmenü eines Servers unter "Diagnose" oder im Aktionsbereich den Punkt "Launch Diagnostic Console", landen Sie in der Diagnose-Konsole "Spotlight on Active Directory", die einen detaillierten Überblick über den Zustand des Systems und des Active Directory erlaubt.

Futuristische Diagnose-Konsole

Die Diagnose-Konsole erinnert ein wenig an Raumschiff Enterprise: Hier werden die für das Active Directory relevanten Komponenten grafisch animiert und deren Zustand farblich dargestellt. Existieren viele Replikationen, bewegen sich die Pfeile schneller. Ist die Schlange an abzuarbeitenden Operationen zu lang, ändert sich der Status auf gelb oder rot. So erlangen Sie sehr schnell eine gute Übersicht über den Zustand Ihres Domänencontrollers.

In der Navigationsleiste auf der rechten Seite können Sie für jeden Domänencontroller zwischen der Ansicht "Spotlight on AD" oder "Spotlight on Windows" wählen, um entweder AD- oder systemrelevante Stati zu erhalten. Bemerkenswert sind die Funktionen, die sich hinter der Konsole verstecken. Klicken Sie mit der Maus auf eine der Komponenten, erhalten Sie zum einen die Information darüber, was sich dahinter verbirgt, können aber auch einen "Drilldown" auswählen, um Statistiken oder mehr Details zu der Komponente zu erhalten. Die Administration nach Farben ermöglicht es, relativ leicht die Infrastruktur am Laufen zu erhalten. Aus einer Analyse kommen Sie mit dem Home-Symbol in der Menüleiste immer zurück auf den Überblick.

Fazit

Spotlight on Active Directory ist eine Suite aus Tools und Konsolen, die Ihnen das Leben einfacher machen: Sie können den Gesundheitszustand der wichtigen Komponenten erkennen, häufig noch bevor Benutzer oder andere Administratoren merken, dass etwas nicht stimmt. Die Lizenzierung pro Domänencontroller ist hierbei fair. Daneben ist die Integration in weitere Werkzeuge interessant: Spotlight on AD wurde optimiert, um den Active Directory- und Betriebssystem-Status zu überprüfen und kann seine Ergebnisse an das System Center, MOM oder als SNMP-Traps weiterleiten. Verwenden Sie auch Spotlight on Exchange, integrieren sich die Konsolen und vereinfachen das Überprüfen. Und wenn Sie "InTrust" von Quest nutzen, können Sie sich aus dem Spotlight heraus die Änderungen am AD in der letzten Zeit berichten lassen. *(dr)*

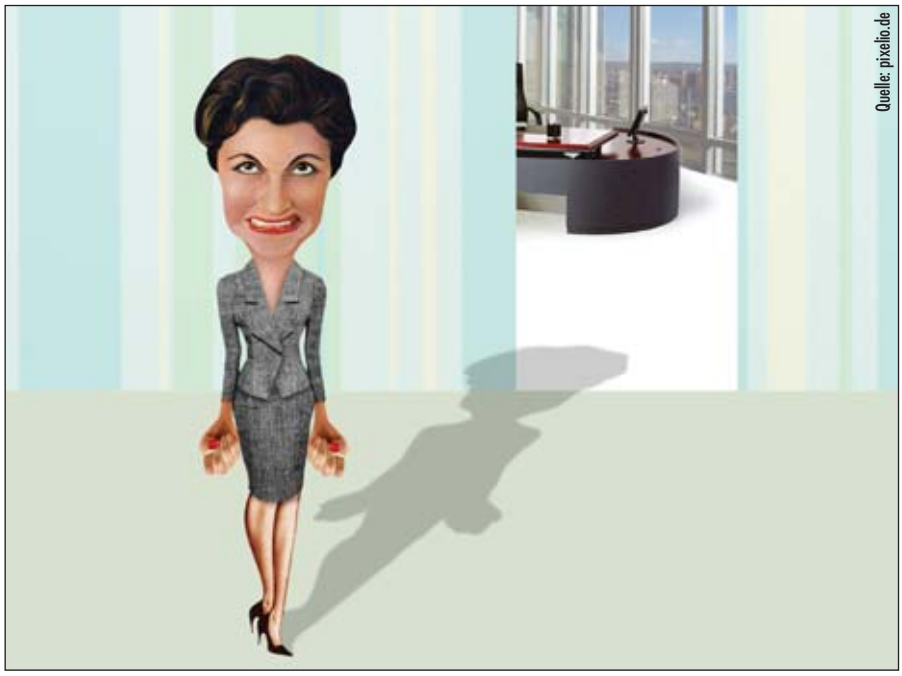
[1] Quests Spotlight on Active Directory Pack
www.quest.com/spotlight-on-active-directory-pack/

Links

Active Directory-Replikation meistern

Verteilte Ordnung

Das Active Directory ist das Rückgrat moderner Windows-Netzwerke. Meist versieht es klaglos seinen Dienst und toleriert einzelne Serverausfälle oder auch einen großen Netzwerk-Umbau. Hin und wieder jedoch steht der Administrator vor Problemen mit dem Datenabgleich – der Replikation der gemeinsamen Datenbank. Die folgenden Workshops beleuchten Hintergründe, Technik und Praxis der komplexen AD-Replikation.



Frau Ellen Bogen hat kürzlich geheiratet und nun zusätzlich den Namen ihres Mannes angenommen – alle wissen Bescheid, nur das Active Directory nicht

Das Active Directory (AD) basiert auf dem Lightweight Directory Access Protocol (LDAP), das den Zugriff auf große Objektmengen, die sich in Unternehmen meist als hierarchische Struktur darstellen, ermöglicht. Schon der Grundentwurf des "NT Directory Service", wie der Dienst zunächst Microsoft-intern hieß, hatte ehrgeizige Ziele: Er sollte die zentrale Anmeldung (Single Sign-on) an allen Servern und Workstations ermöglichen, gleichzeitig aber mit älteren Clients kompatibel bleiben. Mechanismen zur Lastverteilung und Ausfallsicherheit sowie die Integration von Anwendungsdaten betonten die Eignung für große Unternehmen. Den Administratoren sollten Funktionen wie ein zentrales Client-Management bei gleichzeitig dezentraler Verwaltbarkeit zugutekommen. Und schließlich band Redmond seine detaillierte Berechtigungssteuerung in den Dienst ein, der schon bei den Dateidiensten Maßstäbe gesetzt hatte.

Den technischen Kern des AD bildet ein ausgefeiltes Replikationssystem, das den Anwendern ermöglicht, die logische Domänenstruktur unabhängig von der Netzwerktopologie zu betreiben. Das AD beruht auf einer selbsterzeugenden Multi-Master-Replikation: Alle Domänencontroller (DC) einer Domäne haben denselben lesenden und schreibenden Zugriff auf die Verzeichnisdatenbank. Fällt ein DC aus oder fügt der Administrator einen weiteren hinzu, so berechnet AD selbst die günstigste neue Replikationsstruktur, um alle DCs mit den aktuellen Daten zu versorgen. Auf diese Weise ist der Verzeichnisdienst skalierbar von kleinen Umgebungen bis zu weltweiten Konzernnetzen.

In einer solch verteilten Datenbank können jedoch viele Konflikte entstehen, wenn Änderungen nicht zusammenpassen, die Administratoren verschiedener Standorte vornehmen. Daher umfasst das AD Behandlungsroutinen für typische Administrationsfehler. Legen entfernt voneinander arbeitende Administratoren etwa neue Benutzerobjekte mit denselben Namen an, so benennt das AD automatisch eins der Konten um und vermeidet so die Kollision. Ähnlich geht es in anderen Fällen vor (siehe Kasten "Konflikte vermeiden").

Aufbau der Replikationstopologie

Um seine mächtige Replikationstechnik auszunutzen, teilt das AD seine Datenbank in mehrere Partitionen ein, so genannte "Namenskontexte" (Naming Context, NC). Der bekannteste ist der Domänen-Namenskontext, in dem sich alle produktiven Objekte der jeweiligen Domäne befinden. Diese Partition repliziert sich vollständig zwischen allen DCs derselben Domäne.

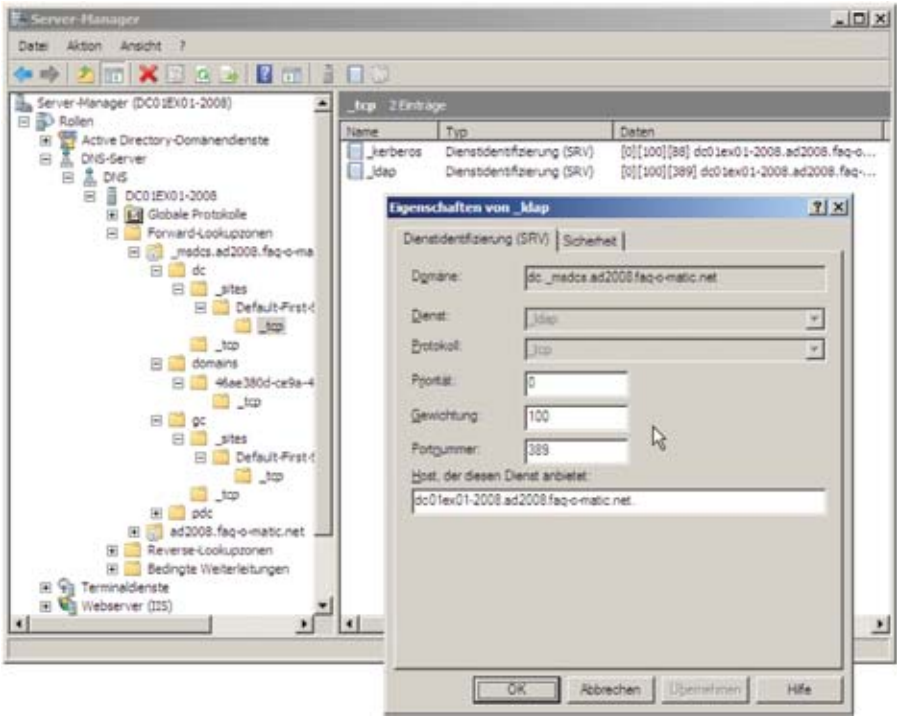


Bild 1: Zentral gepflegt: Das Active Directory legt zahlreiche Einträge im DNS an, über die Clients die zugehörigen Dienste finden

Separate Replikationstopologien baut das AD für seine Konfigurationspartition und für das Schema auf. Im "Configuration NC" speichert das AD Informationen zur Replikation und auch Applikationen können sich hier eintragen, so etwa Exchange. Die Konfigurationspartition replizieren alle DCs des gesamten AD-Forest, denn sie ist domänenübergreifend gültig. Gleiches gilt für das Schema, also die Datenbankdefinition, die festlegt, wie Objekte und Attribute beschaffen sind. Mit *ADSI Edit* können Sie sich diese speziellen Partitionen einmal ansehen. In Windows Server 2008 ist das Programm bereits enthalten, auf früheren Versionen installieren Sie es aus den Support Tools nach. Führen Sie auf dem obersten Knoten einen Rechtsklick aus und wählen Sie "Verbinden". Das Programm fragt Sie dann nach dem Namenskontext, den Sie unter "Bekannten Namenskontext auswählen" in der Liste markieren.

In Windows Server 2003 hat Microsoft einen weiteren Partitionstyp eingeführt: Applikations-Namenskontexte. So ist es dem AD möglich, Daten bestimmter Anwendungen separat von den "technischen" AD-Daten zu replizieren. Von Haus aus liegen DNS-Daten in solch einer Partition, doch Administratoren können auch eigene "Application Partitions" erzeugen. Die Replikation der DNS-Partition können Sie über die GUI festlegen. Rufen Sie dazu im DNS-Snap-In mit einem Rechtsklick die Eigenschaften der DNS-Zone auf. Unter "Allgemein" nutzen Sie dann den Button "Ändern" für die Replikation, um die Einstellung zu bearbeiten. Für andere Applikationspartitionen müssen Sie, falls die jeweilige Applikation kein Verwaltungstool hat, das Werkzeug *NTDSUtil* nutzen. Näheres dazu finden Sie bei Bedarf in Microsofts TechNet [1].

Um die Replikationstopologie zu erzeugen, benötigt das AD Informationen zum Aufbau des Netzwerks. Diese holt es sich nicht selbst, sondern der Administrator muss einige Rahmendaten zur Verfügung stellen. Entscheidend sind dabei die LAN-Standorte, aus denen das Netz besteht, und die Qualität der WAN-Verbindungen dazwischen: Netzwerke mit "schnellen" Verbindungen betrachtet AD als "Standorte" (Sites). Als weitere Anforderung kommen eindeutige IP-Subnetze hinzu: Ein IP-Netzwerkbereich (etwa 192.168.1.0/24) muss vollständig zu einem Standort gehören; Adressen dieses Bereichs dürfen an anderen Standorten nicht vorkommen. Umgekehrt kann eine Site aber durchaus mehrere IP-Subnets beherbergen.

Die Leitungsgeschwindigkeit zwischen Standorten geben Sie nicht etwa in Bits pro Sekunde an, sondern nur relativ zueinander als abstrakten "Kostenwert". Dieser ist numerisch; als Standard gibt das AD den Wert 100 vor. Eine langsame

Das Active Directory kann viele Replikationskonflikte erkennen und beheben. Die wichtigsten Mechanismen:

- **Objektnamenskonflikt:** Erzeugen zwei Admins an verschiedenen Servern etwa zur selben Zeit mehrere Objekte mit demselben Namen, so benennt AD das "jüngere" Objekt um. Dazu hängt es an den Namen die Zeichenfolge "CNF:" (für Conflict) sowie die intern eindeutige Kennung (Globally Unique Identifier, GUID) an. Es empfiehlt sich, in großen Umgebungen regelmäßig nach solchen Namen zu suchen und die Objekte manuell zu bearbeiten. Hierfür können Sie in der benutzerdefinierten Suche der AD-MMC den Suchstring "(name=*CNF*)" nutzen.
- **Attributwertkonflikt:** Ändert ein Administrator den Nachnamen eines Benutzerobjekts auf "Müller" und gleichzeitig ein anderer denselben Namen auf "Meyer", so übernimmt AD die zeitlich letzte Änderung. Der andere Wert wird kommentarlos überschrieben. Erst Windows Server 2008 bietet dafür eine Protokollfunktion auf Attributebene, die aber zunächst aktiviert werden muss. Dazu definieren Sie in der Default Domain Controllers Policy zunächst allgemein die Überwachung für den Verzeichnisdienstzugriff. Danach schalten Sie über die Kommandozeile die Werteverfolgung ein:
  `auditpol /set /subcategory:"directory service changes" /success:enable`
- **Verwaister-Container-Konflikt:** Legen Sie in der OU "Vertrieb" ein neues Objekt an, während ein Kollege gerade die OU "Vertrieb" löscht, so verschiebt AD das neue Objekt bei der nächsten Replikation in den Container "LostAndFound" (standardmäßig ausgeblendet). Ein so "verwaister" Benutzer kann sich also anmelden, befindet sich aber nicht im richtigen Verwaltungsbereich der Domäne.

Konflikte vermeiden

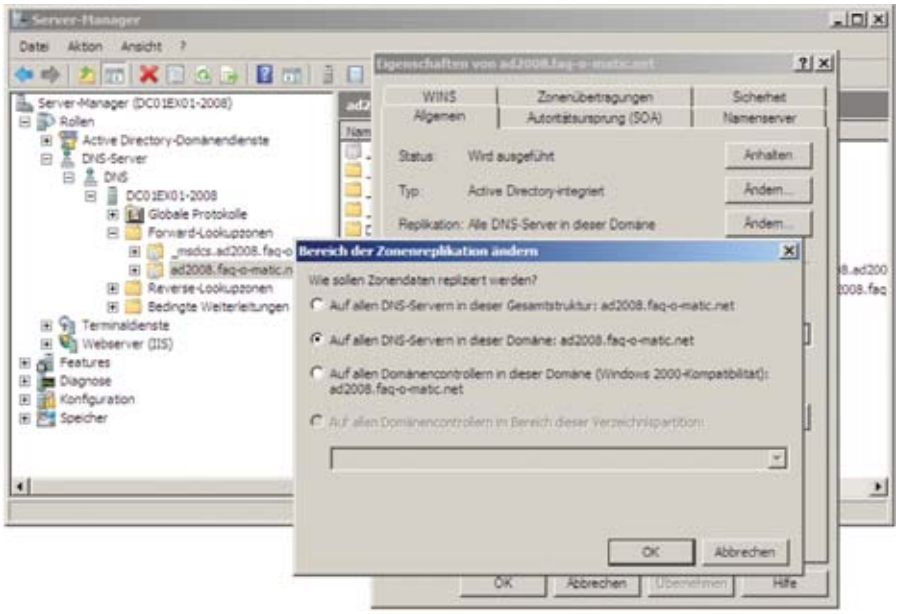


Bild 2: Für Applikationspartitionen des AD (hier die DNS-Partition) kann der Administrator den Replikationsbereich selbst festlegen

Verbindung bekommt hohe Kosten (beispielsweise 200 oder 1.000), eine schnelle dementsprechend niedrige. Gibt es nun mehrere mögliche Verbindungen zwischen zwei Standorten, so wählt AD die mit den geringsten Kosten. Sollte diese nicht verfügbar sein, nimmt AD den Weg mit den nächst höheren Kosten – ähnlich einer Routing-Tabelle (näheres hierzu beleuchten wir im weiteren Verlauf des Workshops).

Verteilung von Änderungen im AD

Die Replikation der Änderungen verwirklicht das Active Directory über Benachrichtigungen, sogenannte "Change Notifications", die die direkten Replikationspartner erhalten. Direkte Replikationspartner sind hierbei andere Domänencontroller, die sich in der Site des Quelldomänencontrollers befinden. Welcher DC direkt mit welchem anderen repliziert, bestimmt ein Active Directory-interner Dienst, der Knowledge Consistency Checker (KCC), über den Aufbau der Replikationstopologie.

Der Quell-Domänencontroller sendet nach Ablauf einer kurzen Wartezeit seine Change Notification an seine direkten Replikationspartner. Diese Wartezeit ist sehr wichtig, um nicht bei jeder Änderung eine separate Benachrichtigung versenden zu müssen, sondern im Falle mehrerer Änderungen in einem kurzen Zeitintervall eine Benachrichtigung für alle Änderungen versenden zu können. Die Wartezeit beträgt für Windows Server 2003 und Server 2008 15 Sekunden, während Windows 2000 ganze fünf Minuten wartet. Für darauffolgende Änderungen wird die Wartezeit verkürzt – hier werden lediglich drei Sekunden in Windows Server ab 2003 oder 30 Sekunden in Windows 2000 gewartet. Benachrichtigte DCs können daraufhin die Änderungen an den NCs über den Quell-Domänencontroller abfragen. Deshalb ist bei der AD-Replikation auch von einer "Pull"-basierten Replikation die Rede. Änderungen an den Namenskontexten werden nicht per "Push" an die Replikationspartner gesendet, sondern vom Quelldomänencontroller zur Verfügung gestellt.

Steuerung der Replikation

Das Sicherstellen der Replikation und das effiziente Verteilen von Neuigkeiten ist Aufgabe des KCC. Der KCC läuft als Dienst in einem Intervall von 15 Minuten auf allen Domänencontrollern und prüft die Konfiguration in "Active Directory-Standorte und -Dienste" und der darin hinterlegten Parameter, um daraufhin eine Replikationstopologie für alle verfügbaren Domänencontroller zu erstellen. Aus dieser Replikationstopologie ist zu entnehmen, welcher Domänencontroller Aktualisierungen von welchen anderen Domänencontrollern empfangen kann. Der KCC versucht stets, einen bidirektionalen Ring von Domänencontrollern zu erstellen, in dem sich Ringnachbarn über Änderungen informieren und die Replikation initiieren. Eine Replikationstopologie wird pro Namenskontext erstellt. In großen Gesamtstrukturen mit mehreren Domänen bedeutet dies, dass für die Domänenpartitionen und die forestweiten Partitionen getrennte Replikationspläne erstellt werden müssen. In übersichtlicheren Gesamtstrukturen mit nur einer Domäne kann es sich der KCC jedoch leicht machen: Da alle Domänencontroller dieselben NCs besitzen, genügt eine Topologie für alle Namenskontexte.

Um der Replikationsdaten Herr zu werden und die von anderen Domänencontrollern empfangenen Aktualisierungen der Namenskontexte einpflegen und prüfen zu können, bedarf es eines Mechanismus, Änderungen anhand ihrer Reihenfolge sortieren zu können. Schließlich soll es nicht passieren, dass DC1 die aktuellen Änderungen von DC2 repliziert und DC3 später einen älteren Stand der Objektdaten nach DC1 repliziert und die Neuerungen überschreibt, weil DC3 selbst noch nicht die neuesten Änderungen von DC2 empfangen hat.

Verteilte Systeme begegnen diesem Problem auf unterschiedliche Arten. Für das Active Directory böte sich an, einen Änderungszeitstempel als Kriterium zu verwenden – schließlich ist die Zeit auf allen Domänencontrollern und Clientcomputern der Domäne nahezu gleich, was eine zwingende Voraussetzung für das Authentifizieren mit Kerberos ist. Da das Active

Directory aber unter Umständen aus mehreren hundert verschiedenen Knoten in unterschiedlichen Standorten mit variierenden Latenzen bestehen kann, reichen "nahezu" synchrone Uhren nicht aus.

USN und HWMV steuern die Replikation

Das AD verwendet deshalb mehrere Vektoren, die bei Änderungen erhöht werden und bei der Replikation zwischen den beiden Partnern ausgewertet werden. Sie speichern dabei die Datenbankstände anderer Domänencontroller. Einer dieser Vektoren ist die "Update Sequence Number" (USN). Jeder DC besitzt eine eigene USN, die bei jeder durchgeführten Datenbank-Transaktion automatisch erhöht wird. Eine Objekterstellung wird ebenso als eine Transaktion gewertet wie das Ändern eines einzelnen Benutzerattributes, etwa des Nachnamens oder der "Beschreibung". Dabei wird die USN sowohl mit den in der Transaktion geänderten Attributen gespeichert als auch im Attribut "highestCommitedUSN" des Verzeichnisdienstkopfes (rootDSE) hinterlegt.

Um zu wissen, welchen Datenstand ein Domänencontroller bereits von einem anderen repliziert hat, merkt sich jeder DC die USN der Namenskontexte seiner Replikationspartner. So können DCs, die Änderungen von ihren Partnern anfragen, den letzten Stand (USN) des Namenskontextes, den sie per Replikation mit diesem Partner erhalten haben, mit in der Anfrage senden. Partner können auf diese Weise nur die Änderungen vorbereiten und replizieren, die seit der letzten erfolgreichen Replikation vorgenommen wurden. Die USN-Stände der letzten Replikation werden im so genannten "High-Watermark Vector" (HWMV) gespeichert.

Beispiele für den High Watermark Vector von DC-1

Namenskontext	Replikationspartner	HWMV
Domänen-NC	DC-2	766474
Domänen-NC	DC-3	222934
Configuration-NC	DC-2	723222
Configuration-NC	DC-3	179682
Schema-NC	DC-2	758860
Schema-NC	DC-3	215320

Beispiele für den High Watermark Vector von DC-2

Namenskontext	Replikationspartner	HWMV
Domänen-NC	DC-1	866548
Domänen-NC	DC-3	222934
Configuration-NC	DC-1	823296
Configuration-NC	DC-3	179682
Schema-NC	DC-1	758860
Schema-NC	DC-3	858934

UTDV verhindert Endlosschleifen

Zu guter Letzt wird ein weiterer Vektor benötigt, der "Up-To-Dateness"-Vektor (UTDV), der dem HWMV ähnelt. Dieser Vektor speichert allerdings nicht nur die USNs der aktuellen direkten Replikationspartner. Für den Up-To-Dateness-Vektor werden alle letzten USNs jeglicher Partner gespeichert, von denen ein Domänencontroller jemals einen so genannten "Originate Change" repliziert hat – dies schützt vor Endlosschleifen bei der Verteilung von Aktualisierungen.

Die Replikation unterscheidet zwischen zwei eingehenden replizierten Änderungen: "Originate Change" bezeichnet Änderungen, die auf einem direkten Partner vorgenommen wurden und direkt von diesem Partner übernommen wurden. "Replicated Changes" sind hingegen Änderungen, die ein entfernter DC vorgenommen hat und die mit Hilfe eines direkten Replikationspartners, der die Änderungen bereits empfangen hat, repliziert wurden. Der direkte Replikationspartner hat die Änderung also nicht selbst erstellt, sondern ist nur "Mittelsmann" bei der Änderungspropagierung.

Zusammenspiel der Vektoren

In welcher Art und Weise die Vektoren zusammenspielen und welche Bedeutung sie bei der Replikation haben, wird durch ein Beispiel deutlich. Im nachfolgenden Szenario wurde ein Forest mit einer Domäne erstellt. Die Domäne hat drei Domänencontroller, DC-1, DC-2 und DC-3. DC-4, ein Test-Domänencontroller, wurde vor einiger Zeit wieder zum Mitgliedsserver heruntergestuft. Die Tabellen zeigen die HWMV und UDTV der aktiven Domänencontroller. Da der UTDV die USNs aller direkten Replikationspartner speichert, damit auch die derer, die in der Zwischenzeit nicht mehr verfügbar sind, wird DC-4 ebenfalls im Vektor aufgeführt.

In unserem Beispiel wird ein Attribut eines Benutzerobjektes verändert. Frau Ellen Bogen aus der Personalabeilung hat

kürzlich geheiratet und nun zusätzlich den Namen ihres Mannes angenommen. Um die Namensänderung auch korrekt im AD hinterlegen zu können, öffnet ein Administrator "Active Directory-Benutzer und -Computer" und verbindet sich daraufhin – automatisch – mit DC-1. Dort trägt er den neuen Namen ein: sie heißt jetzt Frau Ellen Bogen-Schmerz. Die Änderung an Ellens Benutzerkonto hat eine Erhöhung der USN auf DC-1 zur Folge, und zwar von 2555 auf 2556. DC-1 informiert daraufhin seine beiden Replikationspartner, DC-2 und DC-3, dass Änderungen am Domänen-NC vorgenommen wurden. DC-2 erhält die Change Notification und prüft den eigenen HWMV. Als Antwort auf die Change Notification sendet DC-2, neben anderen Parametern, wie etwa die maximal erlaubte Objektzahl für die Replikation oder den betreffenden Namenskontext, seinen kompletten UTDV und HWMV an DC-1. Aus dem HWMV von DC-2 kann DC-1 erkennen, dass die Namensänderung der Benutzerin Ellen noch nicht bei DC-2 eingetroffen ist und repliziert diese daraufhin. Als Anhang an die Replikationsdaten sendet DC-1 seine neue USN mit, sodass DC-2 nun die Replikationsdaten mit Ellens neuem Nachnamen, die USN von DC-1 und seine eigene USN inkrementieren kann. Die Änderungen speichert DC-2 in seiner HWMV und UTDV, da DC-1 ein direkter Replikationspartner ist und die Replikation ein Originating Update war.

Nun fordert DC-3 die Änderungen von DC-1 an – schließlich hat auch dieser DC die Change Notification erhalten. Auch hier wird die Replikation vorgenommen und die entsprechenden Vektoren angepasst – es resultieren die geänderten HWMV- und UTDV-Werte.

Der DC-3 hat nach der Replikation alle Änderungen von DC-1 übernommen. Auch DC-3 hat bereits seine USN erhöht (1468) und informiert nun DC-2 über die Änderungen an seinem Domänen-NC, da er nicht weiß, dass DC-2 bereits Änderungen direkt von DC-1 repliziert hat. Wie aus der HWMV-Übersicht rechts hervorgeht, kennt DC-2 alle Änderungen von DC-3 bis zur USN 1467. DC-3 hat allerdings durch das "Originating Update" von DC-1 und Ellens Nachnamen seine USN inkrementiert (1468). Dies würde bedeuten, dass die Namensänderung erneut repliziert wird. Da DC-2 aber nun seine komplette UTDV-Tabelle an DC-3 sendet, kann DC-3 erkennen, dass DC-2 zwar eine veraltete USN von ihm besitzt, in seinem UTDV für DC-1 aber die neueste Änderung von DC-1 (2556) bereits ebenfalls per Originating update repliziert hat. DC-3 muss also nichts weiter tun, als DC-2 seine neue USN (1468) schicken, damit DC-2 sie in seiner HWMV-Tabelle speichern kann. Aus dem Beispiel lässt sich erkennen, warum es eine HWMV-Vektortabelle und eine Up-To-Dateness-Vektortabelle gibt. Während der HWMV die aktuellen Aktualisierungsstände der direkten Replikationsnachbarn speichert, schützt der UTDV vor Replikationsschleifen.

Die High-Watermark-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	HWMV
DC-1 – HWMV (USN: 2555)	Domänen-NC	DC-2	2299
	Domänen-NC	DC-3	1467
DC-2 – HWMV (USN: 2299)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2555
	Domänen-NC	DC-3	1467
DC-3 – HWMV (USN: 1467)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2555
	Domänen-NC	DC-2	2299

Die Up-To-Dateness-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	UTDV
DC-1 – UTDV (USN: 2555)	Domänen-NC	DC-2	2299
	Domänen-NC	DC-3	1460
	Domänen-NC	DC-4	765
DC-2 – UDTV (USN: 2299)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2555
	Domänen-NC	DC-3	1467
	Domänen-NC	DC-4	765
DC-3 – UTDV (USN: 1467)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2534
	Domänen-NC	DC-2	2299
	Domänen-NC	DC-4	765

Problemerkennung

Sobald Sie einen Server zum Domänencontroller heraufstufen, versuchen die KCCs der anderen DCs eine Re-

plikationstopologie zu erstellen und das neue Mitglied einzubinden. So einfach sich die Replikation von allein regelt, so schleichend können Probleme auftreten. Oft bemerken Sie Probleme mit der Replikation erst, wenn Benutzer anrufen und sich beschweren, dass ihr gerade eben geändertes Passwort plötzlich nicht mehr funktioniert und sie das alte Passwort verwenden mussten – oder dass das Adressbuch in Outlook total veraltete Daten anzeigt. In diesen beiden Fällen kann eine gestörte Replikation das schuldige Übel sein, denn wenn sich Änderungen nicht replizieren lassen, könnten Benutzer mit veralteten Daten konfrontiert werden.

Leider heulen im AD keine Sirenen auf, wenn mit der Replikation etwas nicht in Ordnung ist oder wird der Administrator automatisch mit einer E-Mail zinformiert, wenn der Datenabgleich scheitert. Zwei einfache Methoden gibt es allerdings, die Replikation zu überprüfen und sich ein Bild zu machen, ob das verteilte System wirklich rund läuft. Eine Methode basiert auf der Ereignisanzeige von Windows. Beim Heraufstufen zu einem Domänencontroller erstellt der Assistent ein neues Ereignislog namens "Verzeichnisdienst". Hier protokolliert AD alle Ereignisse. Gibt es Probleme mit der Replikation, lässt sich dies anhand dieses Ereignislogs erkennen – der KCC meldet etwa alle 15 Minuten, wenn es Schwierigkeiten mit der Erstellung der Replikationstopologie geben sollte.

Das Eventlog wird im Fehlerfall also regelrecht vollgeschrieben. Ist es allerdings ruhig um die Verzeichnisdiensteinträge, ist davon auszugehen, dass auch die Replikation erfolgreich funktioniert. Wer keine Serververwaltungssoftware wie beispielsweise System Center Operations Manager einsetzt, die Eventeinträge sammelt und die Gesundheit der Server überwacht, kann sich mit Visual-Basic- oder Powershell-Skripting oder mit bereits fertigen Tools wie EventComb [2] Ereignisse aus der Ereignisanzeige sammeln und automatisiert zustellen lassen. EventComb ist ein Programm aus dem Windows Server 2003 Resource Kit, das Ereignisanzeigen vorgegebener Computer nach Ereignissen durchsuchen kann. Gefiltert nach den Ereignis-IDs 1311, 1566 und 1865 lassen sich so zumindest die häufigsten Replikationsprobleme sammeln. Aber Vorsicht: Das Tool ist nur für eher kleine Umgebungen geeignet, in größeren gerät es schnell durcheinander.

Ein zweites, sehr wertvolles Kommandozeilenprogramm ist "repadmin" aus den Support Tools. Repadmin erlaubt es, den Status der letzten Replikation aller Namenskontexte abzufragen. Dabei zeigt es – abhängig vom DC, mit dem das Tool verbunden ist – pro Namenskontext an, mit welchen Domänencontrollern die Replikation versucht wurde und wann die letzte erfolgreiche Replikation stattgefunden hat. Aufgerufen mit dem Befehlsparameter "/showrepl" zeigt repadmin den Replikationsstatus an.

Replikationspfade anzeigen

Für einen oder alle verfügbaren Domänencontroller zeigt der Schalter "/showrepl" alle replizierten Namenskontexte und ihren letzten Replikationsstatus an.

Die geänderten High-Watermark-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	HWMV
DC-1 – HWMV (USN: 2556)	Domänen-NC	DC-2	2300
	Domänen-NC	DC-3	1468
DC-2 – HWMV (USN: 2300)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-3	1467
DC-3 – HWMV (USN: 1468)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-2	2299

Die geänderten Up-To-Dateness-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	UTDV
DC-1 – UTDV (USN: 2556)	Domänen-NC	DC-2	2299
	Domänen-NC	DC-3	1460
	Domänen-NC	DC-4	765
DC-2 – UDTV (USN: 2300)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-3	1467
	Domänen-NC	DC-4	765
DC-3 – UTDV (USN: 1468)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-2	2299
	Domänen-NC	DC-4	765

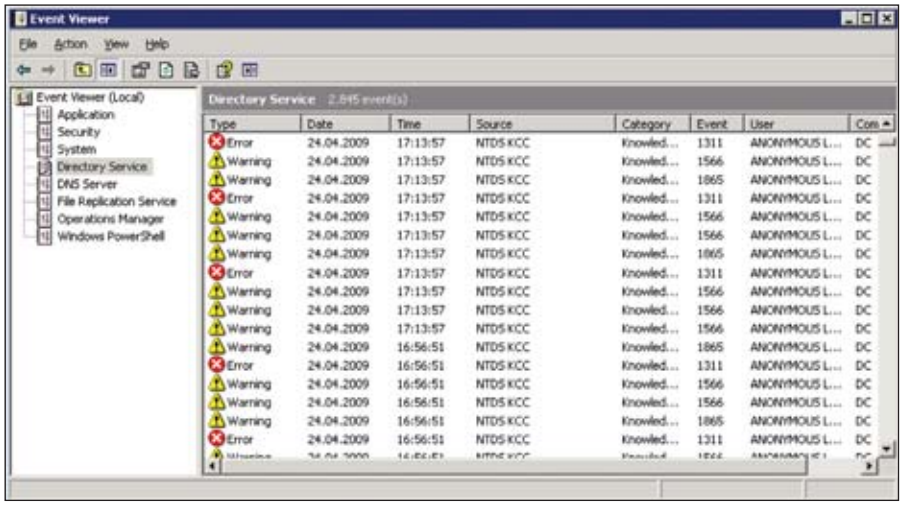


Bild 3: Die Ereignisanzeige informiert über auftretende Probleme bei der Replikation

Mit *repadmin /showrepl {DC-Name}* lässt sich ein beliebiger Domänencontroller für die Ausgabe angeben. Einzige Bedingung ist, dass der Domänencontroller erreichbar ist, da die Replikationsdaten direkt vom Zieldomänencontroller abgefragt werden. Um alle Domänencontroller der Gesamtstruktur abzurufen, verwenden Sie einen Stern als Jokerzeichen: *repadmin /showrepl ***

Je größer allerdings die Gesamtstruktur, desto schwieriger gestaltet sich der Überblick über die Replikationspfade und die Verteilung der Namenskontexte. Ausfälle und Änderungen bei Domänencontrollern oder Standortverbindungen versucht der Dienst "Knowledge Consistency Checker" (KCC) selbstständig zu korrigieren, was in Einzelfällen jedoch scheitern kann.

Um den möglicherweise verloren gegangenen Überblick wiederzuerlangen, bringt repadmin den Schalter "/csv" mit, der alle Ergebnisse im CSV-Format ausgibt. Wandeln Sie "showrepl" in das CSV-Format und leiten die Ausgabe in eine Datei um, können Sie das Ergebnis hervorragend etwa mit Excel analysieren: *repadmin /showrepl * /csv > C:\repadmin\gesamteReplikation.csv*

Dank der geordneten Struktur lassen sich nun, einfacher als über die Kommandozeile, Probleme zwischen Replikationspartnern, ganzen Standorten oder Namenskontexten erkennen. Tiefere Einblicke in die Active-Directory-Replikation ermöglichen die Schalter "/showutdvector" und "/showobjmeta". Während "showutdvector" den Up-to-Dateness-Vektor eines Namenskontextes auf einem bestimmten Domänencontroller anzeigt, gibt *showobjmeta* Metadaten eines Verzeichnisobjektes aus. Unter den angezeigten Metadaten befinden sich die Version des Attributes, die Update-Sequence-Number (USN) und der Name des DCs, der die letzte Änderung an einem Attribut vornahm. Das zu untersuchende Objekt geben Sie mit seinem "distinguishedName", dem Pfad im Verzeichnis, an: *repadmin /showobjmeta {DC-Name} {DN eines Objektes}*.

Nützlich ist *showobjmeta* bei der Betrachtung von Active Directory-Gruppen. Der Schalter zeigt an, ob Gruppenmitglieder per "Linked Value Replication" (LVR) aktualisiert werden. LVR, eingeführt in Windows Server 2003, verbessert das Replikationsverhalten, indem es bei mehrwertigen Attributen wie etwa Gruppenmitgliedschaften nicht mehr das vollständige Attribut mit allen Gruppenmitgliedschaften, sondern stets einzelne, geänderte Gruppenmitgliedschaften repliziert. Die unterschiedliche Replikation zeigt Repadmin mit den beiden Schlagworten "PRESENT" für das Server 2003-Replikationsverhalten und "LEGACY" für das Verhalten von Server 2000 an.

Sollte es einmal zu Replikationsproblemen kommen oder müssen Sie den Stand zweier Namenskontexte auf unterschiedlichen DCs vergleichen, zeigt das Feature "showchanges" seinen Nutzen. Der Schalter vergleicht hierbei die Updatenummernversion des Namenskontextes mit der zuletzt gespeicherten Version des angegebenen Domänencontrollers und listet alle Änderungen auf, die seit der letzten Replikation durchgeführt wurden. Die Syntax für diese Prüfung lautet: *repadmin /showchanges {DC-1-Name} {DSA GUID-DC-2} {Namenskontext}*. Der Schalter führt Änderungen am angegebenen Namenskontext auf DC-2 auf, die noch nicht von DC-1 repliziert wurden. Die DSA GUID, die "showchanges" als Parameter fordert, identifiziert einen DC während seiner kompletten Lebenszeit eindeutig – selbst wenn sich der Name des DCs ändern sollte. Die DSA GUID erhalten Sie mit *repadmin*

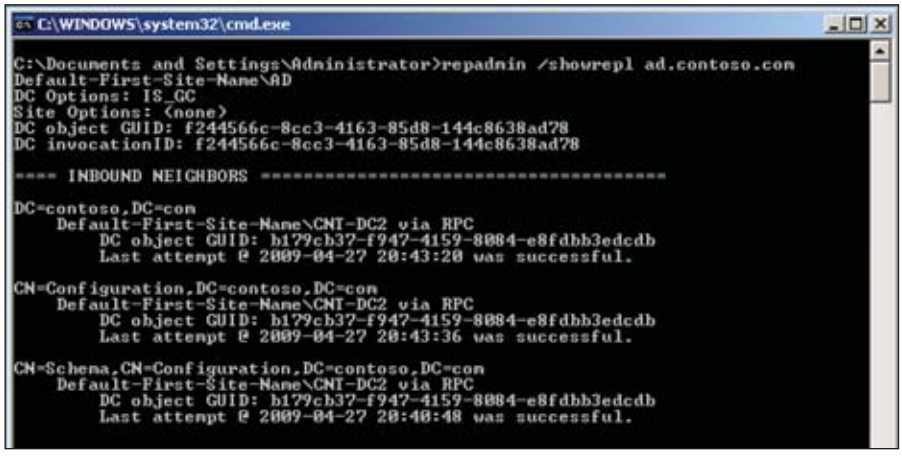


Bild 4: Repadmin zeigt für jeden Namenskontext den Status der letzten Replikation mit allen Replikationspartnern an

/showrepl, da Active Directory bei internen Verweisen in der Replikation stets diese GUID verwendet.

Standorte im Active Directory

Versäumen Sie es, die Beschreibung des Netzwerks in die AD-Konfiguration einzutragen, so hat der Verzeichnisdienst keine Chance, die optimalen Replikationsverbindungen zu erzeugen. Dabei hört sich dies aufwändiger an, als es in der Praxis ist. In kleinen Netzwerken mit nur einem einzigen LAN-Standort braucht der Netzwerkverwalter gar nichts zu tun: Ohne genauere Daten geht Active Directory davon aus, dass sich alle Server und Clients am selben Standort befinden. Hierfür reicht der vordefinierte AD-Standort mit dem unhandlichen Namen "Standardname-des-ersten-Standorts" völlig aus. Sobald es aber mehrere LAN-Standorte gibt, ist der Verantwortliche in der Pflicht, dies dem AD mitzuteilen. Der Verzeichnisdienst benötigt aber keine Details zur Topologie, sondern nur ein paar grobe Rahmenwerte.

Ein Standort im Sinne von Active Directory ist ein zusammenhängendes Netzwerk, an dem LAN-Verbindungsqualität herrscht und das aus einem oder mehreren vollständigen IP-Subnets besteht. Das folgende Beispiel nimmt die drei Standorte Hannover, Reit im Winkl und Liestal in der Schweiz an, an denen jeweils Netzwerke mit eigenen IP-Subnets arbeiten. Hannover und Reit im Winkl sind per MPLS mit 8 MBit/s verbunden, zwischen Reit im Winkl und Liestal gibt es eine VPN-Strecke mit nominellen 2 MBit/s und Hannover und Liestal sind mit einem 1-MBit-VPN verbunden. Als Backup gibt es zwischen Hannover und der Schweiz ISDN-Router mit Kanalbündelung.

Sollen an jedem der drei Standorte Domänencontroller laufen, müssten Sie für jede Lokation einen AD-Standort (Site) definieren. Netzwerkstandorte sind dann Kandidaten für AD-Standorte, wenn dort ein oder mehrere DCs postiert werden. Eine Lokation ohne DC benötigt meist keinen AD-Standort. Sie starten also das Verwaltungsprogramm "Active Directory-Standorte und -Dienste" und erweitern dort den Knoten "Standorte". Mit dem Befehl "Neu" aus dem Kontextmenü lässt sich ein neuer AD-Standort erzeugen, der einen kurzen, sprechenden Namen erhält und zunächst dem "Default IP Site Link" zugeordnet werden kann. Sind alle Standorte erzeugt, informiert man AD über die WAN-Strecken.

Standortverknüpfungen

Damit das AD nicht nur die Netzwerkstandorte kennt, sondern auch die Leitungsqualität dazwischen bewerten kann, legen Sie "Standortverknüpfungen" (Site Links) an. Diese symbolisieren die tatsächlichen WAN-Verbindungen, die sie über vier wesentliche Eigenschaften beschreiben:

- Kosten: Die Kosten sind ein symbolischer Wert, den der Knowledge Consistency Checker des Active Directory heranzieht, um die optimale Replikationsstruktur zu berechnen. Der Vorgabewert ist 100; durch höhere oder niedrigere Werte lassen sich wie bei einer Routingtabelle bevorzugte oder weniger geeignete Verbindungen kennzeichnen. Ist ein Standort von einem anderen aus über mehrere Wege erreichbar, so wird das AD denjenigen mit dem geringsten Kostenwert bevorzugen.
- Replikationsintervall: Dieser Wert steuert, wie oft das Active Directory seine Daten über diesen Link replizieren darf. Der Vorgabewert sind drei Stunden; dies lässt sich in 15-Minuten-Schritten zwischen einer Viertelstunde und einer Woche justieren.
- Zeitplan: Zusätzlich zum Replikationsintervall gibt der Zeitplan an, zu welchen Tageszeiten eine Verbindung zur Replikation zur Verfügung steht. Netzwerke mit sehr hoher Nutzlast auf der WAN-Leitung während der Geschäftszeiten können von dieser Einstellung profitieren.
- Transportprotokoll: Theoretisch erlaubt das Active Directory zwei Protokolle zur Replikation, nämlich IP (womit eine direkte RPC-Verbindung zwischen den Servern gemeint ist) und SMTP (E-Mail). In der Praxis findet sich aber keine Umgebung, die SMTP zur Replikation nutzt: Es ist technisch aufwändig, wenig zuverlässig und dieses Protokoll unterstützt nur die Replikation von Schema und Konfiguration, aber nicht die Domänenreplikation.

In unserem Beispiel könnten wir den Link zwischen Hannover und Reit im Winkl bei 100 belassen, Reit im Winkl und Liestal mit dem Wert 200 verbinden und zwischen Hannover und Liestal die Kosten auf 500 setzen. So würden die AD-Daten, die von Hannover nach Liestal müssen, intern über Reit im Winkl repliziert werden, weil der indirekte Weg "günstiger" ist. Dafür sorgt eine automatisch erzeugte "Brücke" zwischen den Links. Nachdem Sie einen neuen Link erzeugt haben, können Sie nun die Standorte zuordnen. Dazu öffnen Sie jedes Standortobjekt, das eine solche Verbindung nutzt, und weisen den Link dort zu.

Subnets im Verzeichnisdienst zuweisen

Alle IP-Subnets, die an den Lokationen genutzt werden, sollte man den AD-Standorten zuweisen. Dazu erzeugen Sie im Ast "Subnets" die zugehörigen

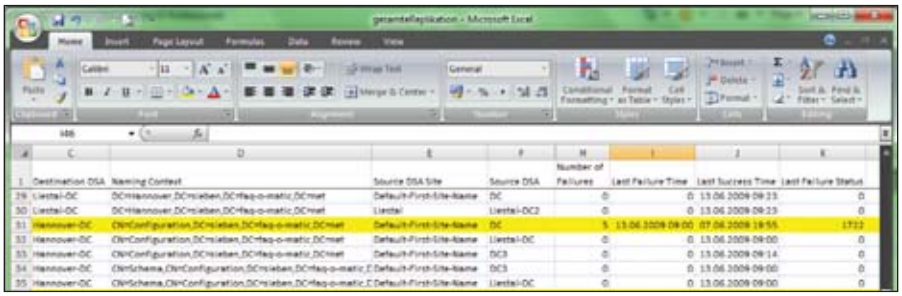


Bild 4: Als kommaseparierte Ausgabe kann die Replikationstopologie in weiteren Programmen, im Beispiel Microsoft Excel, analysiert werden

Objekte und hinterlegen dort die IP-Subnetz-Kennung. Ein Subnet gehört zu genau einem AD-Standort, umgekehrt kann ein Standort mehrere IP-Subnets haben. Unser Beispiel ordnet dem Standort Hannover die Subnets 192. 168.1.0/24, 192.168.10.0/24 und 192.168.11.0/24 zu. Reit im Winkl hat das Subnet 192.168.20.0/24 und Liestal 192.168.30.0/24. Zu welchem Standort ein AD-Subnet gehört, wird in dessen Eigenschaften ausgewählt. Gibt es eine Lokation ohne DC, so können Sie deren Subnet dem AD-Standort zuweisen, dessen DC die Clients zur Anmeldung nutzen sollen. Clients erfragen ihre Standort-Zugehörigkeit mit Hilfe ihrer IP-Adresse. Die Domänencontroller muss der Administrator hingegen bis Windows Server 2003 manuell im Programm "Standorte und Dienste" in den richtigen Standort schieben. Erst Windows Server 2008 schlägt anhand der Server-IP-Adresse selbst den passenden Standort vor. Ein kleines Skript, das die aktuelle Konfiguration der Standorte, Subnets und Server übersichtlich als HTML-Seite ausgibt, finden Sie unter [3].

Replikation zwischen Standorten

Die Replikation von Änderungen am Verzeichnis haben wir bereits ausführlich behandelt: Innerhalb eines Standortes benachrichtigen sich Domänencontroller gegenseitig über Änderungen, die an ihren Datenbankinstanzen durchgeführt wurden. Benachbarte Domänencontroller können anschließend Neuerungen seit der letzten erfolgreichen Replikation anfordern.

Über Standorte hinweg ist diese Praxis aus verschiedenen Gründen meistens nicht tragbar. Standortübergreifende Verbindungen leiden oftmals unter hoher Bandbreitenauslastung, sind eventuell nicht ständig verfügbar oder schlicht zu teuer für eine ständige Datenübertragung. Aus diesem Grund verwendet das Active Directory ein leicht modifiziertes Benachrichtigungsmodell über Standortgrenzen hinweg. Statt sofort Benachrichtungen zu versenden, hält sich Active Directory an die Konfiguration der Standortverknüpfung (Kosten, Replikationsintervall und Replikationszeitplan).

Pro Standort bestimmt der KCC mit Hilfe eines Algorithmus für jeden Namenskontext einen Domänencontroller, der innerhalb dieser Site eine besondere Rolle einnimmt: den Bridgehead-Server. Der Bridgehead-Server ist für die Replikation von Namenskontexten mit anderen Standorten verantwortlich. Replikationsbenachrichtigungen an einen Standort werden an ihn gerichtet. Umgekehrt ist es ebenso der Bridgehead-Server, der andere Standorte – genauer: den Bridgehead-Server des anderen Standortes – über Änderungen aus seiner Site benachrichtigt. Standortübergreifende Replikation findet somit nur zwischen Bridgehead-Servern statt.

Erfolgt eine Änderung an der Datenbank, versendet der Bridgehead-Server keine Änderungsnachricht an die angebundenen Standorte. Gemäß der Konfiguration in "Active Directory Standorte und Dienste" senden Server eine Änderungsanfrage an ihre Nachbarn. Während die Replikation innerhalb eines Standorts (intra-site) auf "Notify & pull" basiert, ist der Intersite-Abgleich als reiner "Pull" realisiert. Wer "Nachbarn" sind, bestimmt der Systemverwalter mit Hilfe der Kosten, die er in den Standortverbindungen angegeben hat. Das konfigurierte Intervall wird gemäß Zeitplan eingehalten. Standortverknüpfungen können Sie demnach so konfigurieren, dass an Wochenenden keine Replikation stattfindet, da dort erfahrungsgemäß wenige Änderungen an der Datenbank vorkommen. Möglich ist auch der Umkehrfall, falls die Replikation innerhalb der Arbeitszeiten die Leitung nicht belasten darf und zu verkehrsruhigeren Zeiten stattfinden muss.

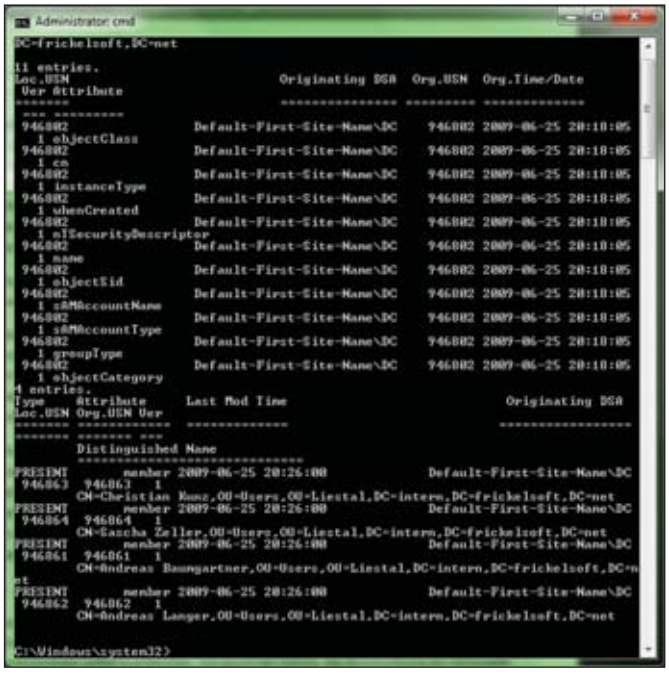


Bild 5: Mit dem Schalter "/showobjmeta" können Sie attributgenau nachvollziehen, welcher Domänencontroller zu welchem Zeitpunkt Änderungen an einem Objekt vorgenommen hat

Schneller übertragen

Zwei Spezialfälle der Replikation durchbrechen das bisher bekannte Schema und erzeugen eine beschleunigte Replikation. Der Hintergrund ist in beiden Fällen ein höheres Sicherheitsniveau, das in bestimmten Situationen nötig ist. Eine solche Situation ist das Sperren eines Kontos: Ein Angreifer hat Kennwörter ausprobiert und aufgrund der Kontenrichtlinien sperrt Active Directory nach beispielsweise fünf falschen Versuchen das Konto. Nun könnte der Angreifer seine Attacke an einem anderen DC fortsetzen, wenn die normale Replikationsverzögerung von 15 Sekunden (seit Windows Server 2003) oder sogar fünf Minuten (Windows 2000) aktiv wäre. Daher übergeht ein DC in solchen Fällen die Verzögerung und in-

formiert seine Partner sofort von der Änderung. Der Effekt ist eine beschleunigte Replikation solcher Vorkommnisse, bekannt als "Urgent Replication". Zwischen zwei Standorten greift dies allerdings nur bei aktivierter "Inter-site Change Notification".

Eine zweite Ausnahme macht das Active Directory bei Passwort-Änderungen. Es kommt vor, dass ein Benutzer, verbunden mit einem DC, sein Kennwort ändert und sich direkt danach nicht anmelden kann, weil ein anderer DC die Anmeldung bearbeitet. Um solche Situationen zu vermeiden, repliziert AD ein geändertes Kennwort sofort an den DC, der die PDC-Emulator-Rolle innehat – unabhängig von Standortgrenzen. Umgekehrt wird ein DC, der von einem Benutzer ein ungültiges Kennwort erhält, direkt beim PDC-Emulator prüfen, ob dies vielleicht das gerade geänderte neue Kennwort ist ("Immediate Replication").

Obwohl der KCC selbsttätig Bridgehead-Server für Namenskontexte auswählt, kann es Fälle geben, in denen Sie den Bridgehead-Server manuell auswählen müssen. Das ist der Fall, wenn der vom KCC ausgewählte Domänencontroller die Replikationslast nicht bewältigen kann oder für eine Wartung vom Netz genommen werden muss und ein spezieller Domänencontroller zum Einsatz kommt. Die manuelle Auswahl eines Bridgehead-Servers führen Sie mit der MMC-Konsole "Active Directory Standorte und Dienste" durch. Wählen Sie hierzu den betreffenden Standort aus dem Container "Standorte" aus. In den Eigenschaften des Domänencontroller-Objektes können Sie dann per "Hinzufügen" einen Domänencontroller als Bridgehead-Server für den Standort wählen.

Ein Hinweis ist hier angebracht: Sobald ein Bridgehead-Server für Namenskontexte in einem Standort manuell konfiguriert ist, greift der KCC nicht mehr in die Auswahl der Server ein. Sind auf Grund eines Fehlers alle Bridgehead-Server für einen NC im Standort nicht verfügbar, wählt der KCC keinen neuen Bridgehead-Server aus. Die Folge: Replikationsstillstand. Definieren Sie also die Bridgehead-Server für einzelne Standorte selbst, so müssen Sie darauf achten, dass die ausgewählten Domänencontroller stets verfügbar sind.

Bridgehead-Server manuell bestimmen

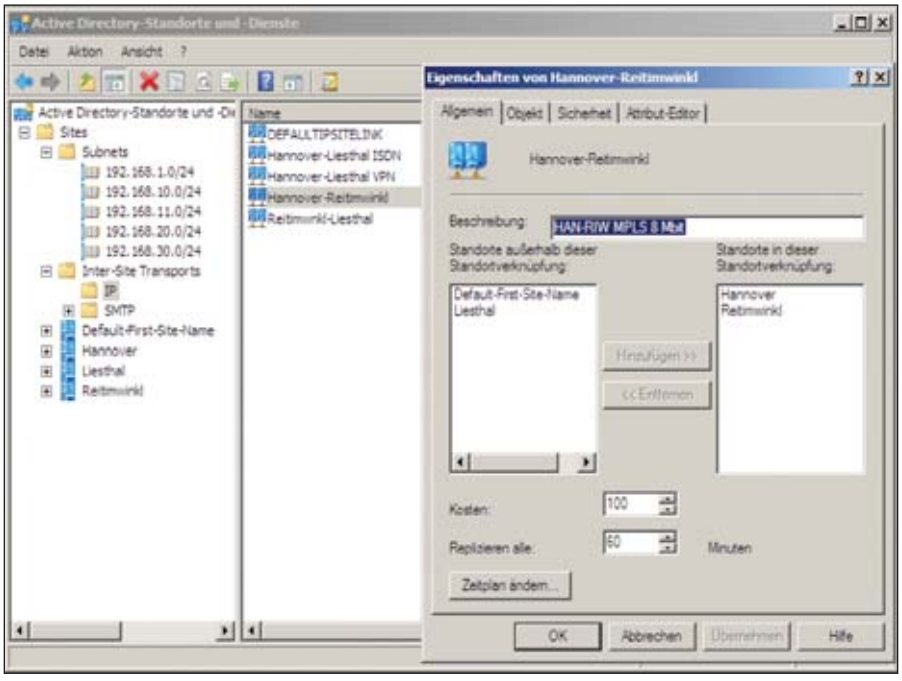


Bild 6: Die Kosten einer Verbindung geben an, wie geeignet diese für die Datenübertragung ist

Replikation von fremden Domänenpartitionen

Eine weitere, wichtige Komponente in einer Active Directory-Gesamtstruktur stellt der Globale Katalog ("Global Catalog", GC) dar. Domänencontroller können mit dieser Rolle beauftragt werden, um Benutzern und Diensten domänenübergreifende Suchen zu ermöglichen. Für diese Funktion replizieren Globale Kataloge zusätzliche Daten: neben der eigenen Domäne, Schema und Konfiguration verfügen GCs über Replikate aller Objekte sämtlicher Domänen des Forest, allerdings um einige Attribute reduziert. Der globale Katalog kann somit in allen Domänenpartitionen der Gesamtstruktur nach Objekten suchen. GCs haben nur auf ihrer eigenen Domänenpartition schreibenden Zugriff – auf alle weiteren Partitionen kann nur lesend zugegriffen werden.

Um an die Daten fremder Domänenpartitionen zu kommen, muss der GC Replikationsverbindungen zu anderen DCs erstellen. Die Verbindungen können entweder andere GCs sein, die die Partitionen der anderen Domänen bereits vollständig repliziert haben oder Domänencontroller der betreffenden Domänen. Der KCC erstellt hierfür eine eigene Replikationstopologie. Die Replikation der GC-Daten (auch als "Partial Attribute Set" bezeichnet) hält sich an die Regeln der Intra- beziehungsweise Inter-site Replikation. Gemäß der Zeitpläne und Intervalle werden Änderungen an fremden Domänenpartitionen repliziert.

Abfangen von Replikationsverzögerungen

Die Replikation hilft dabei, an allen DCs den gleichen Datenbankstand herbeizuführen und sorgt dafür, dass sämtliche Änderungen wirklich überall zur Ausführung kommen. Dies mag in überschaubaren Umgebungen nachvollziehbar sein, kann in verteilten Strukturen jedoch zu Überraschungen führen, wenn neue Daten oder Änderungen nicht umgehend am anderen Ende der Gesamtstruktur ankommen. Dieses Problem wird als "Propagation Delay" oder Replikationslatenz bezeichnet: Die Zeit, welche die Replikation dazu benötigt, um eine Änderung von A nach B zu kommunizieren.

Meist schlagen genau diese Replikationsverzögerungen dann zu, wenn eine andere Person bestimmte Änderungen

an einem Objekt sehnlichst erwartet. Befindet sich diese Person an einem anderen Standort, kann es schon einmal länger dauern, bis die neuen Daten am entfernten Standort auftauchen. Wer sich der Verzögerung bewusst ist, der kann Abhilfe schaffen: Alle Active Directory MMC-Snap-Ins erlauben es, den verbundenen Domänencontroller zu ändern. Werden Anpassungen an Objekten an einem entfernten Standort erwartet, kann sich der Administrator einfach mit einem Domänencontroller des Standortes verbinden und die Änderung direkt dort durchführen – so umgeht er die Verzögerung der Replikation. Wählen Sie dazu im geöffneten Snap-in per Rechtsklick auf den Domänenknoten den Domänencontroller aus.

Sinnvoll ist dieses Vorgehen auch bei Passwortänderungen für Benutzer entfernter Standorte. Durch das Benachrichtigen des PDC-Emulators mit Hilfe der "Immediate Replication" wird die Passwortänderung an eine zentrale Stelle geschickt, um eine schnellere Verteilung neuer Kennwörter zu erreichen. Standort-DCs, die keine direkte Verbindung zum PDC herstellen können und ein Passwort vom PDC verifizieren lassen müssen, profitieren davon allerdings nicht. In diesem Fall weist der Standort-Domänencontroller die Authentifizierung ab und nimmt ein neu vergebenes Passwort, obwohl es der Benutzer korrekt eingegeben hat, nicht an. Das direkte Ändern des Passworts auf einem DC am Standort des Benutzers umgeht dieses Problem.

Replikation von Schema-Änderungen

Das Schema, die Datenbank-Definition des Active Directory, ist für alle Domänen des Forest einheitlich. Daher baut der Verzeichnisdienst hierfür eine eigene Replikationstopologie auf, die sich in größeren Netzwerken von der Replikation der Domänendaten unterscheiden kann. Änderungen am Schema wollen gut geplant sein, denn neben der Replikationslast besteht vor allem auch ein Risiko, die Funktionalität des AD zu beschädigen.

Ein Beispiel: Ein Unternehmen könnte entscheiden, dass es für seine Mitarbeiter auch die Schuhgröße im Active Directory speichern muss. Da AD hierfür kein Datenfeld vorsieht, erweitern die Administratoren das Schema und fügen der Objektklasse "User" ein neues Attribut namens "Schuhgroesse" hinzu. Die Personalabteilung pflegt die nötigen Daten ein. Einige Zeit später entfällt der Bedarf für diese Daten. Da sich Erweiterungen des Schemas nicht löschen, sondern nur deaktivieren lassen, schalten sie das Attribut "Schuhgroesse" kurzerhand ab. Mit einem Schlag sind alle Benutzerobjekte ungültig, denn die noch vorhandenen Schuhgrößen-Werte sind in einem Attribut gespeichert, das gar nicht mehr zur Klasse "User" gehört.

Dieses Szenario ließe sich durch etwas Sorgfalt leicht vermeiden, doch es illustriert, wie heikel solche Manipulationen am Rückgrat des AD sein können. Vor eigenen Arbeiten am Schema gilt es also, genau und vorausschauend zu planen. Doch es gibt ja auch kommerzielle Produkte, die das AD-Schema erweitern, allen voran Exchange. Solche professionellen Schema-Updates sind in der Regel gut durchdacht, so dass keine Schäden durch die Anwendung zu erwarten sind. Trotzdem ist etwas Vorsicht angebracht, denn das Update könnte durch einen Serverausfall mittendrin abbrechen, und das zieht erhöhten Support-Aufwand nach sich. Ein strukturiertes Vorgehen grenzt dieses Risiko sinnvoll ein.

Zum Ersten sollten Sie jede Schema-Erweiterung in einer abgeschotteten Testumgebung prüfen, schon um den Ablauf des Erweiterungsprogramms kennenzulernen, der bei jedem Produkt anders sein kann. Für die produktive Umsetzung im zweiten Schritt empfiehlt sich ein wenig Vorbereitung. Schema-Updates laufen auf dem Domänencontroller ab, der die Rolle "Schema-Master" innehat. Welcher das ist, verrät Ihnen das Kommando *netdom query fsmo* in der Eingabeaufforderung. Sollte das Update komplett fehlschlagen, kann es notwendig sein, den Schema-Master dauerhaft aus dem Netz zu nehmen, daher sollten Sie die Rolle gegebenenfalls auf einen DC übertragen, der keine anderen wichtigen Dienste ausführt.

Melden Sie sich direkt am Schema-Master mit einem Konto an, das der Gruppe "Schema-Admins" angehört. Zwar können Sie eine Schema-Erweiterung theoretisch remote ausführen, doch könnten in diesem Fall Netzwerk-Aussetzer zum Problem werden. Kopieren Sie alle Daten, die der Vorgang benötigt, vom Installationsmedium der Applikation auf die Festplatte. So können auch DVD-Lesefehler nicht zu einem Abbruch führen. Zur Sicherheit sollten Sie nun den Schema-Master vorübergehend von der AD-Replikation ausschließen. Sollte es wider Erwarten danach zu einem kritischen Fehler beim Schema-Update kommen, so bleiben alle anderen Domänencontroller davon unberührt.

Mit folgendem Kommando in der Eingabeaufforderung richten Sie dies ein:

```
repadmin /options
  +DISABLE_OUTBOUND_REPL
```

Dadurch schaltet Active Directory alle ausgehenden Replikationen ab. Nun führen Sie die Schema-Erweiterung aus. Nach erfolgreichem Abschluss können Sie den Schema-Master wieder in die Replikation einbinden:

```
repadmin /options
  -DISABLE_OUTBOUND_REPL
```

Sollte der Ablauf tatsächlich völlig danebengegangen sein, so führen Sie den letzten Befehl nicht aus. Stattdessen trennen Sie den nun unbrauchbaren Schema-Master vom Netzwerk und lassen ihn offline. Übertragen Sie die Schema-Master-Rolle auf einen anderen Domänencontroller und entfernen Sie den abgeschalteten ehemaligen Schema-Master aus dem Active Directory. Hinweise hierzu liefert Artikel 216498 in Microsofts

Knowledge Base [4]. Aus der Praxis ist uns allerdings kein Fall bekannt, in dem dies tatsächlich nötig gewesen wäre. Nach einer Schema-Änderung ist in modernen Windows-Netzwerken nicht mit einer wesentlich stärkeren Replikation zu rechnen. Unter Windows 2000 führte jede Manipulation des Schemas noch zu einer Komplettreplikation aller Objekte – das ist seit Windows Server 2003 aber nicht mehr der Fall.

Einfaches Bestimmen der Latenzzeiten

Einzelne Änderungen an Objekten lassen sich ohne Weiteres zwischen Domänencontrollern replizieren. Bei den allermeisten Änderungen dürfte es keine Rolle spielen, wann genau alle Domänencontroller das Update in ihre Datenbank eingepflegt haben. Auf Minuten kommt es nur in seltenen Fällen an. Anders sieht das mit Schemaänderungen aus. Oder einer Massenänderung an Benutzer- und Computerattributen im Active Directory, um eine neu eingeführte Software in allen Standorten benutzen zu können. Dann ist es notwendig zu wissen, wann eine Änderung an welchem Standort vollzogen wurde. Ebenso sollte Ihnen bekannt sein, ob ein Zeitfenster, in dem das Netzwerk unbelastet ist, ausreicht, um die Änderungen zu replizieren. Hier ist eine genaue Information darüber sehr sinnvoll, wie lange das Propagieren von Änderungen an alle Domänencontroller in allen Standorten dauert.

Wie lange die Replikation benötigt, lässt sich mit etwas Mühe aus den Einstellungen im Menü "Active Directory-Standorte und -Dienste" herausfinden, indem Sie die Replikationsintervalle betrachten und die maximalen Wartezeiten summieren. Praktischer geht es allerdings mit einem Test: Objekten, die eine Änderung erfahren haben, setzt das Active Directory einen Zeitstempel auf. Dieser Zeitstempel wird im Attribut "whenChanged" auf jedem Domänencontroller gespeichert – und nicht repliziert. Der Domänencontroller setzt den Zeitstempel, sobald er von der Änderung erfahren hat und diese in seiner lokalen Datenbank vollzogen hat. Die Zeitstempel unterscheiden sich also von DC zu DC, abhängig davon, wann sie die Änderung durchgeführt haben.

Die Verzögerung der Replikation können Sie mit Hilfe des Attributs "whenChanged" messen, indem Sie ein Objekt auf einem Domänencontroller erstellen und dann einige Zeit warten, bis die Replikation das Objekt auf allen weiteren DCs erstellt hat. Dann prüfen Sie das Attribut des neuen Objekts auf den DCs– die Differenz des Zeitstempels zwischen "whenChanged" auf dem Quell-DC, auf dem das Objekt erstellt wurde, und einem DC in einer entfernten Site ist die Zeitdauer, die die Replikation benötigt hat, um die Änderung zu verteilen.

Ausprobieren lässt sich diese Messung entweder von Hand, indem Sie ein Objekt in einem beliebigen NC, selbstverständlich auch den gesamtstrukturweiten, anlegen und anschließend prüfen. Pfiffiger geht es allerdings mit einem Skript namens "ADRepCheckLatency" [5], das diese Arbeit automatisiert erledigt: Das Skript besteht aus zwei Teilskripten: Das erste Skript *ADRepCheckLatency-Inject.vbs* führt eine Änderung an einem bestimmten Objekt auf einem ausgewählten DC aus. Das zweite Skript *ADRepCheckLatency-Detect.vbs* sucht nach dieser Änderung auf einem anderen DC, den der Admin als Parameter beim Skriptaufruf angibt.

Anschließend zeigt das Skript die Zeitstempelunterschiede für die ausgewählten Domänencontroller an. Angemerkt sei an dieser Stelle, dass eine einzelne Messung keine eindeutigen Ergebnisse liefert, da das Replikationsintervall zwischen Standorten gerade günstig sein könnte oder der Zeitplan der Replikation nicht mitspielt. Nur wiederholt durchgeführte Messungen, untereinander verglichen und im Durchschnitt betrachtet, vermitteln eine Idee, wie lange eine vollständige Replikation einer Änderung dauern wird.

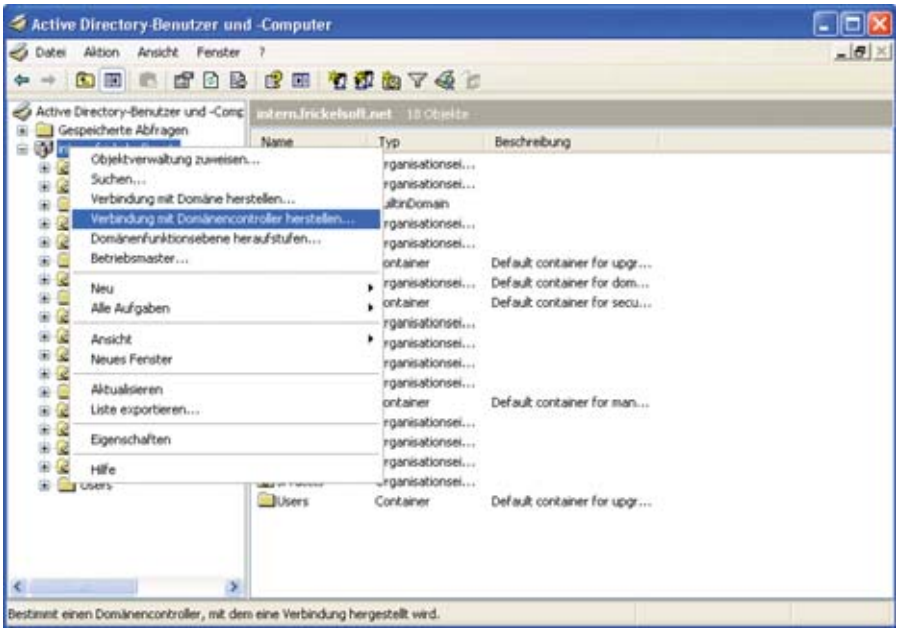


Bild 7: Die Verwaltungskonsole "Active Directory-Benutzer und -Computer" erlaubt das Verbinden mit anderen Domänencontrollern

Image vs. Backup

Replizierte Umgebungen stellen besondere Anforderungen an die Datensicherung: Da es ja mehr als nur eine Instanz der Daten gibt, muss das System besondere Vorkehrungen für bestimmte Situationen treffen. Betrachten Sie etwa die vielen Vektoren, die das Active Di-

rectory zur Kontrolle der Replikation zwischen den Servern verwendet, so erkennen Sie schnell, dass ein Eingriff an der falschen Stelle zum Scheitern des Datenabgleichs führen kann. Die Datensicherung kann ein solcher Eingriff sein, denn sie dient ja gerade dazu, einen historischen Zustand der Datenbank festzuhalten, um diesen ganz oder teilweise wiederherzustellen. Active Directory bietet dafür eine Reihe von Mechanismen, die dafür sorgen, dass das Gesamtsystem dabei nicht aus dem Tritt gerät. Eine beliebte Sicherungsmethode verträgt sich allerdings nicht mit der AD-Replikation: Images und Snapshots. Denn diese beruhen darauf, dass ein ganzes Serversystem sozusagen eingefroren und auf einen exakten Zustand zurückgesetzt wird. Dies ist für Domänencontroller definitiv ungeeignet, wie ein kleines Beispiel zeigt:

Stellen Sie sich eine Domäne vor mit zwei DCs, in der es die Objekte "User1", "User2" und "User3" gibt. Der Server DC1 hat die letzte Änderung mit der Update Sequence Number (USN) 1147 ausgeführt. Aufgrund der Replikation weiß DC2 dies und speichert für DC1 den High-Watermark-Vektor 1147. In diesem Moment – sagen wir um 14:31 Uhr – erzeugt der Administrator ein Image von DC1. Die Domäne arbeitet weiter und DC1 führt einige weitere Änderungen aus. Um 17:41 Uhr repliziert er das Objekt "User4" mit der USN 1203 an seinen Partner. Dieser speichert die Daten und den neuen High-Watermark-Vektor 1203 für DC1.

Fünf Minuten später hat DC1 einen Fehler und der Administrator spielt das Image von 14:31 Uhr wieder ein. DC1 startet normal – offenbar ist das Problem behoben. Doch der Schein trügt, denn nun fangen die Schwierigkeiten erst an. Denn um 14:31 Uhr kannte DC1 das Objekt "User4" noch gar nicht. Er kann es aber nicht von seinem Replikationspartner erhalten, denn dieser ist ja auf dem aktuellen Stand und weiß, dass DC1 das Objekt bereits kennen muss. Nun ändert sich auf DC1 ein Objekt, wofür er die USN 1148 vergibt. Beim Replikationsversuch erkennt DC2 einen Fehler: Die USN 1148 ist für DC1 gar nicht aktuell, er erwartet Nummer 1204 für die nächste Änderung. Als Folge schaltet DC1 seine Replikation ab und meldet im Eventlog die Fehler 2095 und 2103.

Diese Situation ist als "USN Rollback" bekannt. Das Active Directory erkennt solche Fehler, kann sie aber nicht beheben. Abhilfe für den Admin: Er muss das Active Directory von DC1 entfernen und ihn neu zum DC hochstufen. Allerdings könnten bereits Folgeprobleme aufgetreten sein, etwa doppelte Security-IDs, die nur schwer zu beheben sind. Diese Probleme entstehen immer wieder, wenn Admins ein Image eines Domänencontrollers wiederherstellen. Der einzige Tipp kann hier nur lauten: Setzen Sie niemals einen DC per Image (oder per Snapshot auf VM- oder SAN-Ebene) auf einen historischen Zustand zurück. Nutzen Sie zur Datensicherung das unterstützte Verfahren, also das System-State-Backup. Nur so können Sie auf die korrekte Replikation vertrauen.

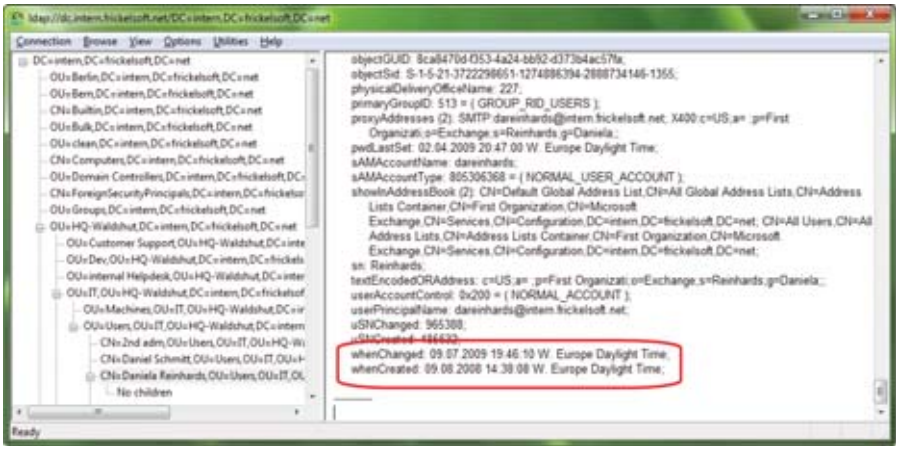


Bild 8: Das Active Directory protokolliert, wann es ein Objekt geändert hat

Problemzonen Sysvol und Netlogon

Keine Beschreibung der AD-Replikation ist vollständig, wenn sie nicht eine wichtige Komponente des Windows Server Systems bis 2008 beschreibt: FRS. Das Kürzel steht für den "File Replication Service" in Windows, der neben Freigaben des Distributed File Systems (DFS) auch die für Domänen wichtigen Verzeichnisse Sysvol und Netlogon repliziert. Mit diesen beiden veröffentlichten Verzeichnissen macht Active Directory System- und Gruppenrichtlinien verfügbar und bietet eine zentrale Ablagestelle für das Standard-Benutzerprofil für neu angelegte Benutzer. Durch die Replikation durch FRS kann Windows die Daten auf alle Domänencontroller verteilen.

FRS zeigt in seiner Funktionsweise viele Parallelen zum Active Directory. Es ist ein Multi Master-System, das allen Domänencontrollern erlaubt, schreibend auf alle Daten in den replizierten Verzeichnissen zuzugreifen. Dieser Dienst erkennt mit Hilfe eines Änderungsjournals und der Nutzung von Aktualisierungsnummern – wie Active Directory mit USNs –, welche Partner Änderungen erhalten müssen. Bei der Replikation der Daten müssen sich Administratoren nicht sorgen: FRS ist sich des Standorts bewusst und erkennt, wenn sich ein Replikationspartner in einer anderen Site befindet. Gemäß der in der Konsole "Active Directory Standorte und Dienste" hinterlegten Standortdaten hält es sich an ein konfigurierbares Replikationsintervall zwischen entfernten Standorten: eine Replikation pro Stunde.

Führen Sie sich die Ähnlichkeiten zwischen FRS und Active Directory vor Augen und vergleichen Sie die Komponenten, die für eine erfolgreiche Verteilung von Änderungen Betriebsbereitschaft melden müssen, unter anderem DNS und Kerberos, erkennen Sie schnell: Soll die Replikation von FRS erfolgreich funktionieren, müssen Sie das Verzeichnis und die Dienste pflegen.

Obwohl FRS durchgeführte Änderungen in ein Änderungsjournal schreibt und sich dabei Aktualisierungsnummern (USN) für jede geänderte Datei notiert, kann es in Einzelfällen zu Problemen kommen: Ist ein Replikationsmitglied offline und alle weiteren FRS-Mitglieder erstellen so viele Aktualisierungen, dass vorangegangene Einträge des Änderungsjournals aus Platzmangel überschrieben werden, kann der Offline-Knoten den Anschluss verlieren. Wird die zuletzt vom außer Betrieb genommenen Domänencontroller erhaltene Änderungs-USN durch eine Flut von Änderungen im Journal überschrieben, gehen zuvor notierte Aktualisierungen verloren. Dieses Verhalten heißt auch "Journal Wrap".

Um den verlorenen Bruder zurück in die Gemeinschaft zu holen, müssen Sie die FRS-Synchronisation zwischen den Domänencontrollern wiederherstellen. Sie wählen hierzu einen geeigneten Domänencontroller aus, der alle aktuellen Anpassungen repliziert hat und konfigurieren ihn als Replikationsquelle. Den problematischen Domänencontroller konfigurieren Sie als Replikationsziel. Er soll sich alle Änderungen vom Quell-DC holen. Die Neusynchronisation beginnt mit dem Stoppen des FRS-Dienstes auf Quell- und Ziel-DC. Anschließend muss der Registry-Schlüssel "BurFlags" in "HKLM \ SYSTEM \ CurrentControlSet \ services \ NtFrs \ Parameters \ Cumulative Replica Sets \{GUI}" angepasst werden. Für den Quell-DC wählen Sie "D4" (hexadezimal), um ihn als "authoritative" zu markieren.

Den zweiten DC, der den Datenbestand des Quell-DCs übernehmen soll, versehen Sie mit dem Wert "D2" (hexadezimal). Gibt es mehrere aus dem Tritt gekommene DCs, konfigurieren Sie alle weiteren DCs ebenfalls mit "D2", um auch diese zu zwingen, den Datenbestand vom Quell-DC zu laden. Abschließend starten Sie den FRS-Dienst neu. Nach dem Neustart setzen Sie den Schlüssel "BurFlags" auf seinen Vorgabewert "0" zurück. Ist die Neusynchronisation auf dem Ziel-DC abgeschlossen, listet die Ereignisanzeige das Event 13516. Das Verfahren ist in einem weiteren Knowledgebase Artikel [6] ausführlich beschrieben.

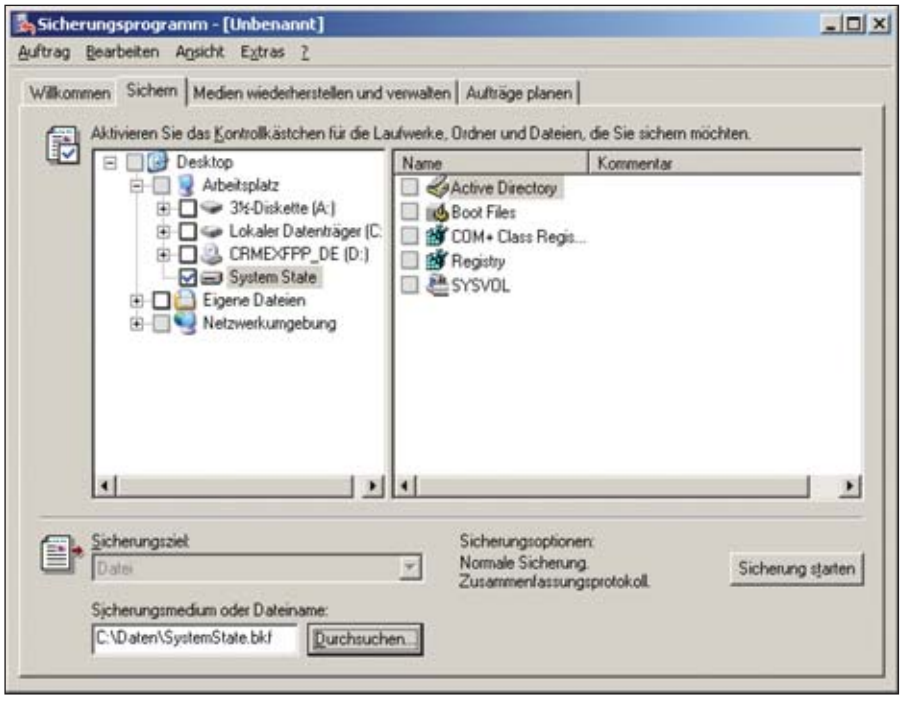


Bild 9: Die Datensicherung des AD sollte nur über geeignete Werkzeuge geschehen, etwa dem eingebauten Backup

Fazit

Das Active Directory ist ein leistungsfähiger Verzeichnisdienst für Windows-Netzwerke, der ausgefeilte Methoden enthält, um Veränderungen der Umgebung nachzuvollziehen oder Probleme selbst zu beheben. In den meisten kleineren Umgebungen verrichtet das Active Directory klaglos seinen Dienst. Nimmt der Admin aber Änderungen an der Replikationskonfiguration vor oder treten Fehler auf, für die das Active Directory keine Mechanismen enthält, ist es wichtig, die Interna zu verstehen. Dieser Workshop hat Ihnen einige der wichtigsten Hintergründe vorgestellt. *(ln)*

Von Florian Frommherz und Nils Kaczenski

[1] **Verwalten von Anwendungsverzeichnispartitionen**
http://technet.microsoft.com/de-de/library/cc755918.aspx

[2] **EventComb – Windows Server 2003 Resource Kit Tools**
www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&d

[3] **Tool "Borg"**
www.faq-o-matic.net/?s=borg

[4] **Entfernen von Daten aus dem Active Directory nach fehlgeschlagener Domänencontroller-Herabstufung**
http://support.microsoft.com/kb/216498/de/

[5] **Skript zur Messung von Replikations-Latenzzeiten**
http://www.faq-o-matic.net/?s=ADRepCheckLatency

[6] **Beheben von Journalumbruch-Fehlern auf Sysvol- und DFS-Replikatsätzen**
http://support.microsoft.com/kb/292438/de/

Links

Replikation und Firewalls

Durchgangsschleusen fürs Active Directory

Das Active Directory wird immer häufiger über Netzwerke und damit auch Firewalls hinweg betrieben – sei es für VPNs und Remote-Einwahl, in der DMZ, landesübergreifend oder einfach um die Netzwerksicherheit besser steuern zu können. Was Sie hierbei berücksichtigen müssen, zeigt dieser Beitrag.

Die Mitglieder einer Windows-Domäne müssen mit ihren Infrastrukturdiensten wie DNS und Active Directory (AD) über GPOs kommunizieren. Auch die Domänencontroller (DC) müssen miteinander kommunizieren können, um etwa die Inhalte des AD sowie der Gruppenrichtlinien zu synchronisieren. Je nach Konfiguration wenden sich DCs für die Namensauflösung oder ihren eigenen Log-on zudem an benachbarte DCs. Damit die Kommunikation reglementiert werden kann und Firewalls so weit wie möglich geschlossen werden können, ist es notwendig, dass die Active Directory-Topologie auf diese Anforderungen abgestimmt ist. Zum Beispiel bringt es wenig, wenn Domänenmitglieder in der DMZ stehen, aber zunächst versuchen, sich an einem Domänencontroller jenseits der Firewall anzumelden. Oder wenn ein Domänencontroller hinter der Firewall die Replikation mit beliebigen DCs auf der anderen Seite der Firewall starten möchte. Als Ergebnis werden dann häufig entweder alle DCs in der Firewall freigeschaltet oder einer der DCs veraltet und keiner bemerkt dies. Irgendwann muss er dann aus dem Netzwerk entfernt werden, damit es keine "lingering Objects" gibt – also Datenleichen im AD.

Standorte und Replikation

Das Active Directory benutzt Standorte, um die Kommunikation zu regeln – sowohl für Clients, die ihre zugehörigen DCs suchen, wie auch DCs, die miteinander replizieren wollen. Innerhalb eines Standortes, der auf den IP-Adressen basiert, bilden die DCs einer Domäne immer einen Replikationsring mit Abkürzungen dazwischen, falls der Ring zu groß wird. Standortübergreifend werden im AD also Standortverbindungen definiert, die eine physische oder logische Verbindung reflektieren sollen. Häufig kommt eine sternförmige Struktur zum Einsatz, so dass alle Außenstellen zunächst in die Zentrale replizieren. Damit ist jede Änderung innerhalb eines Replikationsintervalls in der Zentrale, und innerhalb eines weiteren Replikationsintervalls an allen dezentralen Standorten vorhanden.

Doch die Standortverbindungen dienen dem AD letztlich nur als Information darüber, welcher Standort mit welchem anderen Standort replizieren soll. Sie verknüpfen nämlich nur Standorte, repliziert wird jedoch von DC zu DC. Daher gibt es im AD zwei interne Prozesse, den "Intersite Topology Generator" und den "Knowledge Consistency Checker", die miteinander die Replikationsinfrastruktur bestimmen. Diese erstellen, abhängig von den Standorten und den Standortverbindungen, die eigentlichen Replikationsverbindungen. Eine Replikationsverbindung hat immer nur eine Richtung. Daher spricht man auch von eingehenden und ausgehenden Replikationsverbindungen.

Während die Replikationsverbindungen innerhalb eines Standortes einen Kreis bilden, werden standortübergreifend nor-

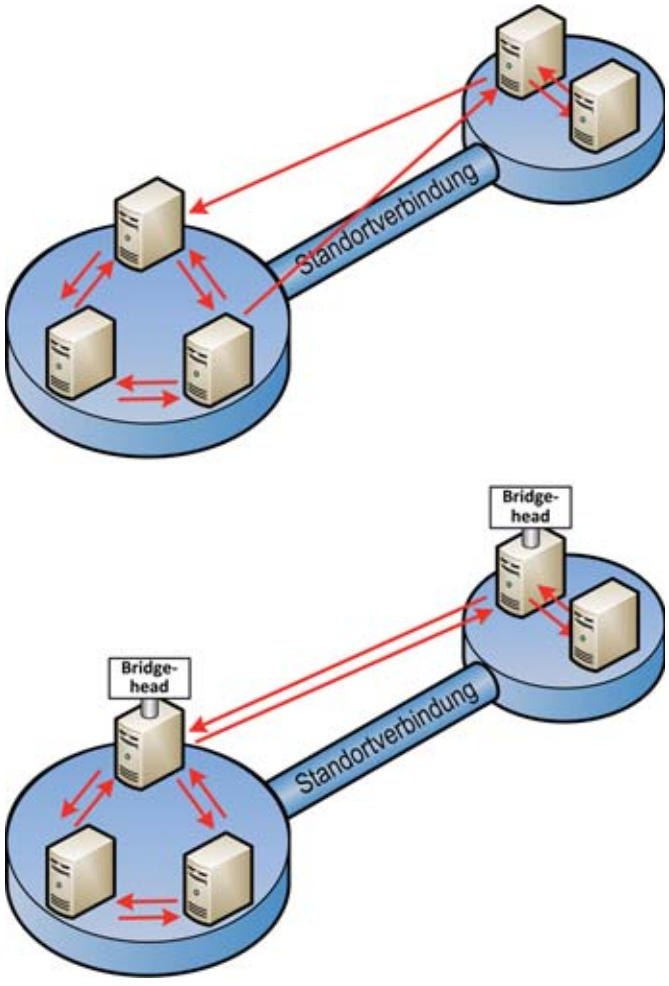


Bild 1: Die Replikationsverbindungen richten sich nach der Standortstruktur im AD. Werden Bridgeheadserver verwendet, kümmern sich diese um die standortübergreifende Replikation.

malerweise nur zwei Replikationsverbindungen erstellt: eine eingehende und eine ausgehende. Dabei ist es jedoch nicht notwendig, dass beide zwischen denselben Servern ablaufen. Je nachdem, wie die Active Directory-Konfiguration aussieht, werden die Replikationsverbindungen zwischen beliebigen DCs der jeweiligen Standorte erstellt und können sich auch ändern. Auch müssen Sie beachten, dass die Replikationstopologie davon abhängt, welche Namenskontexte die jeweiligen Server führen. Sind mehrere Domänen im Spiel und ist nicht jeder Domänencontroller Globaler Katalogserver oder halten manche DCs keine oder unterschiedliche AD-integrierte DNS-Zonen, muss dies in der Replikationstopologie berücksichtigt werden.

Soll die Replikation zwischen Standorten über eine Firewall funktionieren, so müssen alle DCs auf beiden Seiten über die benötigten Ports kommunizieren können – mehr dazu später. Möchten Sie einschränken, dass alle DCs eines Standortes übergreifend kommunizieren, definieren Sie bestimmte DCs als Bridgeheadserver. Diese übernehmen dann die standortübergreifende Kommunikation und die Firewall kann restriktiver eingerichtet werden. Erwähnenswert ist in die- sem Zusammenhang, dass RODCs nur eingehend, aber nicht ausgehend replizieren.

Sehen wir uns das doch einmal in der Praxis an: Öffnen Sie die "Active Directory-Standorte und -Dienste". Dort navigieren Sie zu dem Standort, dann unterhalb Servers zu dem Server, dessen Replikationsverbindungen Sie sehen möchten. Gehen Sie im Navigationsbaum auf das NTDS Settings-Objekt unterhalb des Servers. Hier sehen Sie die eingehenden Replikationsverbindungen des Servers. Wichtig ist hier, dass in den meisten Fällen auf dem Verbindungsobject "<automatisch generiert>" steht. Ist dies nicht der Fall und Sie sehen zum Beispiel eine GUID, wurde das Objekt bereits manuell verändert, oft versehentlich.

Dies kann passieren, wenn Sie die Eigenschaften öffnen und dort eine Änderung, zum Beispiel im Feld "Beschreibung" durchführen, diese dann wieder zurücknehmen, aber den Dialog mit "OK" anstatt mit "Abbrechen" beenden. Dieses wird dann auch nicht mehr bei Änderungen in der Replikationsinfrastruktur automatisch angepasst, was zu Fehlfunktionen führen kann. Sollte das bei Ihnen der Fall sein, können Sie das Objekt wieder auf "automatisch generiert" setzen. Öffnen Sie hierfür das Verbindungsobjekt, gehen Sie auf den Attribut-Editor, suchen Sie das Attribut "Options". Dieses hat einen geradezahligen Wert, ändern Sie es einfach, indem Sie 1 dazuzählen in einen ungeraden Wert. Wenn Sie die Anzeige von Standorten und Diensten aktualisieren, ist das Objekt jetzt automatisch generiert.

Möchten Sie ein Replikationsdiagramm erstellen, fertigen Sie sich am besten ei-

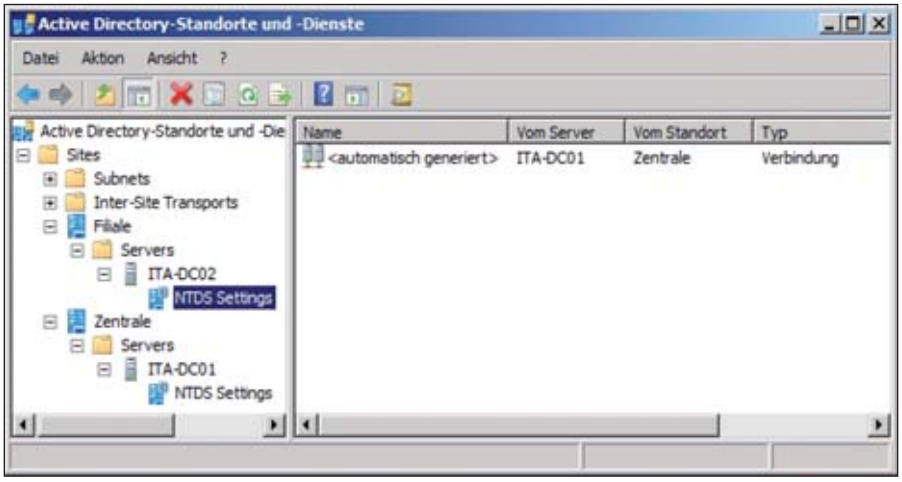


Bild 2: In "Active Directory-Standorte und -Dienste" werden die "eingehenden Replikationspartner" angezeigt

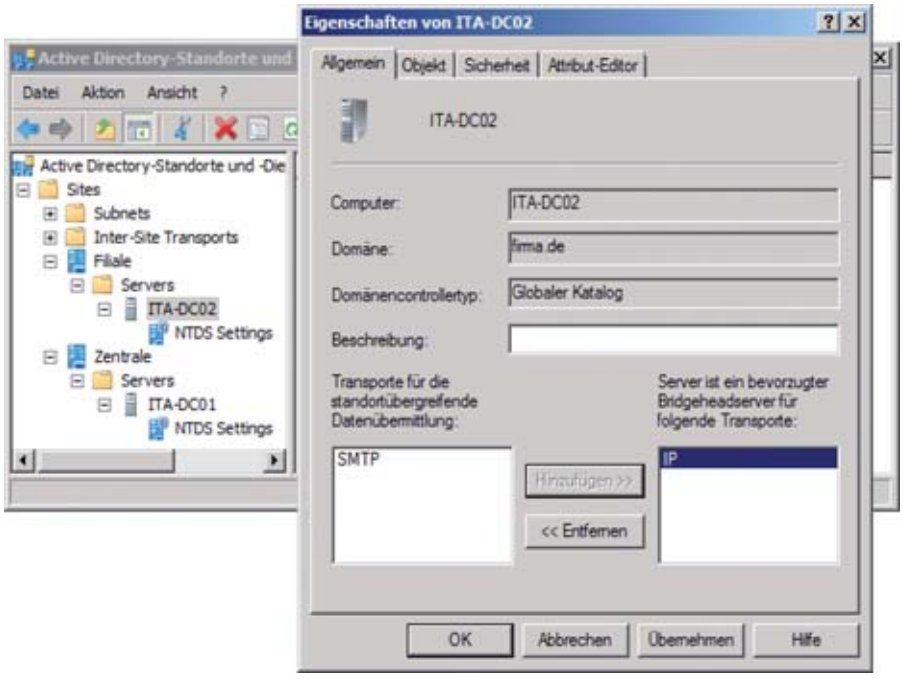


Bild 3: Welche Domänencontroller Bridgeheadserver für einen Standort sind, richten Sie auf dem Serverobjekt in "Active Directory-Standorte und -Dienste" ein

ne Skizze der DCs an und gehen Sie dann durch die Server in "Active Directory-Standorte und -Dienste". Hier notieren Sie sich die eingehenden Verbindungen. Grundsätzlich gilt: Möchten Sie über eine Firewall replizieren, sollten Sie die Standorte und Standortverbindungen korrekt eingerichtet haben. Dann sollten Sie sich noch überlegen, ob Sie Bridgeheadserver verwenden. Sobald mehrere DCs in einem Standort arbeiten, lässt sich ansonsten nicht definieren, wer mit wem repliziert. Das statische Einrichten von Verbindungsobjekten sollten Sie dabei unterlassen, damit im Fehlerfall die Automatismen funktionieren.

Freischalten der nötigen Ports

Für die Kommunikation selbst gibt es zwei Möglichkeiten: Die Kommunikation wird über IPSec verschlüsselt oder die Firewall erlaubt die standardmäßige Windows-Kommunikation. Welche Ports werden also für die Kommunikation von Windows Systemen und für die Replikation von Domänencontrollern benötigt? Die Kommunikation in der Windows-Infrastruktur ist relativ komplex, da zahlreiche Dienste zusammenarbeiten. Folgende Protokolle sind hier relevant:

- ICMP: Wird sowohl von Clients wie auch Servern benötigt, unter anderem um festzustellen, wie schnell die Verbindung zwischen zwei Systemen ist. Wenn ICMP geblockt wäre, würden zum Beispiel die Gruppenrichtlinien annehmen, dass sie es mit einer langsamen Verbindung zu tun haben und würden je nach Konfiguration nur teilweise angewendet.
- RPC: Wird auf alle Fälle benötigt und auf Grund der Komplexität im nächsten Abschnitt behandelt.
- LDAP für den Domänenkontext: Ist sowohl für die "normale" Kommunikation per TCP wie auch für den LDAP-Ping per UDP nötig.
- LDAP via SSL: Heutzutage sollten Zertifikate auf Domänencontrollern liegen, um LDAP über SSL verschlüsselt zu erlauben.
- Globaler Katalog: Wird für den Client-Logon sowie die DC-zu-DC-Kommunikation benötigt.
- Globaler Katalog über SSL
- MB: Wird für die Dateifreigabe von Sysvol (Gruppenrichtlinien) benötigt.
- Kerberos: Notwendig für die Authentifizierung.
- DNS: alle Domänenmitglieder müssen ihre DNS-Server errichen. Domänencontroller, die DNS-Server sind, müssen andere DNS-Server erreichen, wenn diese als DNS-Server eingetragen sind, wenn sekundäre Zonentransfers durchgeführt werden sowie wenn die anderen Server in Weiterleitungen oder Delegationen eingetragen sind. Seit Windows Server 2003 muss bei DNS nicht nur UDP, sondern auch TCP freigeschaltet werden, da größere DNS-Abfragen oder Zonentransfers per TCP kommuniziert werden.
- NetBios: Wird von Windows seit Jahr und Tag benötigt, sowohl Name Service, Datagram wie auch der Session Service.
- NTP: Auch der Windows-Zeitdienst verwendet je nach Konfiguration das Network Time Protocol.
- Active Directory Web Services: Wird bei Windows Server 2008 R2 zusätzlich benötigt (oder wenn auf einem älteren DC der AD Management Gateway installiert ist), wenn die PowerShell oder das Administrative Center über die Firewall hinweg eingesetzt werden soll.

Bei einigen dieser Protokolle lohnt es sich, genau zu analysieren, welche Sie für das eigene Szenario benötigen. Zum Beispiel ist SMB nur für das Anwenden der Gruppenrichtlinien nötig – die Replikation zwischen den DCs erfolgt per RPC. Wenn Sie über eine Firewall replizieren, können Sie also unter Umständen auf SMB verzichten, solange die Domänenmitglieder den DC im jeweiligen Standort verwenden. Gleiches gilt für DNS. Werden alle DNS-Dienste aus dem gleichen Standort verwendet und die Zonen in das AD integriert, kann es ausreichen, die DNS-Protokolle nicht über die Firewall freizugeben. Die Replikation erfolgt innerhalb des Active Directory ebenfalls per RPC. LDAP und GC ohne SSL werden nur benötigt, wenn keine Zertifikate installiert sind. In diesem Fall werden die SSL-Ports nicht benötigt. Wenn

aber alle Applikationen sicheres LDAP sprechen können, erhöhen Sie die Sicherheit, indem Sie diese Protokolle blockieren. Daher gilt es immer, das individuelle Szenario zu betrachten, zu testen und dann zu implementieren.

RPC – die große Unbekannte

In der Windows-Welt arbeiten einige Dienste über das Remote Procedure Protocol (RPC). Hierbei gibt es einen statischen Port, den RPC Endpoint Mapper, der immer freigeschaltet sein muss. Möchte ein Dienst über RPC kommunizieren, fragt der Client den Server auf dem RPC Endpoint Mapper an, ob er einen bestimmten Dienst zur Verfügung stellt. Hierfür übermittelt er eine GUID. Stellt der Server den Dienst zur Verfügung, konfiguriert er ihn auf einem dynamischen, zufällig ausgewählten Port, und teilt dem Client diesen Port mit.

Diese dynamischen Ports sind bis Windows Vista und Server 2008 alle Ports von 1.024 bis 65.535, seit Vista und 2008 die Ports ab 49.152 bis 65.535. Für die Kommunikation von Domänenmitgliedern und die Kommunikation von Domänencontrollern unter sich ist ebenfalls RPC notwendig – sei es der Logon-Dienst, die AD-Replikation oder Dateireplikation über NTFRS (bis Windows Server 2008) oder DFS-R (ab Windows Server 2008). Damit müssen in der Firewall sowohl der RPC Endpoint Mapper auf 135 TCP und UDP geöffnet werden, wie auch alle Ports ab 1.024 beziehungsweise 49.152 für TCP.

Da dies nicht gewünscht ist, gibt es zusätzlich die Möglichkeit, einzelne Dienste so zu konfigurieren, dass sie einen statischen RPC-Port verwenden. Die Prozedur ist dann die gleiche, der Client fragt auf dem Endpoint-Mapper nach einem Dienst, dieser antwortet aber dann immer mit dem gleichen Port für den jeweiligen Dienst. Für Domänencontroller sind drei Dienste relevant:

- Domänencontroller-Dienste
- File Replication Services (FRS), die für die Replikation von Gruppenrichtlinien bis Windows Server 2008 standardmäßig verwendet werden.
- Distributed File System Replication (DFS-R), das für die Replikation der Gruppenrichtlinien ab Windows Server 2008 verwendet werden kann. Bei DFS-R sollten Sie in migrierten Umgebungen zunächst überprüfen, ob die Sysvol-Replikation tatsächlich hierüber läuft, da dies explizit von FRS migriert werden muss. Die Ereignisanzeige gibt hierüber Aufschluss.

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
ICMP	WAN_DC	*	LAN_DC	*	*		ICMP between DCs
TCP/UDP	WAN_DC	*	LAN_DC	135	*		RPC Endpoint Mapper
TCP	WAN_DC	*	LAN_DC	55555	*		RPC Static for Directory Services
TCP	WAN_DC	*	LAN_DC	55556	*		RPC Static for FRS
TCP	WAN_DC	*	LAN_DC	55557	*		RPC Static for DFS-R
TCP/UDP	WAN_DC	*	LAN_DC	389 (LDAP)	*		LDAP and LDAP-Ping
TCP	WAN_DC	*	LAN_DC	636	*		LDAP via SSL
TCP	WAN_DC	*	LAN_DC	3268 - 3269	*		GC and GC via SSL
TCP/UDP	WAN_DC	*	LAN_DC	445 (MS DS)	*		SMB
TCP/UDP	WAN_DC	*	LAN_DC	88	*		Kerberos
TCP/UDP	WAN_DC	*	LAN_DC	53 (DNS)	*		DNS
TCP/UDP	WAN_DC	*	LAN_DC	137 (NetBIOS -NS)	*		NetBIOS Name Service
UDP	WAN_DC	*	LAN_DC	138 (NetBIOS -DGM)	*		NetBIOS Datagram
TCP	WAN_DC	*	LAN_DC	139 (NetBIOS -SSN)	*		NetBIOS Session Service
UDP	WAN_DC	*	LAN_DC	123 (NTP)	*		NTP
TCP	WAN_DC	*	LAN_DC	9389	*		Active Directory WebService

Bild 4: Für eine Testumgebung der Kommunikation über eine Firewall kann zum Beispiel pfSense verwendet werden

Möchten Sie die Domänencontroller-Dienste auf einen statischen Port setzen, müssen Sie den folgenden Registrierungsschlüssel erstellen: "HKLM \ System \ CurrentControlSet \ Services \ NTDS \ Parameters \TCP/IP Port ={Portnummer}". Um die Datenreplikation (NTFRS) auf einen statischen RPC-Port zu setzen, erstellen Sie dagegen den Registry-Key "HKLM \ System \ CurrentControlSet \ Services \ NTDS \ Parameters \ RPC TCP/IP Port Assignment={Portnummer}". Soll dagegen der DFS-R-Dienst auf einen statischen RPC-Port gesetzt werden, geht dies über den Befehl

```
DFSRDiag StaticRPC /Port:
  {Portnummer}
```

Diese Begrenzung des RPC-Verkehrs müssen Sie auf jedem Domänencontroller durchführen, danach ist ein Neustart erforderlich. Dann müssen nur diese Ports in der Firewall freigeschaltet werden, anstelle des dynamischen Bereichs bis 65.535.

Nutzen Sie keinen Bridgehead-Server, ist es sehr wichtig, dass Sie diese Ports

```
Administrator: Eingabeaufforderung

C:\Users\Administrator>repadmin /bind ita-dc02
DsBindWithCred mit ita-dc02 ist fehlgeschlagen mit Status 1722 (0x6ba):
    Der RPC-Server ist nicht verfügbar.


C:\Users\Administrator>repadmin /bind ita-dc02
Bindung an ita-dc02 war erfolgreich.
NTDSAPI V1 BindState, erweiterte Mitglieder werden gedruckt.
    bindAddr: ita-dc02
Unterstützte Erweiterungen (cb=48):
    BASE                          : Ja
    ASYNCREPL                     : Ja
    REMOVEAPI                     : Ja
    MOVEREQ_V2                    : Ja
    GETCHG_COMPRESS               : Ja
    DCINFO_V1                     : Ja
    RESTORE_USN_OPTIMIZATION      : Ja
    KCC_EXECUTE                   : Ja
    ADDENTRY_V2                   : Ja
    LINKED_VALUE_REPLICATION      : Ja
    DCINFO_V2                     : Ja
    INSTANCE_TYPE_NOT_REQ_ON_MOD  : Ja
    CRYPTO_BIND                   : Ja
    GET_REPL_INFO                 : Ja
    STRONG_ENCRYPTION             : Ja
    DCINFO_VFFFFFFFF              : Ja
    TRANSITIVE_MEMBERSHIP         : Ja
    ADD_SID_HISTORY               : Ja
    POST_BETA3                    : Ja
    GET_MEMBERSHIPS2              : Ja
    GETCHGREQ_V6 (WINDOWS XP PREVIEW): Ja
    NONDOMAIN_NCS                 : Ja
    GETCHGREQ_V8 (WINDOWS XP BETA 1) : Ja
    GETCHGREPLY_V5 (WINDOWS XP BETA 2): Ja
    GETCHGREPLY_V6 (WINDOWS XP BETA 2): Ja
    ADDENTRYREPLY_V3 (WINDOWS XP BETA 3): Ja
    GETCHGREPLY_V7 (WINDOWS XP BETA 3) : Ja
    VERIFY_OBJECT (WINDOWS XP BETA 3): Ja
    XPRESS_COMPRESSION            : Ja
    DRS_EXT_ADAM                  : Nein
    GETCHGREQ_V10                 : Ja
    RECYCLE BIN FEATURE           : Nein
Standort-GUID: 95127f15-02bf-4f69-b2ec-45c6dfbd20be
Replikationsepoche: 0
Gesamtstruktur-GUID: 70c88749-a953-44ab-9a87-451dd44fb7be
Die Sicherungsinformationen auf der Bindung sind wie folgt:
    Angeforderter SPN:          LDAP/ita-dc02
    Authentifizierungsdienst:   9
    Authentifizierungsebene:    6
    Autorisierter Dienst:       0

C:\Users\Administrator>
```

Bild 5: Mit *repadmin /bind {servername}* überprüfen Sie, ob der Domänencontroller via RPC antwortet. Der erste Befehl zeigt das Ergebnis, wenn die Firewall den dynamischen RPC-Port nicht zulässt, beim zweiten ist die Kommunikation erlaubt.

bei einem neuen Domänencontroller konfigurieren, damit die Replikation auch weiterhin funktioniert, wenn die Replikationsverbindungen dynamisch geändert werden. Möchten Sie zumindest RPC auf die Domänendienste verifizieren, können Sie hierfür das Kommando *repadmin /bind* verwenden. Dieses Kommando erstellt eine Verbindung über RPC mit dem Domänencontroller und verrät, welche Dienste dieser zur Verfügung stellt. Erhalten Sie eine Antwort, wissen Sie, dass die Kommunikation mit dem DC über RPC funktioniert.

Häufig Missverstanden ist dagegen der "RPC-Ping" – dieser testet nur, ob der Endpoint-Mapper zur Verfügung steht, nicht jedoch die dynamische Portzuordnung, die in unseren Fall relevanter ist. Da auch andere Windows-Dienste RPC verwenden und es auch keine belegbaren Aussagen gibt, welche Auswirkungen es haben kann, wenn Sie RPC auf einige Ports einschränken, können Sie den relevanten Verkehr durch IPSec verschlüsseln und damit über wenige Ports tunneln.

Einrichten eines IPSec-Tunnels

Die sicherste Methode, um über eine Firewall hinweg zu kommunizieren ist es, den Verkehr zwischen den Domänencontrollern per IPSec zu verschlüsseln. Dann kann die meiste Kommunikation durch den IPSec-Tunnel erfolgen und es müssen nur wenige Ports in der Firewall geöffnet werden. IPSec kennt insgesamt drei Methoden um einen sicheren Schlüssel auszutauschen:

- Über ein "Shared Secret" wird bei allen Kommunikationspartnern ein statischer Schlüssel eingetragen.
- Über Kerberos findet eine gegenseitig verlaufende Authentifizierung statt und ein Schlüssel für die Verschlüsselung wird ausgehandelt.
- Mittels Zertifikaten wird die IPSec-Verschlüsselung zertifikatsbasiert.

Während das Shared Secret die unsicherste Methode des Schlüsselaustauschs darstellt, hat Kerberos bei der Kommunikation über Firewalls den Nachteil, dass die Kerberos-Authentifizerung nicht über IPSec getunnelt werden kann. Da Kerberos aber an sich verschlüsselt ist, stellt das bis auf wenige zusätzlich offene Firewall-Ports kein Sicherheitsrisiko dar. Am besten ist es, wenn die Kommunikation mittels Zertifikaten verschlüsselbar ist. Allerdings benötigen Sie hierfür eine Zertifikatsautorität, die es auch verantwortungsvoll zu betreiben gilt.

Eine IPSec-Richtlinie für die Kommunikation zweier DCs über eine Firewall ist schnell eingerichtet. Auf jedem DC müssen Sie über "Start / Verwaltung" die Verwaltungskonsole "Lokale Sicherheitsrichtlinie" aufrufen. Dann navigieren Sie zum Knoten "IP-Sicherheitsrichtlinie auf Lokaler Computer". Mit der rechten Maustaste wählen Sie "IP-Filterlisten und Filteraktionen verwalten". Jetzt erstellen Sie eine neue Filterliste, zum Beispiel mit dem Namen "DC über Firewall". Im sich öffnenden Assistenten legen Sie einen "gespiegelten" Filter zwischen Ihrer eigenen IP-Adresse und der des DCs auf der anderen Seite der Firewall für einen beliebigen Protkolltypen an. Dann – wieder in dem Fenster "IP-Filterlisten und Filteraktionen verwalten" – erstellen Sie eine Filteraktion. Diese heißt zum Beispiel "DC Replikation", hat die Option "Sicherheit aushandeln", lässt keine unsichere Kommunikation zu und erfordert "Sicherheit und Integrität". Jetzt beenden Sie alle Dialoge und kehren zurück zur Verwaltungskonsole "Lokale Sicherheitsrichtlinie".

Als Nächstes erstellen Sie wieder über die rechte Maustaste eine IP-Sicherheitsrichtlinie. Dieser können Sie den Namen "DC über Firewall" geben. Gehen Sie hierfür den Assistenten mit den Standardwerten durch und setzen Sie am Ende das Häckchen "Eigenschaften bearbeiten". Im Dialogfenster "Eigenschaften von DC über Firewall" wird jetzt noch eine neue Regel hinzugefügt. Diese legt keinen Tunnel fest, bezieht sich auf "LAN"-Verbindungen, und verwendet die zuvor erstellte Filterliste (muss im Feld neben dem Namen aktiviert werden) und Filteraktion.

Nun folgt das Auswahlfeld, in dem Sie die Authentifizierungsmethode bestimmen. An dieser Stelle können Sie "Zertifikat" wählen, wenn Ihnen eines vorliegt, "Kerberos" (wenn das Protokoll durch die Firewall erlaubt ist) oder eine beliebige Zeichenfolge, die auf beiden Seiten identisch sein muss (Shared Secret). Empfohlen ist Kerberos oder Zertifikat. Danach können wieder alle Dialoge geschlossen werden, und die neue Richtlinie muss noch in der Verwaltungskonsole mit Rechtsklick zugewiesen werden.

Haben Sie dies auf allen relevanten DCs durchgeführt und die Firewall noch richtig eingerichtet, sollte die Kommunikation funktionieren. Für die Kommunikation per IPSec sind lediglich die folgenden Protokolle notwendig:

- DNS: Nötig, um die Server auf der anderen Seite zu finden. Wenn allerdings lokale DNS-Dienste verwendet werden, können Sie möglicherweise darauf verzichten.
- Kerberos: Dieses Protokoll kann nicht getunnelt werden, wenn die Kerberos-Authentifizierung für IPSec verwendet wird.
- Internet Key Exchange
- IPSec ESP
- IPSec AH

Möchten Sie die zertifikatsbasierte Sicherheit verwenden, können Sie Kerberos auch so konfigurieren, dass es mit in IPSec getunnelt wird. Hierfür erstellen Sie lediglich den folgenden Registrierungsschlüssel: "HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt" vom Typ REG_DWORD mit dem Wert "1". Auch dies muss auf allen relevanten DCs durchgeführt werden. Die Nutzung von IPSec hat den Vorteil, dass die Administration völlig transparent verläuft – alle benötigten Dienste und Protokolle werden durch IPSec verschlüsselt und darüber getunnelt. Häufig ist es jedoch so, dass die Firewall-Administratoren lieber den Netzwerkverkehr kennen, also die benötigten Ports aufmachen, als einen IPSec-Tunnel zu erlauben, in den nicht eingesehen werden kann. IPSec wird daher in solchen Szenarien selten verwendet.

Weitere Anforderungen

Je nach Szenario werden hinter der Firewall noch weitere Dienste benötigt. Verwendet das Unternehmen zum Beispiel die WINS-Namensauflösung für Kurznamen, muss dieser Port ebenfalls freigeschaltet werden (1.512 TCP und UDP). Wenn WINS-Server auf beiden Seiten der Firewall replizieren, muss die WINS-Replikation über Port 42 TCP und UDP freigeschaltet werden. Möchten Sie die Server per Remote Desktop verwalten, kommt noch den Port 3.389 TCP hinzu.

Ebenfalls vorstellbar wäre, den Servermanager oder die "normalen" Administrationskonsolen zu verwenden, diese freizuschalten bedeutet aber etwas mehr Aufwand, da je nach Konsole eventuell verschiedene Ports benötigt werden. Auch Windows-Updates, Monitoring-Tools und sonstige Serverdienste sind relevant für Server. Outlook / Exchange, Internet und Intranet-Verkehr, Business-Anwendungen wie SAP oder Siebel et cetera kommen ins Spiel, sobald Clients oder Terminalserver mit entsprechenden Applikationen auf der anderen Seite der Firewall betrieben werden.

Fazit

Für unterschiedlichste Szenarien kann es interessant sein, den Active Directory-Netzwerkverkehr über Firewalls hinweg kommunizieren zu lassen. Am besten ist es, das jeweilige Szenario genau zu planen. Zunächst sollten Sie sich überlegen, zu welchem Zweck über die Firewall kommuniziert werden soll und wie die "Verkehrswege" über die Firewall aussehen. Diese sollten gegebenenfalls angepasst werden. Dann ist es wichtig zu planen, wie und wo welche Applikationen und Dienste laufen sollen.

Sind diese Fakten bekannt, muss noch die Entscheidung getroffen werden, ob die Kommunikation getunnelt werden soll oder ob sie offen bleiben soll, um danach die Firewall-Ports zu definieren. Auf alle Fälle lässt sich das Active Directory in unterschiedlichsten Konfigurationen über eine Firewall einsetzen, sei es zwischen den Domänencontrollern oder hin zu Clients oder Terminalservern. *(dr)*

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
TCP/UDP	WAN_DC	*	LAN_DC	88	*		Kerberos
TCP/UDP	WAN_DC	*	LAN_DC	53 (DNS)	*		DNS
UDP	WAN_DC	*	LAN_DC	500 (ISAKMP)	*		Internet Key Exchange (IKE)
ESP	WAN_DC	*	LAN_DC	*	*		IPSec ESP
AH	WAN_DC	*	LAN_DC	*	*		IPSec AH

Bild 6: Nach einer IPSec-Konfiguration reichen bereits deutlich weniger Ports aus

Migration vom File Replication Service zur Distributed File System-Replication

In drei Schritten zur besseren Replikation

Neben der Active Directory-Datenbank replizieren Domänencontroller auch das freigegebene Sysvol-Verzeichnis mit seinen Gruppenrichtlinien-Dateien, Anmelde- und Startskripten und das vordefinierte Netlogon-Standardprofil für neue Benutzer. Die Replikation der Dateien übernimmt seit Windows 2000 der "File Replication Service" (FRS). Nicht nur Replikationsfunktionen des ebenfalls in Windows 2000 gelieferten "Distributed File Systems" (DFS) bewegte Microsoft dazu, den veralteten FRS nicht mehr weiterzuentwickeln. Wie Sie auf den Replikationsdienst des DFS migrieren, zeigt dieser Workshop.

DFS hat sich mit den Jahren stetig weiterentwickelt, während FRS im selben Zeitraum wenige bis keine Entwicklungen erfahren hat. Faktisch hat Microsoft seit Windows Server 2003 R2 keine Verbesserungen mehr für FRS bereitgestellt, und so hat FRS gegenüber DFS einige Nachteile: Bei der Replikation neuer oder geänderter Daten versucht FRS stets, die komplette geänderte Datei zu übertragen. Änderungen an großen Dateien führen dazu, dass die komplette Datenmenge zwischen den Domänencontrollern (DC) übertragen wird. DFS nutzt "Remote Differential Compression" und berechnet die Datenunterschiede zwischen Quelle und Ziel auf Blockebene. Anschließend werden nur geänderte Dateiblöcke zwischen den DCs übertragen. Im Bestfall bedeutet dies, dass DCs nur einen Bruchteil der Datei replizieren.

Quelle: Martina Berg – Fotolia.com

Hat ausgedient: der alte Replikationsdienst FSR

FRS tut sich zudem schwer, dem Administrator seinen Zustand mitzuteilen. Zwar gibt es einige Kommandozeilenprogramme, die bei Benutzung weitestgehend Auskunft über den aktuellen Status des Dienstes und den Freigaben geben, eine integrierte Überwachungslösung bietet allerdings nur DFS. Die DFS-Konsole kennt eigene Berichte, auch für die Einsicht in den Zustand von Freigaben. Für Managementsysteme wie System Center bietet Microsoft sogenannte Management Packs an, um große DFS-Implementierungen überwachen zu können.

Den Einsatz von RODCs unterstützt FRS nur bedingt – bei Änderungen am SYSVOL auf dem RODC kann es zu Problemen kommen. Wenn die Anzahl der Änderungen ein gewisses Maximum überschreitet, dann steht die SYSVOL-Replikation komplett. Eine Änderung hierfür ist nicht in Sicht – FRS befindet sich in der Wartungsphase bei Microsoft, die Updates nur für Sicherheitsprobleme erlaubt. Neue Features oder unkritische Änderungen werden nicht mehr durchgeführt.

Migration zu DFSR

Aus den genannten sowie weiteren Gründen [1] sieht die Zukunft des FRS nicht gerade rosig aus. Domänen, die mit Server 2008 R2 erstellt und im Domänenfunkti-

Migrationsschritte mit dfsrmig.exe

Bezeichnung	Status	Kurzbeschreibung	Replikationsmedium
Started	0	Der Grundstatus, in dem sich jede Domäne befindet, deren SYSVOL-Dateistruktur mit FRS repliziert wird. Hier wird die Migration gestartet.	Einziger Replikationsdienst für SYSVOL ist FRS. DFS kann bereits installiert worden sein, wird jedoch nicht für SYSVOL verwendet.
Prepared	1	Der erste Migrationsstatus. DFS ist bereits installiert und repliziert die SYSVOL-Daten parallel.	FRS ist weiterhin der Hauptreplikationsdienst für SYSVOL. Für DFSR wird eine eigene SYSVOL-Kopie erstellt und so konfiguriert, dass die aktuellen SYSVOL-Daten parallel zur FRS-Replikation ebenfalls zwischen den DCs repliziert werden. Sowohl FRS als auch DFS replizieren in diesem Status.
Redirected	2	Der zweite Migrationsstatus. DFS übernimmt die Replikation von SYSVOL.	DFS übernimmt die Hauptreplikation des SYSVOL-Verzeichnisses. FRS wird weiterhin als Backup-Lösung verwendet und repliziert weiterhin die SYSVOL-Daten. Sowohl DFS als auch FRS sind in der Lage, Daten unter den DCs zu replizieren.
Eliminated	3	Der dritte und finale Status. FRS ist deaktiviert, DFS ist der einzige Replikationsdienst.	DFS übernimmt die alleinige Replikation des SYSVOLs. Der FRS-Dienst und die FRS-SYSVOL-Freigabe werden deaktiviert und gelöscht. Der FRS-Dienst kann als Rolle von den Domänencontrollern entfernt werden.

onsmodus "Server 2008 R2" geschaffen wurden, verwenden von vornherein DFSR. Alle anderen Active Directory-Domänen, ältere oder mit Windows Server 2008 aufgesetzte, benötigen eine Migration zu DFSR, um für die Replikation des System Volumes fit gemacht zu werden. Voraussetzung für den Wechsel ist Windows Server 2008 als DC-Betriebssystem und der Domänenfunktionsmodus "Windows Server 2008". Frühere Windows-Systeme sind nicht in der Lage, DFSR als Replikationsdienst zu verwenden. Als weitere Voraussetzung für die DFS-Migration sind die installierten DFS-Komponenten des "Dateiserver"-Features zu nennen. Sie müssen auf allen DCs installiert sein.

Grundlage der Migration ist das Kommandozeilen-Werkzeug *dsfrmig.exe*, das Microsoft mit Server 2008 ausliefert. Mit dem Tool manövrieren Sie Ihre Domäne durch drei aufeinanderfolgende Migrationsschritte, aus denen die eigentliche Ablösung von FRS durch DFS besteht. Die Schritte sind jeweils in sich abgeschlossen und können somit ohne Zeitdruck durchgeführt werden. Das macht es möglich, jeden Schritt zu verifizieren, die Gesundheit der Replikation ständig zu testen und selbst in stark verteilten Umgebungen mit langer Replikationskonvergenz ein gutes Ergebnis zu erzielen. Nach jedem Schritt, außer dem finalen, ist ein Rollback zum vorherigen Stand möglich. Die vier Zustände vor, zwischen und nach den Migrationsschritten heißen "Started", "Prepared", "Redirected" und "Eliminated". "Started" ist der Grundstatus, indem sich jede Domäne befindet, deren SYSVOL-Replikation FRS verwendet.

Bevor die Migration in Angriff genommen wird, muss der aktuelle Zustand der Replikation untersucht werden. Die momentane Replikation mit FRS wird mit Sonar, Ultrasound und FRSDiag überprüft. Alle Tools sind frei bei Microsoft zum Download verfügbar [2]. Gerade FRSDiag gibt einen guten Überblick über die Replikation, listet Probleme aus den Ereignisanzeigen auf und durchkämmt das Ntfrs-Logfile.

Während der Migration sollten Sie darauf achten, dass keine umfangreichen Änderungen an der Datenbasis des SYSVOLs durchgeführt werden. In der Regel finden die Statuswechsel für die Migration am besten zu Randzeiten statt, in denen Domänencontroller und die verfügbare Bandbreite geringerer Last ausgesetzt sind. Während der Statuswechsel stoppen Domänencontroller die Veröffentlichung des SYSVOLs für kurze Momente – in dieser Zeit ist das Verzeichnis dann nicht durchgängig erreichbar.

Schritt 1: Von Startet zu Prepared

Im ersten Migrationsschritt, der die Umgebung von "Started" in "Prepared" überführt, dupliziert *dfsrmig.exe* das SYSVOL-Verzeichnis und erstellt eine zweite Freigabenstruktur für die Replikation mit DFSR. Der Replikationsdienst wird hierbei so konfiguriert, dass dieser eine zusätzliche Replikation von SYSVOL erstellt. Im Migrationsstatus "Prepared" angelangt, replizieren Domänencontroller das SYSVOL-Verzeichnis doppelt: wie gewohnt mit FRS, das als Hauptreplikationsdienst fungiert und zusätzlich mittels DFS. Dieser erste Migrationsschritt wird, wie alle weiteren Schritte, auf dem Domänencontroller ausgeführt, der die PDE-Emulatorrolle trägt. Bei Unsicherheit darüber, welcher DC das ist, hilft das Kommando *netdom query fsmo*. Es listet alle Träger der FSMO-Rollen auf. Die Migration leiten Sie mit dem Befehl *dfsrmig.exe /SetGlobalState 1* ein, wobei der globale Migrationsstatus 1 für "Prepared" steht. Das Tool führt dann selbstständig die notwendigen Schritte für die DFSR-Konfiguration und die Duplizierung des SYSVOL-Verzeichnisses aus. Am Ende der Tätigkeiten informiert es den Nutzer mit der Meldung "Succeeded".

Die Änderung wird an allen Domänencontrollern der Domäne vorgenommen. Es kann einige Zeit in Anspruch nehmen, bis alle DCs entsprechend konfiguriert sind und den SYSVOL-Share auf DFSR-Ebene erstellen. Den Gesamtfortschritt überprüfen Sie nun ebenfalls mit *dfsrmig.exe* – mit dem Schalter "/GetMigrationState":

```
dfsrmig.exe /GetMigrationState
```

Das Migrationstool kontaktiert alle Domänencontroller, prüft ihren lokalen Mi-

Bild 1: Der Migrationsstatus wird mit dem Schalter "GetMigrationState" abgefragt – *dfsrmig.exe* fragt den Status aller DCs ab

grationsstatus und vergleicht ihn mit dem Sollstatus auf dem PDC, der zuletzt via "SetGlobalState" gesetzt wurde. Sind bereits alle teilnehmenden DCs migriert, quittiert das Tool den Status mit einer Erfolgsmeldung. Konnte der neue Migrationsschritt noch nicht auf allen DCs durchgeführt werden, meldet *dfsrmig.exe* die noch fehlenden Mitglieder. Bleiben diese Domänencontroller länger als über die Replikationsdauer hinaus in diesem falschen Status, sollten Sie die Replikation und das Ereignislog auf diesen Mitgliedern kontrollieren.

Ist der aktuelle Status in der gesamten Domäne einheitlich, wird es vor dem nächsten Migrationsschritt Zeit, die Dienste zu testen. Zu prüfen sind in diesem Stadium beide Replikationen – die Replikation des SYSVOL-Verzeichnisses via FRS mit den zuvor verwendeten Überwachungstools, sowie das SYSVOL-Duplikat des DFSR. Die beteiligten Domänencontroller sollten nun über zwei SYSVOL-Freigaben verfügen. Im Dateisystem, per Vorgabe in *%systemroot%*, sind sie als "SYSVOL" und "SYSVOL_DFSR" gekennzeichnet. Beide Freigaben beinhalten nach der Überführung nach "Prepared" dieselben Daten. Änderungen am Live-SYSVOL werden nicht direkt in das SYSVOL-Duplikat für DFSR übernommen, denn es besteht keine ständige Duplizierung oder ein Abgleich zwischen den beiden SYSVOL-Freigaben. Das Kopieren des SYSVOLs in den SYSVOL_DFSR findet nur zu den beiden Statusüberführungen nach "Prepared" und "Redirected" statt. Zwischen den beiden Stati, etwa in diesem Stadium der Migration, findet kein automatischer Abgleich statt. Die Überprüfung der DFSR-Replikation beschreiben wir später in dieser Rubrik des Sonderhefts detailiert, hierfür eignen sich die DFS-eigenen Werkzeuge bestens.

Haben alle Domänencontroller den richtigen Migrationsstatus übernommen und sind die Tests zu FRS und DFSR positiv ausgefallen, ist die Domäne bereit für den folgenden Schritt – die Überführung in den Status "Redirected". Wie Sie in unserer Tabelle "Migrationsschritte mit dfsrmig.exe" sehen, wird im Zustand "Redirected" der Wechsel der Replikationsdienste vollzogen. Der Inhalt des FRS-SYSVOLs wird nochmals nach SYSVOL_DFRS kopiert, wonach anschließend DFSR als verantwortlicher Dienst für die SYSVOL-Replikation konfiguriert wird. FRS läuft als Dienst weiterhin auf den DCs – auch die Replikation des "alten" SYSVOL-Verzeichnisses wird weiterhin durchgeführt, neue Änderungen behandelt allerdings DFSR.

Schritt 2: Redirected

Der neuerliche Statuswechsel für den nächsten Schritt der Migration leiten Sie mit *dfsrmig.exe /SetGlobalState 2* ein – Status 2 für "Redirected". Erneut vergehen einige Minuten bis Stunden, je nach Replikationstopologie, bis alle Domänencontroller der Domäne den neuen Migrationsstatus annehmen. In diesem Stadium ist besonders wichtig, die Replikation mit DFSR im Auge zu behalten. Der Migrationsschritt "Redirected" ist vermutlich der Status, der während einer Umstellung über einen langen Zeitraum genutzt wird – nicht nur, weil die Replikation mit DFSR ausgiebig getestet werden muss, sondern weil ein Sprung auf die nächste Stufe "Eliminated" auch keinen Weg zurück bedeutet. Den Fortschritt des Statuswechsels überwachen Sie erneut mit dem Schalter "/GetMigrationState". Arbeiten alle Domänencontroller im "Redirected"-Status, ist die eigentliche Arbeit vollbracht: Das System Volume wird mit DFSR repliziert. Es ist an der Zeit, die DFSR-Replikation auf Herz und Nieren zu testen. Läuft alles zur vollsten Zufriedenheit, dürfen Sie dann mit dem letzten Schritt, der Eliminierung des FRS-Dienstes auf den DCs, liebäugeln.

Einen Schritt zurück

Kommt es wider Erwarten zu Problemen bei einem der Migrationsschritte oder soll die zuletzt durchgeführte Änderung rückgängig gemacht werden, können Sie bis zu diesem Zeitpunkt mit *dsfrmig.exe* den Migrationsstatus um eine Stufe zurücksetzen. Klappt der Wechsel von "Prepared" (Status 1) auf "Redirected" (Status 2) nicht korrekt auf allen DCs, auf einigen jedoch schon, sollten Sie den Status per *dfsrmig.exe /SetGlobalState 1* zurücksetzen. Anschließend können Sie das Problem analysieren und den Statuswechsel zu "Redirected" erneut durchführen. Beim Zurückrollen eines Migrationsschrittes führt *dfsrmig.exe* die Migrationsschritte in umgekehrter Reihenfolge erneut aus und nimmt alle Änderungen zurück. Kopierte Daten von "SYSVOL" nach "SYSVOL_DFSR" werden beim Rollback zurückkopiert – gegebenenfalls auch mit neuesten Änderungen, falls in der Produktivumgebung bereits mit dem System Volume gearbeitet wurde.

Bild 2: DCs, die noch nicht in den aktuellen Status überführt wurden, meldet *dsfrmig.exe*

Schritt 3: Eliminated

Führen Sie nun den letzten und endgültigen Statuswechsel mit *dsfrmig.exe /SetGlobalState 3* aus, werden sämtliche FRS-Referenzen von den Domänencontrollern entfernt. Zu diesem Zeitpunkt wurde durch das Administratorenteam mehrfach verifiziert, dass die Replikation mittels DFSR einwandfrei funktioniert, die Domänencontroller keine Fehler in ihren Ereignisanzeigen aufweisen und dass die Ausgabe von *net share* auf allen Domänencontrollern den lokalen Pfad zu SYSVOL und NETLOGON zum Ordner "SYSVOL_DFSR" ausweist. Mit der Durchführung des finalen Schrittes können Sie, sofern keine weiteren Verzeichnisse über FRS repliziert werden, den File Replication Service deaktivieren und anschließend komplett von den Domänencontrollern entfernen. Die Migration ist damit abgeschlossen.

DFS(R) überprüfen

DFS bietet deutlich bessere Überwachungsmöglichkeiten als sein Vorgänger FRS. Anders als FRS besitzt es nämlich eingebaute Reportingfunktionen direkt in der Verwaltungskonsole. Beim Durchforsten der Replikationsgruppen und der Auswahl einer beliebigen Gruppe erscheint im rechten Aktionsfeld die Option "Diagnosebericht erstellen…". Es öffnet sich ein Assistent, der den Nutzer zwischen verschiedenen Berichten auswählen lässt. Mit dem "Integritätstest" erstellt die Verwaltungskonsole einen HTML-Bericht, der die Effizienz und den Erfolg der DFS-Replikation aufzeigt. Der Bericht weist auf Fehler einzelner Replikationsmitglieder hin und zeigt generelle Details zur Konfiguration der beteiligten Server an. Der Propagierungstest injiziert eine Testdatei in einen verteilten Ordner, die anschließend, wenn die Replikation funktioniert, auf alle Mitglieder der Replikationsgruppe übertragen wird. Danach kann der Propagierungsbericht erstellt werden, der eine Darstellung aus den injizierten Testdaten erzeugt. Dabei wird verdeutlicht, welche Testinjektionen stattfanden, ob und wie schnell sie auf alle Teilnehmer repliziert werden konnten und wie die Replikation in einem Diagramm aussieht.

Zu Diagnosezwecken und für die Überprüfung des DFS-Betriebes eignet sich das Kommandozeilenprogramm "DFSDiag". Es wird mit der Rolle "Dateidienste", mit der DFS selbst installiert wird, aufgespielt. Die einfachste Überprüfung mit DFSDiag ist die Überprüfung der Konfiguration der beteiligten Domänencontroller. Mit dem Kommando

```
dfsdiag.exe /testdcs /domain:contoso.com
```

überprüft DFSDiag dann, ob der DFS-Namensraumdienst auf den DCs automatisch gestartet wird, ob Standort-IP-Adresszuweiseungen in Active Directory korrekt konfiguriert sind und ob Weiterleitungen auf Grund von Standortkosten für NETLOGON und SYSVOL richtig funktionieren. Für SYSVOL-spezifische Zwecke sollte dann *dfsrdiag.exe* zum Einsatz kommen. Bemerkenswert ist das "R" in der Mitte des Kommandos. DFSRDiag beschäftigt sich ausschließlich mit der DFS-Replikation, während DFSDiag primär DFS-Namespaces fokussiert.

Ein Mittel, um die Replikation selbst zu prüfen, ist auch das sogenannte "Backlog". Das Backlog ist die Menge der zur Replikation ausstehenden Daten. Je größer das Backlog – also die Menge an Daten, die noch nicht zwischen DCs repliziert wurde – desto sicherer gibt es ein Problem mit der Replikation oder der Bandbreite. DFSRDiag hilft bei der Überprüfung des Backlogs:

```
dfsrdiag backlog /RGName:"Domain
  System Volume" /RFName:"SYSVOL
  Share" /SMem:dc1 /RMem:dc2
```

Der Befehl listet die Anzahl der ausstehenden Dateien für die Replikation:

```
Member <dc2> Backlog File Count: 32
```

Dies bedeutet, 32 Dateien stehen zur Replikation von dc1 auf dc2 an. Schrumpft die Zahl bei späterer Betrachtung nicht, kann ein Problem bei der Replikation vorliegen – oder es werden dauerhaft Daten zur Replikation markiert, was auf eine Massenänderung hindeuten kann. Handelt es sich um einen anderen Ordner als "SYSVOL", wäre hier eine sinnvolle Prüfung, ob der Replikationszeitplan korrekt eingestellt ist oder die Replikation erst zu einem späteren Zeitpunkt aufgenommen wird. Eine weitere Problemquelle stellen Virenscanner auf DCs dar, die das Sysvol-Verzeichnis scannen und minimale Änderungen den vorhandenen Daten vornehmen. Dies hat zur Folge, dass DFSR stets nach dem Scanlauf des Virenscanners alle Daten erneut repliziert. Ist die Anzahl der Backlog-Dateien 0, langweilt sich die Replikation im Augenblick – dann sind alle Daten up-to-date.

Fazit

Administratoren, die ihre Domänencontroller bereits auf Windows Server 2008 oder 2008 R2 umgestellt haben, sollten keinen technischen Grund finden, der gegen eine Migration des SYSVOLs auf DFSR spricht. Die höhere Effizienz durch die deutlich performantere, Bandbreitenschonende Replikation und die größere Stabilität, die Journalfehler minimieren, sollten Grund genug für den Wechsel sein. Hinzu kommt, dass FRS nicht mehr aktiv weiterentwickelt wird – und schon seit einiger Zeit keiner Aktualisierung unterzogen wurde. Die Migration mit "dsfrmig" ist zu weiten Teilen ein automatischer Vorgang, der lediglich Kontrollmaßnahmen nach jedem Schritt bedingt. *(dr)*

[1] **The Case for Migrating SYSVOL to DFSR**
http://blogs.technet.com/b/filecab/archive/2007/12/26/what-s-new-in-windows-server-2008.aspx

[2] **Download Details: File Replication Service Diagnostics Tool (FRSDiag.exe)**
www.microsoft.com/downloads/details.aspx?familyid=43cb658e-8553-4de7-811a-562563eb5ebf&displaylang=en

Links

Group Policy Preferences effizient nutzen

Mehr Einstellungen, weniger Arbeit

Dank Gruppenrichtlinien bestimmen Sie, was auf Clients läuft und was nicht

Seit der Einführung des Active Directory sind Gruppenrichtlinien ein wichtiger Bestandteil. Mit Windows Server 2008 führte der Hersteller dann gleich mehrere Änderungen bei den Gruppenrichtlinien durch: Die Entwicklerteams änderten das Dateiformat der Administrativen Vorlagen, führten ein zentrales Repository für ADM-Templates ein, verbesserten das Aussehen des Gruppenrichtlinieneditors und verdoppelten beinahe die Anzahl der möglichen Einstellungen. In diesem Beitrag bringen wir Ihnen die Neuerungen der Gruppenrichtlinien näher und zeigen, wie Sie die Änderungen effektiv nutzen können und Stolperfallen aus dem Weg schaffen.

Während des Produktzyklus von Windows Server 2003 hat Microsoft weitere Funktionen zu den bereits vorhandenen Gruppenrichtlinien hinzugefügt. Die Administration wurde durch die Group Policy Management Console (GPMC) bereichert, Software Restriction Policies (SRPs) sorgen für Einschränkungen oder Verbote von unerwünschter Software und WLAN-Einstellungen werden per Richtlinien verteilt und die Anzahl der konfigurierbaren Administrativen Richtlinien wurde nochmals erhöht. Und auch bei den Administrativen Vorlagen hat sich einiges getan.

Administrative Vorlagen 2.0

Administrative Vorlagen werden seit Windows 2000 dafür verwendet, Registrierungseinstellungen über Gruppenrichtlinien zu verteilen. Alle verfügbaren Einstellungen im Gruppenrichtlinieneditor unter "Administrative Vorlagen", sowohl für Computer als auch für Benutzer, sind in sogenannten ADM-Dateien definiert. ADM-Dateien sind einfache, aber speziell formatierte Textdateien, die der Gruppenrichtlinien-Editor einliest und für Administratoren in nutzbare Einstellungen verwandelt. Wer bereits näheren Kontakt mit Administrativen Vorlagen und deren Erstellung zu tun hatte, wird sich mit Sicherheit nur sehr ungern an das gewöhnungsbedürftige Format der ADM-Dateien erinnern. Obwohl ADM-Dateien aus einfachem Text bestehen, sind die verwendete Syntax und die Anordnung der Schlüsselworte nicht einfach zu verstehen. Ein weiteres Problem der ADM-Dateien ist, dass sie nicht sprachneutral sind. Eine englische ADM-Datei wird auf allen Zielsystemen in englisch dargestellt – egal welche Sprache der Rechner spricht, auf dem der Richtlinieneditor aufgerufen wird. Für Konzerne mit mehrsprachigen Administratoren bedeutet dies, dass ADM-Templates in mehrfacher Ausführung in unterschiedlichen Sprachen vorliegen müssen.

Dies war Anlass genug, ein neues, verbessertes Format für die Administrativen Vorlagen zu entwickeln. Seit Windows Vista und Windows Server 2008 werden Administrative Vorlagen im ADM-Format durch ADMX-Dateien in einer XML-Formatierung ersetzt. Microsoft hat hierbei mehrere Ziele verfolgt: Mit der Umstellung der Dateistruktur auf einen XML-Dialekt sind die Daten um Einiges lesbarer – und für Programmentwickler deutlich einfacher zu interpretieren und anzusteuern. Außerdem ist es Microsoft nun gelungen, die Vorlagen sprachneutral zu gestalten. Die zuvor hardkodierten Texte wurden durch Variablen ersetzt. Die Definition dieser Variablen, die Beschreibungs- und Hilfetexte enthalten, sucht der Gruppenrichtlinieneditor in einem zweiten Dateityp, der ADML. Die Sprachdatei, die genau so

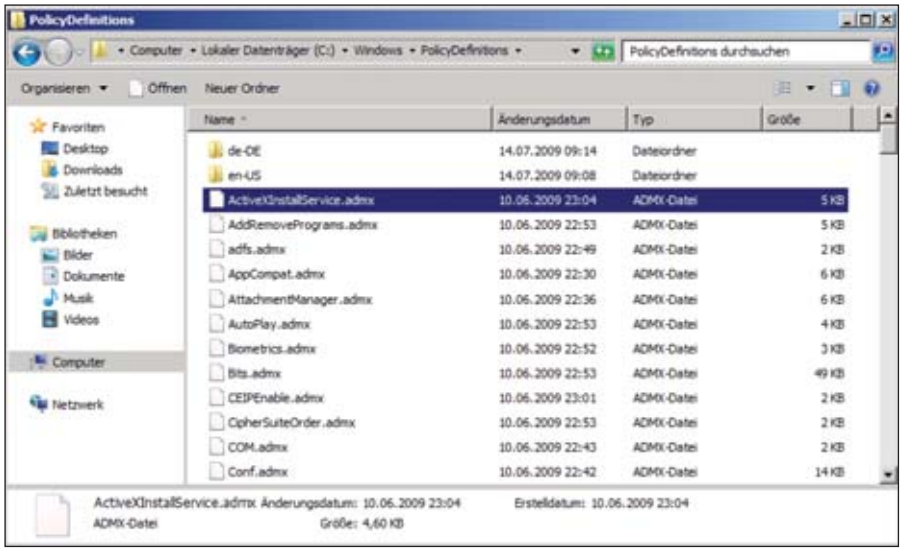


Bild 1: Mehrere Sprachen sind mit ADMX-Dateien und den Sprachdefinitionen in ADML kein Problem mehr

heißt wie die ursprüngliche Administrative Vorlage, kann in mehreren Sprachen, abgelegt werden und in unterschiedlichen Sprachordnern existieren. Der Gruppenrichtlinieneditor lädt daraufhin die Sprachdatei zum ADMX, die zur aktuellen Systemsprache passt. Für die Administrative Vorlage *System.ADMX* können demnach mehrere Sprachdateien namens *System.ADML* existieren, die in den Unterordnern "de-DE" oder "en-US" abgelegt werden – sprachspezifisch für alle eingesetzten Systemsprachen. Der Gruppenrichtlinieneditor englischer Systeme wird die englischen Sprachdateien laden, während deutsche Systeme die ADML-Sprachdatei im Ordner "de-DE" bevorzugen.

An der Art, wie Clients Gruppenrichtlinien verarbeiten, ändert sich dadurch nichts. Die Zielcomputer der erstellten Gruppenrichtlinien bekommen nicht mit, aus welchem Vorlagentyp ihre Richtlinien kreiert wurden. Die Vorlagen dienen nur der visuellen Darstellung im Gruppenrichtlinieneditor – werden Einstellungen definiert oder verändert, speichert der Editor die Definitionen in einer vorlagenunabhängigen Datei ab – der *Registry.POL*. Diese Datei wird zum Zeitpunkt der Richtlinienverarbeitung von den Zielcomputern gelesen und verarbeitet. Das Format hat sich zwischen den Betriebssystemversionen nicht verändert, so dass Windows XP-Clients Einstellungen verstehen, die mit Windows Vista-GP-Verwaltungscomputern erstellt wurden. Aus diesem Grund gilt es als offene Empfehlung und Best Practice, dass für die GP-Verwaltung stets ein Rechner mit dem aktuellste Betriebssystem der Umgebung verwendet wird. Administratoren stellen so sicher, dass sie stets die neuesten Einstellungen für kommende Clients ausrollen können und sich gleichzeitig nicht gegenseitig behindern, wenn eines der Administrationsteams ein anderes Betriebssystem zur Administration nutzt.

Die Verwaltungsrechner müssen keineswegs ständig genutzte Computer aus der Domäne sein – für die GPO-Verwaltung ist es ausreichend, einen Windows-Client – etwa unter Windows Vista oder Windows 7 – zu installieren und darauf das "Remote Server Administration Toolkit" zu konfigurieren. Vielerorts hat es sich bewährt, keine physische Maschine für die GP-Administration zu nutzen, sondern eine VM auf einem zentralen Server oder einen Terminal Server hierfür bereitzustellen, auf dem sich dann die Mitglieder des GPO-Teams anmelden können.

Vorlagen zentral lagern

Neben der Sprachneutralität bietet der Einsatz von ADMX-Vorlagen einen weiteren Vorteil: die Möglichkeit, ADMX-Dateien zentral zu lagern. Die zentrale Lagerung wirkt einem Problem entgegen, das seit jeher das Standardverhalten des Gruppenrichtlinieneditors ist: dem sogenannten "SYSVOL-bloat". Wird eine Gruppenrichtlinie mit einer Einstellung aus den "Administrativen Vorlagen" erstellt, so kopiert der Gruppenrichtlinieneditor die verfügbaren Standard-ADM-Vorlagendateien, in den Ordner "adm" in *\\domain.tld\SYSVOL\domain.tld\Policies\{Policy-GUID}\Adm*. Die Vorlagen werden dort abgelegt, um sie für spätere Änderungen an den Einstellungen der Administrativen Vorlagen laden zu können – für die Verarbeitung der Gruppenrichtlinien sind sie nicht nötig. Der entscheidende Nachteil dieses Verhaltens ist, dass der Richtlinieneditor die ADM-Dateien für jede Gruppenrichtlinie erneut kopiert. Dies bläht das SYSVOL-Verzeichnis auf – welches wiederum zu allen Domänencontrollern der Domäne repliziert werden muss. Die Standard-ADM-Vorlagen belasten das replizierte Verzeichnis mit etwa 4 MByte bis Windows Server 2003 und etwa 9 MByte ab Windows Server 2008 pro GPO. Allein 50 Gruppenrichtlinien können das SYSVOL-Verzeichnis auf diese Weise um etwa 200 bis 350 MByte, je nach eingesetztem Managementsystem, vergrößern.

Die Lösung des Problems sieht Microsoft im sogenannten "Central Store". Der Central Store ist ein Ordner in der SYSVOL-Dateistruktur, in dem alle ADMX-Vorlagen samt der benötigten Sprachpakete abgelegt werden. Benötigte Sprachpakete sind die, die von anderssprachigen Gruppenrichtlinien-Administratoren verwendet werden sollen. Per Voreinstellung sind die Betriebssysteme ab Windows Vista, auch die Serverversionen, so konfiguriert, dass sie beim Öffnen des Gruppenrichtlinieneditors bevorzugt die ADMX-Dateien des Central Stores laden. Nur wenn kein Central Store definiert ist, werden lokal installierte ADMX-Dateien aus dem Ordner "%systemroot%\PolicyDefinitions" verwendet.

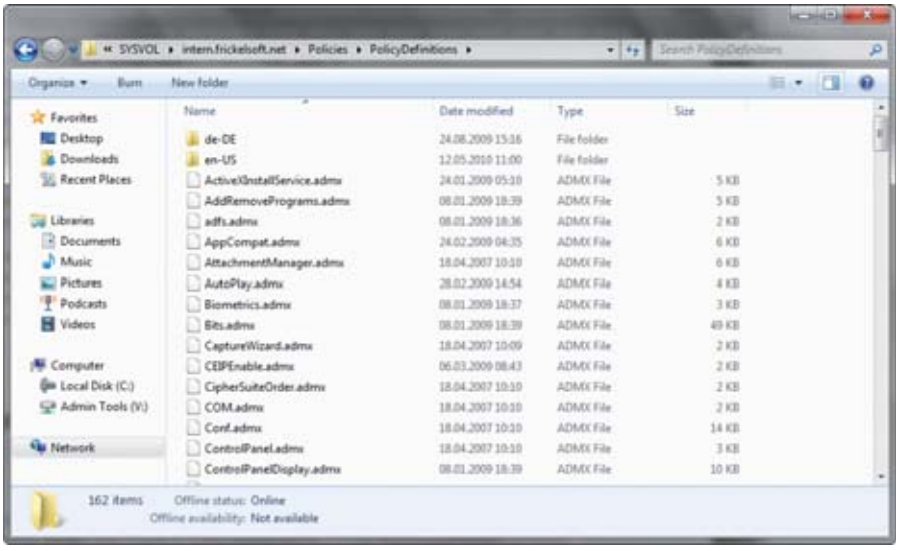


Bild 2: Der Central Store minimiert das SYSVOL-Bloat-Problem

Den Central Store anzulegen gestaltet sich einfach: Im SYSVOL unter *\\domain.tld\SYSVOL\domain.tld\Policies* legen Sie einen neuen Ordner namens "PolicyDefinitions" an, in den Sie anschließend alle verwendeten ADMX-Dateien kopieren. Die ADMX-Dateien befinden sich auf jedem Windows-Rechner ab Vista im Ordner "%systemroot%\PolicyDefinitions". Bevorzugt sollten Sie allerdings die ADMX-Dateien des neuesten Betriebssystems der Umgebung verwenden. Als Unterordner werden hier die jeweiligen Sprachordner gespeichert, in denen die ADML-Dateien für die zusätzlichen Sprachen liegen.

Leider funktioniert der Central Store nur für ADMX-Dateien und nicht für ältere ADM-Dateien. Bei der Erstellung einer Gruppenrichtlinie, die ein ADM-Template verwendet, werden weiterhin die notwendigen Daten in das ADM-Verzeichnis der Richtlinie auf dem SYSVOL kopiert – und füttern damit den bereits aufgeblähten Speicher. Es wird also dringend empfohlen, die Gruppenrichtlinienverwaltung auf Windows Clients ab Vista zu verlagern, um das neue Vorlagenformat und den Central Store nutzen zu können. Wer die Möglichkeit hat, sollte die GP-Administration also von einer aktuell gepatchten Windows 7-Maschine durchführen. Umgebungen mit vielen selbsterstellten ADM-Templates sollten sich um eine Konvertierung der Vorlagen ins ADMX-Format bemühen. Einen komfortablen ADM-zu-ADMX Konverter finden Sie unter [1].

Suchen, finden und kommentieren

Obwohl die Richtlinien in einer kategorisch geordneten Baumstruktur angeordnet sind und seit Windows Vista mit der Einführung von ADMX-Templates noch granularer aufgeteilt wurden, ist es manchmal schwierig, die richtige Richtlinie für seine Vorhaben zu lokalisieren. Eventuell erinnern Sie sich noch daran, wie die Richtlinie hieß oder für welche Betriebssysteme sie genutzt werden kann – doch wenn Sie sich nicht an den Ort in der Knotenstruktur erinnern können, hilft nur die Internetsuche. Ein Ausweg ist das "Group Policy Reference Sheet" im Excel-Format [2]. Admins können darin suchen, nach Betriebssystem und Knoten filtern und sich die Registrierungszweige ansehen, die die Einstellungen verändern. Das Sheet behandelt die Einstellungen der "Administrativen Vor-

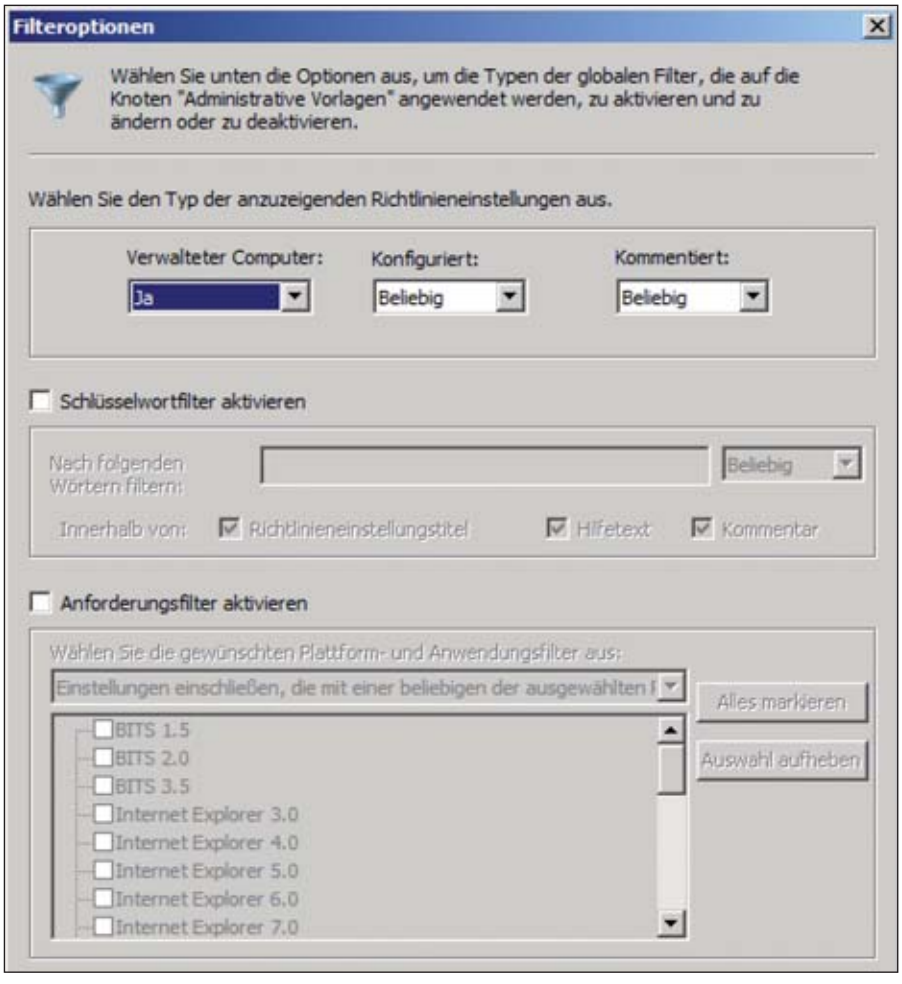


Bild 3: Der GPEditor hilft Administratoren bei der Suche nach Administrativen Vorlagen

lagen". Für Suchen nach "Administrativen Vorlagen" bietet der Gruppenrichtlinieneditor eine Filter-Funktion, die sich per Rechtsklick auf den Knoten bedienen lässt. Ab Windows Vista oder Server 2008 kennt das Kontextmenü die beiden Punkte "Filter aktivieren" und "Filteroptionen". Hierüber definieren Sie Suchparameter, um gewünschte Einstellungen ein- oder auszublenden.

Eine dritte Suchmöglichkeit kommt aus der Cloud und ist auf der Windows Azure-Plattform als Webapplikation verfügbar. Hierbei bietet Microsoft eine Onlinesuche [3] nach Group Policy-Einstellungen an. Neben der Suchfunktion bietet das Webtool interessante Informationen zu den einzelnen GP-Einstellungen – etwa den Pfad im GPEditor oder die unterstützten Betriebssysteme und -komponenten. Es vergisst dabei nicht, den kompletten Registrierungspfad zum verantwortlichen Schlüssel zu nennen.

Wenn viele Köche Brei verderben, liegt das meist daran, dass sich die Akteure unzureichend oder überhaupt nicht absprechen. Große und örtlich verteilte Teams leiden zunehmend unter diesem Problem. Was die Gruppenrichtlinien-Administration angeht, so gibt es bisher leider nicht viel an Unterstützung in Windows, die Teams zur gemeinsamen Administration nutzen können. Eine weitere kleine Funktion im GPEditor kann den Schmerz der geteilten GP-Administration lindern: In den Eigenschaften von GP-Einstellungen darf über den Reiter "Kommentar" in Windows Server 2008 beziehungsweise das Kommentarfeld in 2008 R2 kommentiert werden. Das Feld merkt sich jegliche Eingaben, die Benutzer zur gewählten Einstellung machen und zeigt diese sowohl in der Richtlinienübersicht in der Spalte "Kommentar: ja", als auch im "Einstellungen"-Reiter im HTML-Report der GPMC. Leider werden weder der Zeitpunkt des Kommentars noch dessen Autor gespeichert – es erfordert also weiterhin die Disziplin der Administratoren, Einträge

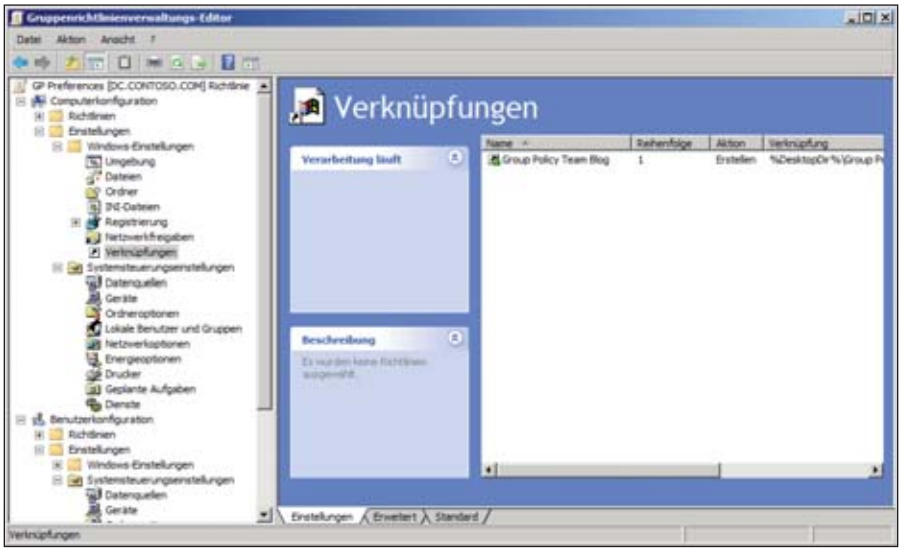


Bild 4: Die Preferences bereichern die bisherigen Gruppenrichtlinien um eine große Anzahl neuer Einstellungen (links)

sorgfältig zu erstellen und zu pflegen. Die Kommentare dienen aber durchaus der Übersicht und der gegenseitigen Information, wenn mehrere GP-Admins am Werk sind – und werden mit Sicherheit, da sie mit der GPO gespeichert werden, wahrscheinlicher gelesen als eine abgelegte GP-Papierdokumentation.

Scripting ade!

Die wohl auffälligste Neuerung bei den Gruppenrichtlinien in Windows Vista und Server 2008 sind zweifelsfrei die "Group Policy Preferences". Diese führen eine ganze Reihe neuer Richtlinieneinstellungen ein, die bis dato – wollte man sie auf Clients erzwingen – mühsam mit Skriptaufrufen ausgerollt werden mussten. Die neuen Einstellungen integrieren sich wie bisherige Einstellungen mühelos im GPEditor. Die Ansicht der Richtlinien unter "Computereinstellungen" und "Benutzereinstellungen" wird neu aufgeteilt: Bisher bekannte Einstellungen finden sich unter "Richtlinien", die neuen Preferences unter "Einstellungen". Besonders hervor sticht die einfache Handhabung der Preferences. Wo immer möglich, hat Microsoft die Administrationsoberfläche der Einstellung in Windows nachempfunden. Schaltflächen, Buttons und Checkboxen wurden nachgebaut, um Ihnen das Ausrollen bekannter Windowseinstellungen zu erleichtern. Ein gutes Beispiel hierfür sind die regionalen Einstellungen, die wir später noch näher behandelt werden.

Ein Missverständnis seit Einführung der Preferences sind die Voraussetzungen für eine korrekte Erstellung und Übernahme der Richtlinien auf Servern und Clients. Da Preferences mit Windows Server 2008 eingeführt wurden, hält sich das Gerücht, dass eine Domäne im Domänenfunktionsmodus "Windows Server 2008" oder zumindest ein Domänencontroller mit Server 2008 in der Domäne vorhanden sein muss – nichts von beidem ist jedoch wahr. Um Preferences nutzen zu können, sind zwei elementare Voraussetzungen zu erfüllen, die streng betrachtet auch für alle anderen Gruppenrichtlinien vorhanden sein müssen: Sie benötigen ein System, von dem aus Sie Richtlinien mit GP Preferences (GPP) erstellen können. Die Clients müssen daneben in der Lage sein, Preference-Einstellungen zu lesen und zu verstehen.

Wie bereits erwähnt, kann es vorteilhaft sein, ein aktuelles System für die Verwaltung von Gruppenrichtlinien zu nutzen. Diese Regel gilt auch für den Einsatz der GPPs. Nur der GP-Editor in der GPMC unter Windows Vista und 7 oder Server 2008/R2 ist in der Lage, GPP-GPOs zu erstellen. Auf älteren Systemen sind die Preferences nicht in der GPMC und ihrem GPEditor ent-

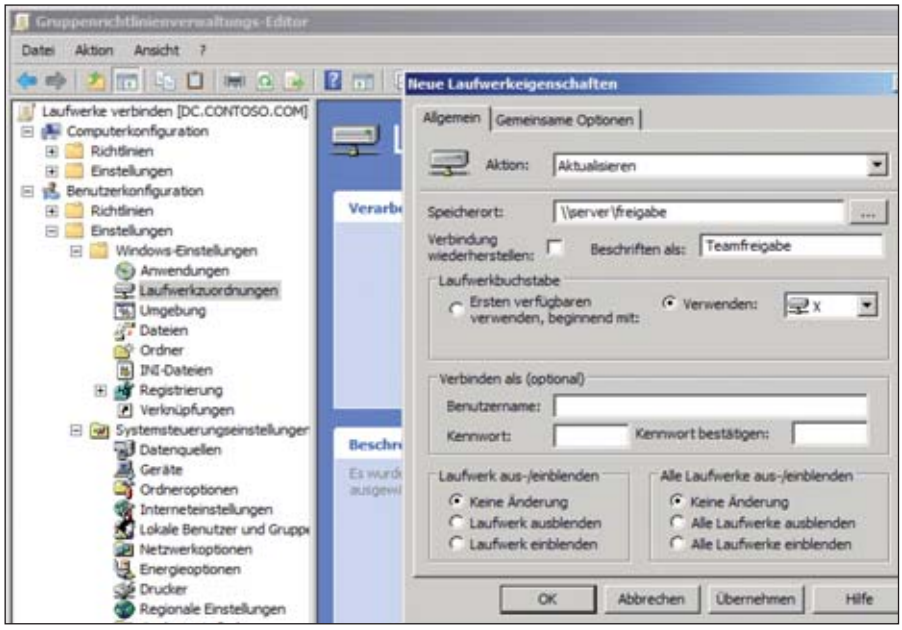


Bild 5: GP-Preferences lassen Administratoren Skriptalpträume zunehmend vergessen – etwa bei der Laufwerkszuweisung

halten. Wollen Sie also Preferences nutzen, ist ein Umzug erforderlich. Die Voraussetzung auf den Zielmaschinen, die für die korrekte Verarbeitung sorgen soll, heißt "Client Side Extension" oder kurz "CSE". Alle Gruppenrichtlinieneinstellungen werden von CSEs abgearbeitet und übernommen – Softwareeinstellungen, Sicherheitseinstellungen, ADM Templates und auch Preferences. Weil aber Preferences erst spät im Lebenszyklus von Windows eingeführt wurden, kennen Windows-Versionen vor 7 die Preferences-CSEs nicht. Deshalb müssen Zielrechner mit den CSEs, soweit nicht bereits geschehen, versorgt werden. Microsoft stellt die CSEs als eigenständigen Download [4] bereit. Alternativ können sie per Windows Update, KB-Nummer 943729, verteilt werden.

Laufwerke gekonnt mappen

Wenn es um Skriptaufgaben im GP-Umfeld geht, sind Beispiele mit Laufwerkszuweisungen geradezu Klassiker. Um mit dieser guten Tradition nicht zu brechen, soll auch dies der Einstieg in GPPs für diesen Abschnitt sein. Administratoren weisen Laufwerke per Skript zu – bevorzugt als Benutzeranmeldeskript, da gerade diese Skripte während der Anmeldung im Kontext des Benutzers laufen und somit das Mapping mit den Benutzerberechtigungen stattfindet. Die Verbindung zu einem Netzlaufwerk erzwingen Sie recht einfach per *NET USE X: \\server\freigabe /persistent:no* in einem Skript, wobei "/persistent:no" dazu dient, die Freigabe nur temporär für die aktuelle Session anzulegen und sie bei einer Abmeldung zu vergessen. Der Befehl verbindet die Freigabe "Freigabe" auf "Server" mit dem Laufwerksbuchstaben "X". Bislang noch recht trivial. Schwieriger wird es, wenn die Zuweisung von Laufwerken nicht so eindeutig vollzogen werden kann, weil das verwendete Skript weitere Abfragen erstellen muss. So etwa ein Skript, das auf eine OU namens "Finanz" verlinkt wird. In der Ziel-OU befinden sich allerhand Benutzer, die teils gemeinsame, teils unterschiedliche Netzlaufwerke benötigen, um ihrer täglichen Arbeit nachzugehen. Als Folge dieser Anforderung bekommt das Skript zusätzliche Logik: etwa eine Abfrage nach Gruppenmitgliedschaft oder Clientcomputer, an dem der Nutzer gerade sitzt – eben zusätzliche Merkmale, die eine Unterscheidung der Zielbenutzer erst möglich machen.

Ein Laufwerksmapping mit Preferences können Sie vollständig im GPEditor erstellen – ganz ohne Skriptarbeit. In "Benutzerkonfiguration / Einstellungen / Windows-Einstellungen / Laufwerkszuordnungen" befindet sich die entsprechende Preference. Mit einem Rechtsklick auf "Neu" öffnen Sie die Eigenschaften für ein neues Laufwerksmapping. Die Standardaktion "Aktualisieren" übernehmen Sie, unter "Speicherort" geben Sie die Freigabeadresse an. Die Option "Verwenden" konfigurieren Sie nun mit dem gewünschten Laufwerksbuchstaben – hier "X". Schon ist das Äquivalent zur oben genannten Skriptzeile fertig.

Nun haben Sie sich das Skript gespart, die komplexere Zuweisung mehrerer Laufwerke an unterschiedliche Benutzergruppen wurde jedoch noch nicht weiter gelöst. Für diesen Zweck nutzen Sie ein weiteres Preferences-Feature: das "Item Level Targeting". Neben den bisher bekannten Methoden der Zielfilterung von Gruppenrichtlinien, dem Verlinken an eine OU, der Sicherheitsfilterung durch Entziehen/Erteilen von

Einige GP-Preferences kennen bei der Erstellung neuer Einstellungen verschiedene Modi, unter denen Sie auswählen können. Im Folgenden erläutern wir Ihnen die vier Modi. Die Erläuterung nutzt die Umschreibung "Objekt" für das gewählte Zielpreference, etwa eine Laufwerkszuweisung, eine Verknüpfung oder ein Druckerobjekt:

- **Erstellen** (grünes Dreieck): Wenn das gewünschte Objekt noch nicht auf dem Zielclient existiert, wird es erstellt. Existiert es bereits, geschieht keine Änderung – es droht also kein Datenverlust, wenn das Objekt bereits existiert.
- **Ersetzen** (rotes Dreieck): Wenn das Objekt auf dem Zielclient existiert, wird es gelöscht. An seiner Stelle wird das neue Objekt erstellt. Existiert noch kein Objekt (mit diesem Namen), wird es erstellt. In jedem Fall wird das neue Objekt am Client erstellt.
- **Aktualisieren** (gelbes Dreieck): Gibt es auf dem Zielclient dieses Objekt, wird es aktualisiert. Dabei werden gewählte Änderungen am Zielobjekt vorgenommen und die bestehenden Einstellungen überschrieben. Einstellungen, die in der Aktualisierung nicht spezifiziert wurden, am Objekt jedoch bestehen, werden nicht überschrieben. Existiert das Objekt als Ganzes noch nicht, wird es erstellt.
- **Löschen** (rotes X): Das Objekt wird ohne weitere Warnung gelöscht.

Erstellen, ersetzen, aktualisieren oder löschen?

Berechtigungen und WMI-Filtern, führen Preferences jetzt Filter ein, die bis auf die Einstellungsebene herunter filtern.

GPOs können mit den bisher bekannten Filtermöglichkeiten, OU-Filterung, Sicherheitsfilterung und WMI-Filter nur als Ganzes angewandt oder weggefiltert werden – niemals einzelne Einstellungen. Eine Methode dieses Problem zu umgehen ist, mehrere Richtlinien zu erstellen und sie den Wünschen entsprechend zu filtern – was zu vielen GPOs und schnell zu Übersichtsproblemen führen kann. Das Item Level Targeting (zu Deutsch: "Zielgruppenadressierung auf Elementebene") für GP-Preferences nimmt sich dieses Problems an: Hiermit filtern Sie auf Einstellungsebene. Die eben erstellte Laufwerkszuweisung kann so konfiguriert werden, dass sie nur in einem bestimmten Fall vom Zielbenutzer angewandt wird – in allen anderen Fällen wird sie ignoriert. Ziel ist es nun, in einer GPO mehrere GP-Preference-Einstellungen zu erstellen und sie so mit Item Level Targeting zu filtern, dass die Zielbenutzer all ihre Laufwerke erhalten – und nur diese. Und das alles mit nur einer GPO.

Um das zuvor begonnene Beispiel fortzusetzen, verwenden wir die Laufwerkszuordnung "X" nur für eine kleine Gruppe von Benutzern. Nur Anwender, die entweder der Gruppe "Finances" oder "Sales" angehören oder deren Rechnername mit "FNCS" für "Finances" beginnt, sollen die Freigabe zugewiesen bekommen. Weitere Klauseln und Abfragemöglichkeiten mit ILT werden später im Beispiel deutlich. Das kleine, aber feine Vorhaben lösen Sie wie folgt: Im Eigenschaftenfenster des Preferences wählen Sie den Reiter "Gemeinsam" und dort die letzte Checkbox "Zielgruppenadressierung auf Elementebene" aus. Nun klicken Sie auf den Button "Zielgruppenadressierung". Die Liste der möglichen Elemente ist lang – viele davon können nur schwer oder teils gar nicht per Skript angesprochen oder untersucht werden. Der Gruppenrichtlinieneditor öffnet daraufhin den Zielgruppenadressierungseditor. In diesem Editor wählen Sie nun – per Auswahl der Elemente aus "Neues Element" – die Bedingungen für die Anwendung des Preferences aus. Für die beiden Gruppenprüfungen ist das Element "Sicherheitsgruppe" das Richtige – dort tragen Sie den Gruppenname entweder von Hand oder per Auswahl ein. Per Vorgabe werden mehrere Elemente mit dem logischen "UND" (im Editor: "AND") verknüpft, das für das Beispiel jedoch nicht korrekt ist. Markieren Sie die zweite Gruppenprüfung und wählen F6, werden die Bedingungen per "ODER" verknüpft.

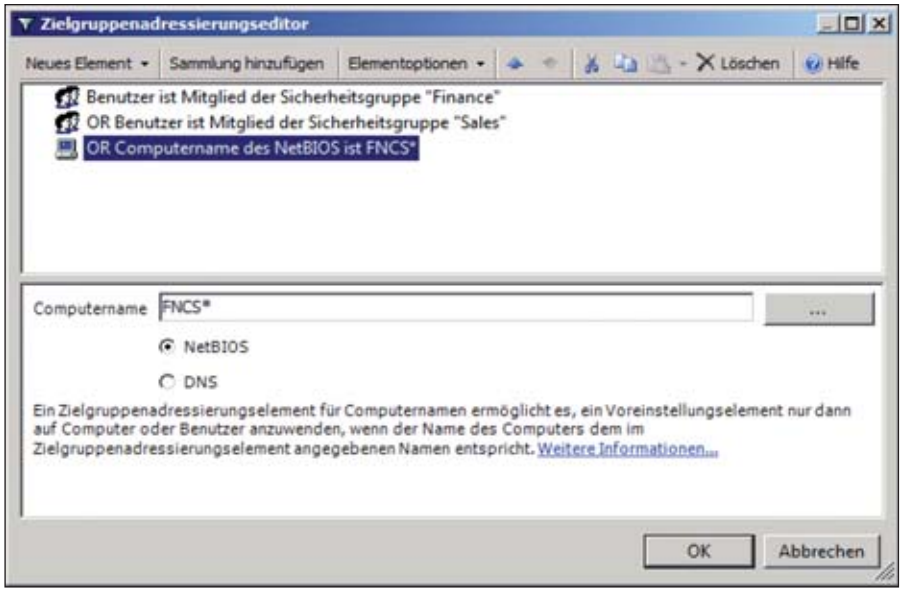


Bild 6: Einfach und komfortabel: Die Filterung auf Einstellungsebene ist mit das beliebteste Feature von GP-Preferences

Einfaches Rot/Grün-Farbsystem

Nicht alle GPP-Dialoge verhalten sich so wie die Laufwerkszuordnungen im vorherigen Beispiel. Eine Stärke der Preferences ist, dass die Administrationsoberfläche oft nahezu analog zum Benutzerinterface in Windows passt. Was Ihnen mit Sicherheit umgehend auffällt, sind rote Linien unter den möglichen Einstellungen, wie bei "Regionale Einstellungen". Diese Linien dienen als Visualisierung, die anzeigt, ob eine Einstellung von Zielclients übernommen werden soll oder nicht. Möchten Sie Einstellungen vom Client übernehmen, müssen Sie diese im Preference-Administrations-UI erst scharf schalten.

Neben der einfachen Änderung der Option im Dialog müssen Sie die Einstellung mit den Tasten F5 (ganzer Dialog) oder F6 (ausgewählte Einstellung) aktivieren. Die farbige Linie wechselt bei aktiven Einstellungen von rot nach grün. Umgekehrt ändert F7 die Einstellung als "für den Client inaktiv", F8 schaltet den ganzen Dialog inaktiv – die Farbe wechselt dann von grün nach rot. Nur Einstellungen, die grün und damit aktiv markiert wurden, werden tatsächlich von Zielclients übernommen und angewandt. Eine häufige Fehlermeldung in Supportgruppen und Foren ist, dass GP-Preferences manche Einstellungen nach der Änderung nicht übernahmen – wenn die Preference nach dem Schließen sofort wieder geöffnet wurde, waren die Anpassungen verschwunden. In der Tat speichert der Gruppenrichtlinieneditor nur die Einstellungen, die zuvor auch grün markiert wurden. Die Rot/Grün-Markierung hilft Ihnen, einzelne Einstellungen an Clients zu bestimmen, andere Einstellungen im Dialog unberührt zu lassen. Nur explizit selektierte Einstellungen sollen von Zielobjekten per Gruppenrichtlinien übernommen werden.

Hierarchie von Einstellungen und Richtlinien

Preferences sind eine gute Sache und zusammen mit Richtlinien bilden sie ein gutes Team. Jedoch gibt es bei der Verarbeitung von GPOs Stolpersteine, die Sie

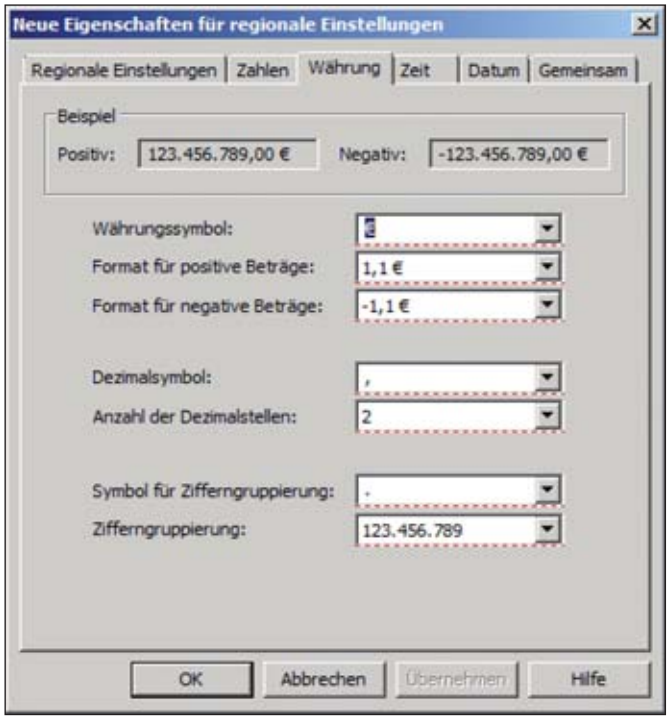


Bild 7: Rot unterstrichene Einstellungen werden nicht von den Clients übernommen

beachten sollten. Wenn Richtlinien und Preferences von Clients verarbeitet werden, gibt es keine Vorfahrtsregel.

Es gibt keine Daumenregel die besagt, ob nun Richtlinien oder Preferences Vorrang genießen. Bei der Richtlinienverarbeitung auf einem Client werden alle GPOs, die auf einen Client wirken, evaluiert. Dabei werden GPOs ohne passende Zugriffsberechtigungen und als "inkorrekt" evaluierte WMI-Filter ausgeschlossen. Die Restmenge der GPOs wird entsprechend angewandt. Jede Client Side Extension übernimmt den resultierenden Satz von Einstellungen am Client, nachdem sie die Reihenfolge der Richtlinien untereinander beachtet hat. Jede CSE schreibt also nacheinander die resultierenden Einstellungen ihrer konfigurierten GPOs in das System.

Nun ist die Aufrufreihenfolge der CSEs entscheidend, denn wie so häufig bei Gruppenrichtlinien gilt: Der als letztes Schreibende gewinnt die Einstellung. Die Aufruf-Reihenfolge der CSEs ist im System verankert und richtet sich nach den GUIDs der CSEs – den eindeutigen Kennungen, die auf allen Systemen gleich sind. Sehen Sie sich im Registry-Editor "regedit" im Schlüssel "HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows NT\CurrentVersion\Winlogon\GPExtensions" um, so finden Sie alle im System registrierten CSEs – der Reihenfolge ihrer GUIDs nach. Dies ist auch fast die Aufrufreihenfolge der CSEs, mit Ausnahme der Registry-CSE, die die Administrativen Vorlagen abarbeitet. Sie wird stets zuerst aufgerufen. Dieses Verhalten ist gerade interessant für "überlappende" Richtlinien und Preferences – etwa Administrative Vorlagen und die "Registrierung"-Preference. Schreiben beide auf einen Registrierungsschlüssel mit unterschiedlichen Werten, gewinnt die Preference, weil ihre Preference-CSE deutlich später aufgerufen wird als das Registrierungs-CSE der Administrativen Vorlagen.

Fazit

Auch in Windows Server 2008 und R2, sowie mit den Clientversionen Windows Vista und Windows 7 wurde die Anzahl der verfügbaren Gruppenrichtlinieneinstellungen nochmals erhöht. Nicht zuletzt durch die Einführung der GP-Preferences lässt sich die Skriptarbeit – bei richtiger Verwendung – stark reduzieren. Um bei der GPO-Definition erfolgreich zu sein, sollte der GP-Adminrechner stets mit einer aktuellen Version von Windows bestückt sein, dann stehen neueste Gruppenrichtlinien, Preferences und ihre ADMX-Definitionen zur Verfügung. *(dr)*

[1] SysPro Software PolMan
http://sysprosoft.com/pol_summary.shtml

[2] Group Policy Settings Reference for Windows and Windows Server
www.microsoft.com/downloads/details.aspx?FamilyID=18c90c80-8b0a-4906-a4f5-ff24cc2030fb&displaylang=en

[3] Group Policy Search
http://gps.cloudapp.net/

[4] Group Policy Preferences CSE
http://blogs.msdn.com/spatdsg/archive/2008/03/17/group-policy-preferences-cse-for-download.aspx

Links

Best Practices Analyzer für das Active Directory

Auf dem richtigen Weg

Keine Implementierung des Active Directory gleicht einer anderen, da bereits die Anzahl der Benutzer, die Netzwerkbegebenheiten und die zusätzlich eingesetzten Applikationen ein Verzeichnis einzigartig machen. Umso schwieriger ist es, sich im Dschungel der Einstellungen zurechtzufinden und korrekte Konfigurationen von Spezialeinstellungen für Sonderfälle zu unterscheiden. Doch mit den "Best Practice Analyzers" lässt sich die Installation und Konfiguration des Active Directory überprüfen und mit empfohlenen Einstellungen vergleichen.

Seit September 2004 liefert Microsoft für einige ihrer Produkte sogenannte "Best Practice Analyzer" (BPA) aus – Analyseprogramme, die die Installation und Konfiguration der Produkte aus Redmond überprüfen und anschließend mit empfohlenen Einstellungen des Herstellers abgleichen. Heraus kommt ein Bericht, der Administratoren über nicht empfohlene Konfigurationen, Probleme und mögliche Schwachstellen im Betrieb informiert. Zunächst nur für Exchange erhältlich, entwickelte Microsoft weitere BPAs für Sharepoint, SQL und Forefront, und schließlich mit Windows Server 2008 R2 auch einen Analyzer für das Active Directory (AD). Der sogenannte AD BPA scannt einige, aber leider nicht alle AD-verwandten Rollen auf einem Server 2008 R2. Zu den überprüften Diensten zählen die Active Directory Domain Services (das AD selbst), Active Directory-Zertifikatsdienste, Active Directory Rights Management Services (AD RMS) und DNS. Als Administrator bedienen Sie AD BPA entweder über den Servermanager oder über die PowerShell. Der Aufruf der Funktionen erfolgt dabei ausschließlich von Windows 7 mit installiertem RSAT oder von einem R2 Server. Server Core-Varianten von Server 2008 R2 können nur per PowerShell angestoßen werden, da sie keinen Servermanager besitzen.

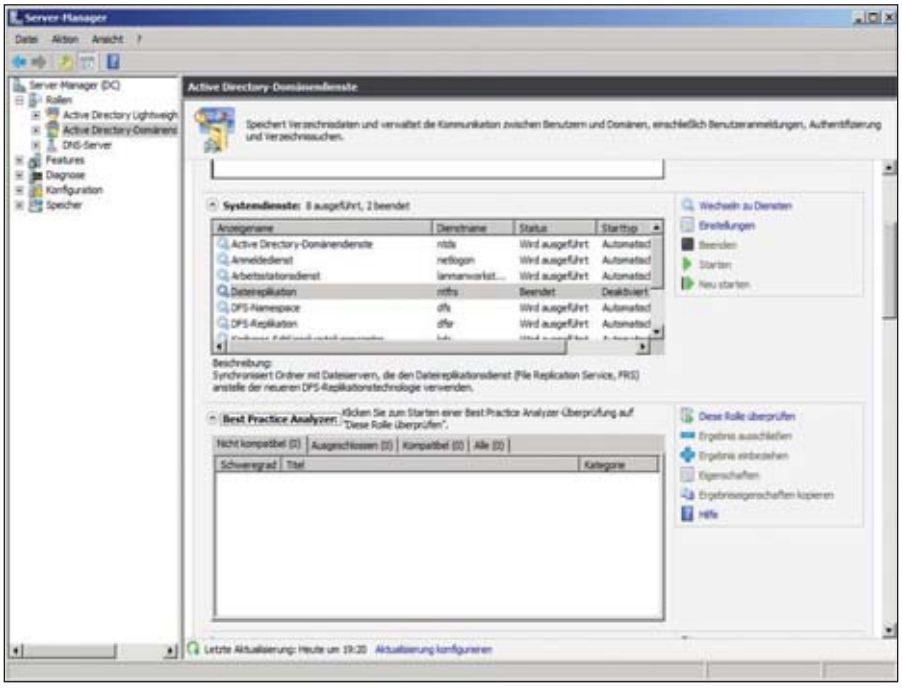


Bild 1: Analysen des AD-BPA werden im Servermanager angestoßen und aufgerufen

Die Analyse starten

Im Server Manager finden Sie den BPA im Knoten "Rollen / Active Directory Domänendienste". Dort angelangt, zeigt sich der Best Practice Analyzer als drittes Element im Abschnitt "Zusammenfassung" unter "Ereignisse" und "Systemdienste". Haben Sie bereits eine Analyse mit dem BPA durchgeführt, sehen Sie dort das letzte Ergebnis. Ansonsten ist das Fenster leer. Der BPA für den DNS-Dienst und die Zertifikatsdienste befindet sich im Server Manager an einer ähnlichen Stelle – anstatt des Knotens "Active Directory-Domänendienste" wird er über die Rollen "DNS-Server" und "Active Directory-Zertifikatsdienste" aufgerufen.

Mit dem Aktionspunkt "Diese Rolle überprüfen" startet der BPA seine Analyse – es sind keine weiteren Eingaben notwendig. Nach kurzer Zeit wird Ihnen das Ergebnis in insgesamt vier Reitern ausgegeben. Der Analyzer gliedert seine Funde dabei in drei Kategorien: "Nicht kompatibel", "Ausgeschlossen" und "Kompatibel" – der vierte Reiter stellt eine Übersicht über alle geprüften Punkte dar.

Als "Kompatibel" kennzeichnet AD-BPA Prüfpunkte, die mit Empfehlungen von Microsoft und deren Best Practices übereinstimmen. "Nicht kompatibel" sind

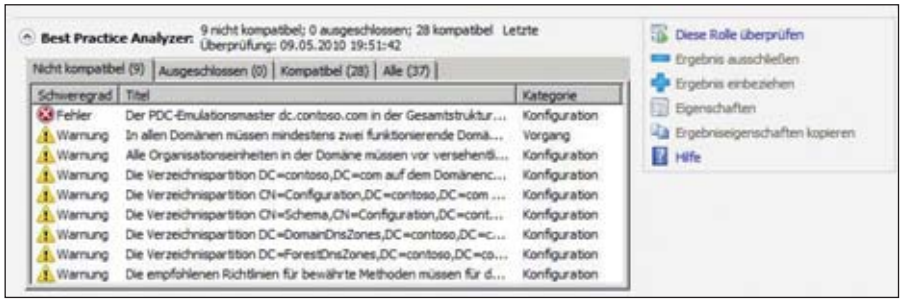


Bild 2: Im Analyseergebnis werden kompatible und nicht kompatible Ergebnisse herausgearbeitet

Punkte, die von empfohlenen Einstellungen und Konfigurationen abweichen. Hierbei wird zwischen Warnungen und Fehlern unterschieden. Fehler sind Prüfpunkte, die momentan ein Fehlverhalten auslösen oder eine Fehlkonfiguration darstellen. Sie sollten möglichst bereinigt werden, um den korrekten Betrieb des Verzeichnisses zu gewährleisten. Ein beispielhafter Fehler ist die Falschkonfiguration der Zeit, die der BPA mit folgender Meldung quittiert: "Der PDC-Emulationsmaster {Name} in der Gesamtstruktur muss so konfiguriert werden, dass die Zeit von einer gültigen Zeitquelle richtig synchronisiert wird". In der Tat hängt die Zeit der Gesamtstruktur vom PDC-Emulator-DC der Forest-Root-Domäne ab, da die Zeit von ihm ausgehend durch alle Domänen propagiert wird. Entsteht eine Zeitdifferenz in der Domäne, scheitert die Kerberos-Authentifizierung von Benutzern, Computern und Domänencontrollern – und legt damit die Arbeit der Mitarbeiter lahm.

Warnungen sollen auf Einstellungen aufmerksam machen, die zwar von Empfehlungen aus Redmond abweichen, jedoch keine merkliche Beeinträchtigung des Verzeichnisses bedeuten. Eine typische Warnung ist die Meldung: "In allen Domänen müssen mindestens zwei funktionierende Domänencontroller für die Redundanz vorhanden sein". Dies ist notwendig, um beim Ausfall eines DCs den Regelbetrieb fortführen zu können. Das Active Directory funktioniert auch mit einem DC pro Domäne. Fällt dieser eine DC jedoch aus, stehen Benutzern und Computern keine Anmelde-DCs zur Verfügung, es werden keine Tickets für das Kontaktieren von Servern ausgestellt und der Zugriff auf Daten und Dienste scheitert. Einen Domänencontroller in einer Domäne zu haben ist kein Fehler – allerdings ein unnötiges Risiko, von dem Microsoft mit einer "Warnung" in der Kategorie "Nicht Kompatibel" abrät.

Zu jedem Prüfpunkt bietet der Best Practice Analyzer weiterführende Informationen an. Sie erreichen die zugehörige Eigenschaftenseite entweder über den gleichnamigen Aktionspunkt oder per Doppelklick. Für "Nicht Kompatibel"-Punkte ist die Eigenschaftenseite immer ähnlich gegliedert. Voran steht die Beschreibung des Problems, gefolgt von einer kurzen Zusammenfassung der möglichen Auswirkungen und einem Lösungsvorschlag. Halten Sie sich bewusst nicht an eine der vom BPA evaluierten Best Practices, etwa weil die eigene Infrastruktur von der Musterlösung aus Redmond abweicht oder Sie einige Punkte erst später umsetzen möchten, können Sie Prüfpunkte von der Analyse ausschließen. Der zugehörige Knopf "Ergebnis ausschließen" verschiebt den markierten Prüfpunkt in den Reiter "Ausgeschlossen", wonach der BPA diesen Punkt auch bei neu durchgeführten Analysen nicht mehr berücksichtigt.

Weil sich Empfehlungen zu Produkten von Zeit zu Zeit ändern, hat Microsoft seinem BPA eine Update-Funktion spendiert. Über das bekannte Windows-Update wird der BPA ständig mit neuen Prüfpunkten oder verbesserten Hilfetexten aus Redmond versorgt. Die Planung sieht vor, dass hierfür halbjährlich Aktualisierungen veröffentlicht werden, die Administratoren entweder direkt per "Windows-Update" oder per Windows Server Update Services (WSUS) gezielt verteilen können.

Optimierung mit der PowerShell

So wie es Microsoft mit vielen seiner Verwaltungswerkzeugen in neueren Versionen hält, so hält die PowerShell auch beim Best Practice Analyzer für das AD Einzug. Ganz im Stile der Exchange-Verwaltungstools und des ADAC basiert der Unterbau des BPAs komplett auf der PowerShell. Die im Servermanager implementierte Funktionalität nimmt Benutzereingaben entgegen und ruft anschließend, im Hintergrund verborgen, PowerShell-Kommandos auf, die dann vom System verarbeitet werden. Kein Wunder, dass sich die BPA-Funktionalität ebenso gut losgelöst vom Server Manager direkt per PowerShell-Skript ausführen und für periodische Berichte nutzen lässt. Hierzu benötigen Sie nur bedingt Skriptkenntnisse – die Syntax des BPAs ist einfach verständlich und nicht schwer mit einem Skript zu erledigen.

Zuerst binden Sie die BPA-Funktionalität in die aktuelle PowerShell-Session per

Bild 3: Zu jedem BPA-Prüfpunkt werden weiterführende Informationen zur Verfügung gestellt, die die Lösung des Problems unterstützen

```
Auswählen Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\Administrator> Import-Module BestPractices
PS C:\Users\Administrator> Get-BPAModel

Id                                          LastScanTime
--                                          ------------
Microsoft/Windows/DirectoryServices         13.05.2010 16:59:59
Microsoft/Windows/DNSServer                 Nie

PS C:\Users\Administrator> Invoke-BPAModel Microsoft/Windows/DirectoryServices

ModelId                          Success Detail
-------                          ------- ------
Microsoft/Windows/DirectoryServices True    {InvokeBpaModelOutputDetail}
```

Bild 4: Der BPA lässt sich auch vollständig über die PowerShell bedienen

Importmodul "BestPractices" ein. Danach ist der BPA-Namespace verfügbar, so dass diePowerShell die zugehörigen Kommandos erkennt. Mit *Get-BPAModel* weisen Sie die Shell an, alle bekannten BPA-Prüfungen anzuzeigen. Die folgende Ausgabe umfasst alle Produkte, deren Rolle auf dem Server installiert ist und für die es einen BPA gibt. Dies beinhaltet auch die sogenannte "ID", die Kennung, unter der ein BPA in der PowerShell zur Verfügung steht, sowie den Zeitpunkt des zuletzt durchgeführten Scans.

Die ID ist es auch, die wir im Folgenden für die Durchführung der Analyse und das Abrufen der Ergebnisse verwenden. Das Starten einer neuen Analyse erfolgt mit dem Befehl *Invoke-BPAModel* gefolgt von der BPA-ID des gewünschten Analyzers:

```
Invoke-BPAModel Microsoft/Windows/
  DirectoryServices
```

Die Ausgabe zeigt in der Spalte "Success", ob die Ausführung erfolgreich war. Das Ergebnis wird aber noch nicht angezeigt. Hierfür kommt ein weiterer Befehl zum Einsatz: *Get-BPAResult*. Dieses Kommando erhält als Parameter erneut die BPA-ID und ruft das Ergebnis des zuletzt durchgeführten Scans ab. Beim Aufruf dieses Kommandos wird die gesamte Ergebnisliste auf der Kommandozeile ausgegeben:

```
Get-BPAResult Microsoft/Windows/
  DirectoryServices
```

Damit lässt sich jedoch nicht sehr viel anfangen. Um den Report lesbar ablegen zu können, kennt die PowerShell mehrere Funktionen, um Ergebnisse in andere Formate zu konvertieren und sie anschließend in Dateien zu schreiben:

```
Get-BPAResult Microsoft/Windows/
  DirectoryServices | ConvertTo-Html
  | set-content report.html
```

Als Alternative zu HTML kann die PowerShell das Ergebnis auch in eine CSV-Datei packen:

```
Get-BPAResult Microsoft/Windows/
  DirectoryServices | ConvertTo-CSV
  | set-content report.csv
```

In diesen Beispielen nutzen wir die Pipe-Funktion der Shell, die, nachdem Befehl für Befehl korrekt abgearbeitet wurde, das Ergebnis des ersten Befehls im darauffolgenden Befehl weiterverarbeitet. Das Kommando ruft zunächst die Resultatsliste des letzten BPA-Scans ab, die die Shell anschließend in HTML oder CSV konvertiert. Im letzten Abschnitt des Befehls schreibt die PowerShell die aufbereiteten Daten in eine Datei. Die fertige CSV-Datei können Sie dann mit einem beliebigen Werkzeug öffnen und ansehen. In unserem Beispiel verwenden wir Microsoft Excel, das per Auto-Filter-Funktion einen schönen Überblick über die Prüfpunkt-Kategorien gibt und den Benutzer nach gewünschten Kriterien filtern lässt.

Sind tatsächlich nur "Warnungen" und "Fehler" vom BPA-Bericht interessant, können Sie auch nur diese Prüfpunkte gesondert in einen Bericht schreiben lassen. An den bereits genutzten Kommandos müssen Sie hierzu wenig verändern – lediglich eine Selektion der kritischen Punkte ist notwendig:

```
Get-BPAResult Microsoft/Windows/
  DirectoryServices | ?{$_.Severity
  -eq "Warnung" -or $_.Severity
  -eq "Fehler" } | ConvertTo-HTML |
  set-content report_critical.html
```

Nachdem die Liste der Ergebnisse abgerufen wurde, kann PowerShell nach den Kategorien "Warnung" und "Fehler" filtern – das Attribut hierzu heißt "Severity", das als PowerShell-Attribut für jeden Prüfpunkt im Report zur Verfügung steht. Anschließend wird die verkürzte Liste der kritischen Punkte erneut konvertiert und in eine HTML-Datei gespeichert. Für

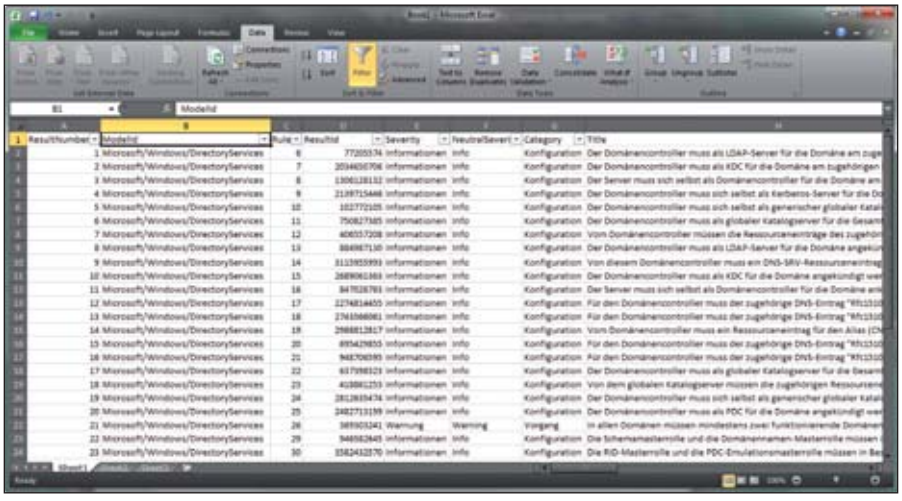


Bild 5: Richtig exportiert, können Administratoren die BPA-Reportdaten komfortabel verwenden und auswerten

englische Systeme sollten Sie die englischen Kategorien, "Warning" für "Warnung" und "Error" für "Fehler" verwenden. Das führt zu einem Skript, das per geplanten Task aufgerufen werden kann, um periodische Reports zu exportieren:

```
Import-Module BestPractices
$date = get-date -Format
  "ddMMyy_HHmmss"
Invoke-BPAModel Microsoft/Windows/
  DirectoryServices && Get-BPAResult
  Microsoft/Windows/
  DirectoryServices | ConvertTo-Html
  | set-content "C:\Reports\AD-BPA-
  Report_$date.html"
```

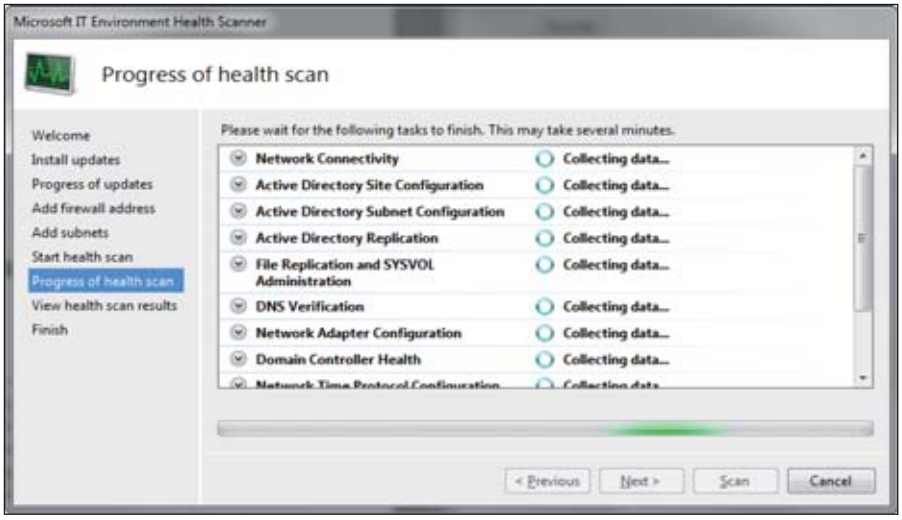


Bild 6: Administratoren sehen in der Scanübersicht, welche Punkte der Scanner erfolgreich oder mit Fehlern abgeschlossen hat

Gesunde Umgebung – gesunder Server

Ein weiteres, ebenso kostenfreies Werkzeug zur Messung der Gesundheit der Infrastruktur ist der "Microsoft IT Environment Health Scanner" [1]. Zielgruppen des Health Scanners sind Unternehmen mit weniger als 20 Servern oder bis zu 500 Clients. Das liegt deutlich unter dem, was Microsoft unter "Enterprise" versteht und fokussiert kleinere und mittelständische Unternehmen. In der Tat stammt das Tool vom Team, das den Essential Business Server (EBS) entwickelt hat – den großen Bruder des Small Business Server. Was den Health Scanner so interessant macht, ist die Anzahl und Art der Prüfungen, die er vornimmt. Anders als beim BPA, wird die DNS-Konfiguration der Infrastruktur sowie die Erreichbarkeit der installierten Dienste, etwa Exchange, überprüft. Die Replikation und die Konfiguration der Standorte sind ebenfalls ein Prüfthema. So warnt das Werkzeug, wenn in einem Standort kein Globaler Katalog existiert und gleichzeitig "Universal Group Membership Caching" deaktiviert ist. Diese Konstellation hat in Mehrdomänenumgebungen zur Folge, dass sich Mitglieder universeller Gruppen nicht an der Domäne anmelden können, bis ein GC verfügbar ist. Eine Prüfung, die der BPA nicht durchführt.

Der Health Scanner überprüft mehrere Aspekte, darunter die "Network Connectivity", "Active Directory Site Configuration", "Active Directory Replication", "File Replication and SYSVOL Administration" und "DNS Verification". Umfasst die Infrastruktur Exchange, führt der Scanner weitere Exchange-spezifische Prüfungen durch, um dessen Gesundheit zu überprüfen. Das Tool verfügt über eine assistentgestützte, grafische Oberfläche, die Benutzer Schritt für Schritt durch den Analysevorgang führt. Beim Start des Scanners wird zunächst ein Internet-Update des Programms durchgeführt. Anschließend wird der Administrator gebeten, die IP und Subnetzmaske der Firewall hinaus ins Internet und alle Subnetze des Netzwerkes anzugeben.

Haben Sie die Umgebung korrekt angegeben, kann der Scan starten. Der Health Scanner verlangt nach einem Benutzernamen und Passwort, mit dem die Checks durchgeführt werden können. Hier sollten Sie ein Benutzerkonto mit ausreichenden Berechtigungen in der Gesamtstruktur wählen. Das Tool verbindet sich mit Domänencontrollern und den in DNS gefundenen Servern und fragt per WMI Status- und Konfigurationsdaten ab – aus diesem Grund verlangt der Assistent ein administratives Konto mit ausreichender Berechtigung. Anschließend führt der Scanner die Analyse der Infrastruktur durch. Das Sammeln und Aufbereiten der Daten kann gut und gerne ein paar Minuten in Anspruch nehmen. Zehnminütige Scans sind keine Seltenheit.

Bricht der Assistent den Sammelvorgang schon nach wenigen Sekunden oder einzelnen Minuten ab, stimmt etwas mit der DNS-Konfiguration oder den Berechtigungen nicht, mit denen der Scanner arbeitet. Dann müssen Sie anhand der beschriebenen Fehlermeldung und der vorgeschlagenen Lösung erst noch einmal Hand anlegen.

Nach Abschluss der Überprüfung zeigt der Health Scanner seine Ergebnisse gesammelt im Abschnitt "View health scan results" an. Das Tool teilt die gescannten Punkte, ähnlich wie der AD BPA, in "Errors", "Warnings" und "Completed" ein. Zu den Warnungen und Fehlern können Sie eine KnowledgeBase-Artikel mit weiterführenden Informationen nutzen. Der Knopf "Open Large View" öffnet den im Hintergrund generierten HTML-Report des Scans, der, wenn auch in manueller Arbeit, zur Archivierung für spätere Reviews abgelegt werden kann. *(dr)*

[1] Microsoft IT Environment Health Scanner
www.microsoft.com/downloads/details.aspx?familyid=dd7a00df-1a5b-4fb6-a8a6-657a7968bd11&displaylang=en

Links

Quelle: s.dorn – Fotolia.com

Application-Performance im Active Directory steigern

Mehr Speed fürs Verzeichnis

Wenn Sie das Active Directory als Zentrum Ihrer Infrastruktur betreiben, sollten Sie für die Performance der Domänencontroller einige Feineinstellungen vornehmen. Obwohl der Verzeichnisdienst nach der Installation bereits reibungslos zu funktionieren scheint, kann es bei Last zu Leistungsproblemen kommen, die sich negativ auf umliegende Anwendungen, Dienste und Benutzeranmeldungen auswirken. Besonders kritisch dabei: suboptimale Suchanfragen. Dieser Workshop hilft Ihnen, das Active Directory mit höchster Leistung zu betreiben

Was bei Desktoprechnern, Laptops und Servern gilt, trifft im Speziellen auch für Domänencontroller (DC) zu: Je mehr Dienste ein DC neben seinen Domänentätigkeiten bereitstellt, desto schwieriger ist es, eine optimale Performance des Verzeichnisdienstes zu erlangen. Teilt sich das Active Directory (AD) die Resourcen mit anderen Diensten, folgen möglicherweise Engpässe beim Zugriff auf die Festplatten oder dem Zugriff auf den Arbeitsspeicher.

Das Ziel sollte demzufolge sein, die AD-Domänendienste möglichst dediziert ohne weiteren Anwendungen zu betreiben . Die Domänendienste sehen das AD sowie den DNS-Serverdienst vor, zusätzlich außerdem die Verwaltungskonsolen für die MMC. Diese zusätzlichen Dienste und Anwendungen an Bord machen es Administratoren schwer, die Performance des Systems zu bewerten und zu verbessern. Für eine Kapazitätsplanung der Server und Dienste im Unternehmen müssen die einzelnen Dienste gesondert betrachtet werden. Das Extrahieren der Arbeitsleistung eines Dienstes gestaltet sich jedoch schwierig, da zuerst die diensteigene Last auf dem Server gemessen, extrahiert, anschließend berechnet und wieder im Kontext mit den anderen auf dem Server befindlichen Diensten betrachtet werden muss. Da im Regelfall alle Dienstanforderungen beim Wachstum der Infrastruktur steigen, darf beispielsweise nicht nur das Active Directory betrachtet werden, wenn zusätzliche Dienste installiert wurden. Zwar lässt sich die AD-eigenen Ressourcenutzung durch Auswerten von Performancemonitoren herauslesen, die Planung für die weitere Zukunft ist aber mit dem Wachstum der verbleibenden Dienste auf dem Domänencontroller zu betrachten.

Stehen Performanceprobleme bereits ins Haus, beginnt beim Betrieb von vielen Diensten die Suche nach dem verantwortlichen Bösewicht. Wenn der Schuldige nicht gerade ein offensichtliches Speicherleck verursacht, das anderen Anwendungen die Luft zum Atmen nimmt, sondern das Problem schleichend oder gar sporadisch auftritt, wird die Fehlersuche umfangreicher. Das Problem kann durch einen, mehrere oder alle Dienste hervorgerufen werden, sollte die Gesamtlast über eine merkliche Schwelle gewachsen sein. Mit jedem Dienst wächst die Zahl der potenziellen Fehlerquellen.

Hardware richtig planen

Die Datenbank des Active Directory besteht, wie ihre Schwestern unter anderem bei Exchange und der Windows-Suche, aus einer Datenbankdatei und sogenannten Transaktionslogs. Bevor Änderungen am Verzeichnis in der Datenbank landen, werden sie in die Transaktionslogs übernommen und erst dann gesammelt in die Datenbank geschrieben.

Der Datendurchsatz bei einer hohen Schreiblast im AD lässt sich steigern, wenn das Betriebssystem, die Datenbank und die Logdaten auf unterschiedlichen Festplatten platziert werden. Mit dieser Maßnahme werden Festplattenzugriffe auf unterschiedliche Datenträger verteilt. Die Wartung des Betriebssystems kann somit unabhängig vom Betrieb des AD stattfinden – und unter AD-Last lässt sich das Betriebssystem weiterhin verwenden. Anzustreben sind aus diesem Grund drei Festplatten, die jeweils entweder das Betriebssystem, die AD-Datenbank oder das Transaktionslog beheimaten.

Die Verteilung der Transaktionslogs und der AD-Datenbank wählen Sie während

des Heraufstufens zum Domänencontroller. Im Installationsassistenten DCPromo können Sie den Ort beliebig wählen. Um die Lage der Datenbank und der Logfiles nachträglich zu ändern, bietet sich das Werkzeug NTDSUtil an. Bei Domänencontrollern vor Windows Server 2008 müssen Sie den DC hierfür im "Verzeichnisdienst-Wiederherstellungsmodus" starten. Ab Server 2008 reicht ein einfaches Stoppen des AD DS-Dienstes. In Server 2008 und 2008 R2 müssen Sie außerdem noch im gestarteten NTDSUtil mit *active instance ntds* die aktuelle Verzeichnisdienst-Instanz auswählen. Anschließend – von nun an verhält sich die Vorgehensweise bei allen Betriebssystemversionen identisch – wechseln Sie per Kommando *files* in den "File Maintenance"-Kontext. Die beiden Befehle *move db to {location}*und *move logs to {location}* führen nun die gewünschten Operationen durch. Mit dem Befehl *info* zeigen Sie die aktuelle Konfiguration an. Danach folgt ein abschließender Neustart des Dienstes oder des Domänencontrollers.

Domänencontroller finden

Um effizient mit dem AD arbeiten zu können – sei es bei der Authentifizierung oder mit AD-kompatiblen Anwendungen – muss das Auffinden von Domänencontrollern schnell und reibungslos möglich sein. Clients finden DCs über den sogenannten DC-Locator-Prozess. Dieser sucht anhand des Heimatstandorts des Clients im DNS-Dienst nach DCs, die den benötigten Dienst bereitstellen. Die korrekte Konfiguration von DNS ist somit eine feste Voraussetzung.

Domänencontroller erstellen beim Start des Netlogon-Dienstes und in zyklischen Abständen während des Betriebes Diensteinträge, sogenannte Service-Records (SRV-Records) in DNS. Für jeden Dienst, den ein DC bereitstellt, erstellt er einen Eintrag in DNS, angefangen im DNS-Zweig seines eigenen Standortes. Nach diesen Diensteinträgen, das sind Einträge für Dienste wie Kerberos-Anmeldung, LDAP oder den globalen Katalog, können Clients per DC-Locator-Prozess suchen und sich eine Liste aller Dienste in einem Standort anzeigen. Ein Client, der einen DC für die Authentifizierung benötigt, erstellt eine DNS-Abfrage nach seinem Standort und dem benötigten SRV-Record und wählt so einen Domänencontroller aus den von DNS zurückgelieferten Ergebnissen aus. Diese SRV-Records sind es, nach denen der DC-Locator-Prozess sucht.

Nun gibt es Standorte, die keine eigenen DC besitzen. Aus der Beschreibung geht hervor, dass DCs SRV-Records für ihre eigenen Standorte erstellen. Wie kommen jedoch die Clients an einem Standort ohne DC zu ihrer Anmeldung? Die Antwort liegt im "automatic site coverage". Alle DCs prüfen, ob es DC-lose Standorte gibt. Das können sie, weil die Konfigurationsdaten aus "Active Directory-Standorte und -Dienste" in der Konfigurationspartition hinterlegt ist, die auf alle DCs der Gesamtstruktur repliziert wird. Jeder DC prüft anhand der Site Link-Kosten, ob sein eigener Standort die beste Verbindung zum DC-losen Standort hat. Ist die Prüfung positiv, registriert der DC seine SRV-Records auch für den DC-losen Standort, so dass er und folglich alle weiteren DCs im gleichen Standort Anfragen aus dem Standort ohne DC beantworten können. Domänencontroller aus benachbarten Standorten mit den geringsten Verbindungskosten bieten ihre Dienste in Standorten ohne DC an.

Anwendungen mit Active Directory-Zugriff optimieren

Trotz aller Vorkehrungen beim Aufsetzen von Domänencontrollern kann es zu Problemen im Domänenbetrieb kommen. Etwa dann, wenn Anwendungen mehrfach in großem Stil auf das AD zugreifen, um Daten auszulesen oder zu schreiben. Lesend können Applikation über LDAP Zugriff erlangen. LDAP ist das Light-weight Directory Access Protocol, mit dem sich standardisierte Suchen in einem Verzeichnisbaum realisieren lassen. Auf jedem Domänencontroller wird ein LDAP-kompatibler Serverdienst ausgeführt, der Suchanfragen auf dem Standardport 389 entgegen nimmt. Gibt der LDAP-Client keinen bestimmten Server an, wird über den DC-Locator-Prozess, den Prozess, der beim Rechnerstart den am nächsten liegenden Domänencontroller für die Authentifizierung findet, ein DC für die Suchanfrage bestimmt. LDAP-Suchen in einem Verzeichnis sind nach einem bestimmten Muster aufgebaut und bedingen einen Satz an Informationen, um korrekte Sucherergebnisse zu finden:

- Startknoten: Der LDAP-Server muss wissen, in welchem Knoten im Verzeichnisbaum die Suche beginnen soll. Hier können Objekte, Container, Organisationseinheiten, einzelne Verzeichnispartition oder das gesamte Verzeichnis durchsucht werden. Für die Organisationseinheit "Sales" in der Domäne "contoso.com" ergibt sich

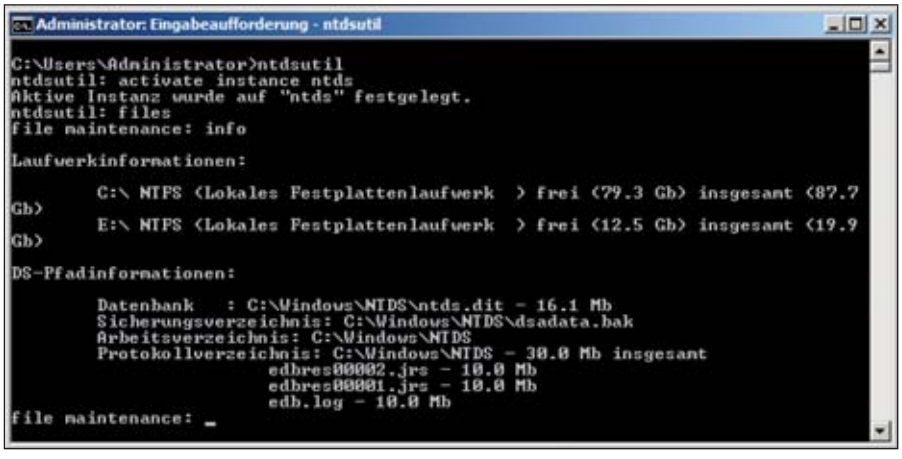


Bild 1: Per NTDSUtil können Logs sowie die Datenbank des AD nachträglich verschoben werden

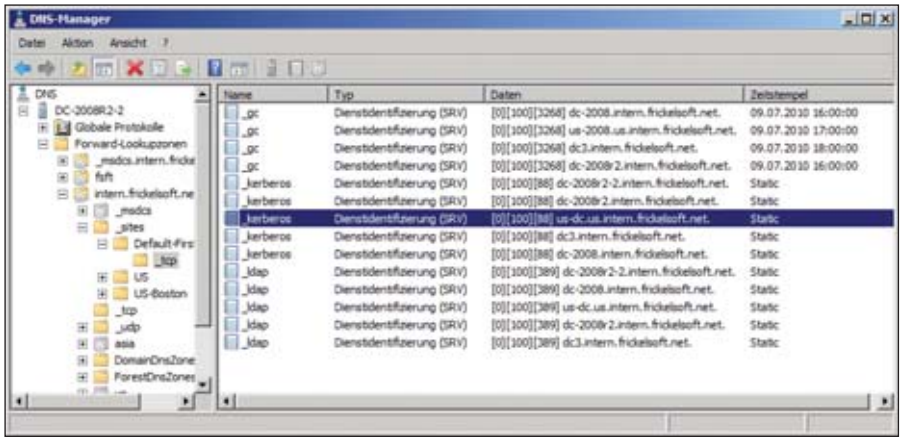


Bild 2: Das DNS-MMC-Snap-in zeigt die SRV-Records, die Domänencontroller für ihre Standorte registrieren

folgender Startknoten in LDAP-Schreibweise: "OU=Sales,DC=contoso, DC=com".

- Suchweite: Um die Suche einschränken zu können und den DC nicht die gesamte Datenbank durchwühlen zu lassen, können Sie die Suchweite auch begrenzen. Zur Verfügung stehen die Einstellungen "base", die nur den angegebenen Startknoten durchsucht, "OneLevel", die nur den Startknoten und alle Kindsobjekte des Startknoten im Verzeichnisbaum einschließt und "Subtree", die Suche im ganzen unter dem Startknoten liegenden Verzeichnisabschnitt.
- Suchfilter: Im Suchfilter wird der eigentliche Ergebnissatz, den der DCs anhand der Suchweite und des Startknotens findet, noch weiter eingeschränkt. Gefiltert werden kann nach nahezu allen Attributen des AD. Die zu suchenden Attribute werden dabei mit logischen Operatoren verknüpft. Folgendes Beispiel sucht nach Usern, deren Vorname mit der Zeichenkette "Mu" beginnt: *(& (objectClass=user) (objectCategory=person) (given-Name=Mu*))*

Eine nähere Anleitung zur Erstellung von LDAP-Abfragen und dem Aufbau von Filtern finden Sie unter [2].

Zu Performanceproblemen mit Suchen kann es kommen, wenn Anwendungen Suchen mit vielen Ergebnissen starten oder Filter definieren, die zwar eine geringe Anzahl an Sucherergebnissen liefert, das AD aber viele Objekte besuchen und evaluieren muss. In beiden Fällen muss das Active Directory sehr große Teile der Datenbank durchsuchen. Das führt dazu, dass zunächst die Suchzeiten in die Höhe schnellen und gleichzeitig Festplattenaktivität erzeugt wird. In Fällen, in denen das Active Directory viele Objekte in der Datenbank durchkämmen muss, ist von "teuren" Suchen die Rede, in Fällen in denen viele Objekte bei wenigen Suchergebnissen besucht werden müssen, von "ineffizienten" Suchen. Bei vereinzeltem Auftreten fallen schlecht geformte Suchen meist nicht weiter ins Gewicht. Suchen Anwendungen und Dienste in größerer Zahl sehr ineffizient oder teuer nach Objekten, kann das die Performance des Verzeichnisses und der Anwendungen selbst beeinflussen.

Performance von LDAP-Suchen messen

Um festzustellen, ob eine Anwendung aufgrund schlecht geformter LDAP-Suchen Performanceprobleme verursacht oder um eine selbstentwickelte Applikation auf Geschwindigkeit zu prüfen, können Sie DCs zur Protokollierung von LDAP-Suchen und deren Effizienz konfigurieren. Die Einstellung ist nicht in der grafischen Oberfläche implementiert und muss in der Registry vorgenommen werden. Der Schlüssel "HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics" zeigt verfügbare Diagnosen, die Sie auf DCs aktivieren können. Die Protokolle werden dann, abhängig von der Stufe der Protokollierung in die Ereignisanzeige "Verzeichnisdienst" geschrieben.

Die Diagnose-Registrierungsschlüssel kennen sechs Stufen, wobei 0 für "kein Protokollieren" und 5 für "exzessives Protokollieren" steht. Die Stufen 4 und 5 sollten Sie generell nur für kurze Diagnosen verwenden, um konkrete Probleme zu lösen. Die beiden Stufen protokollieren in einigen Diagnosen sehr viele Aktionen, was die Performance von Domänencontrollern stark beeinflussen kann. Die Diagnose "15 Field Engineering" protokolliert unter anderem mit, ob ineffiziente oder teure Suchanfragen an den Domänencontroller gestellt wurden. Sie können den Wert von "15 Field Engineering" auf 4 setzen, um beim zyklischen Aufruf des Garbage Collectors alle zwölf Stunden einen Report über die gesammelten, schlecht geformten Abfragen zu erhalten. Das Ereignis trägt die EventID 1643.

In Level 5 protokollieren DCs ineffiziente und teure Suchen direkt bei Auftreten. Zyklische Reports werden weiterhin unter der ID 1643 erstellt. Suchen Anwendungen jedoch mit schlecht geformten Abfragen im Verzeichnis, protokollieren Domänencontroller dies mit der EventID 1644. Zu beachten gilt, dass Sie die Registrierungsschlüssel auf allen DCs aktivieren müssen, für diese Aktivierung aber kein Neustart erforderlich ist. Eine einfache Variante, den Schlüssel auf allen DCs zu verteilen, ist der Einsatz einer Gruppenrichtlinie an der "Domain Controllers"-Organisationseinheit.

Doch mit der Konfiguration der Diagnose allein werden Administratoren kleinerer Umgebungen kaum glücklich. Das AD protokolliert nur Suchanfragen, die es selbst für teuer oder ineffizient hält. Per Voreinstellung kategorisiert das AD Suchen nur dann als teuer, wenn mehr als 10.000 Objekte durchsucht werden mussten. Ineffizient ist eine Suche, wenn die

Trefferquote, das Verhältnis zwischen allen besuchten Objekten und den in den Ergebnissatz aufgenommenen, unter zehn Prozent liegt.

Die Vorgaben lassen sich mit weiteren Registrierungsschlüsseln steuern. In "HKLM\SYSTEM\CurentControlSet\ Services\NTDS\Parameters" können Sie die beiden Schlüssel "Expensive Search Results" und "Inefficient Search Results" als DWORDs anlegen, falls diese noch nicht existieren. Um alle Suchen in die Ereignisanzeige protokollieren zu lassen, können Sie beide Schlüssel mit einem sehr niedrigen Wert konfigurieren, so dass alle Anfragen "durchfallen". Die Konfiguration beider Schlüssel mit dem Werte von jeweils "1" sollte ausreichen. Diese Verwendung dieser Einstellung kann aber zu merkbarer Last auf den DCs führen und sollte nur in Fällen der Fehlersuche einsetzt werden.

Für das Messen und Bewerten eigener Applikationen bietet sich ein einfacherer Weg an. Ist der Quelltext bekannt, können Sie geplante LDAP-Suchen extrahieren und gezielt vorab auf ihre Performanz prüfen. Der im Active Directory implementierte LDAP-Server kann mit sogenannten Controls dazu gebracht werden, die Suche mit Sondereinstellungen durchzuführen. Somit lassen sich gelöschte Objekte in die Suchergebnisse einbeziehen. Eines der verfügbaren Controls weist das Active Directory an, die Suchstatistik mitzuschreiben und neben den Suchergebnissen darzulegen.

Mit LDP, das seit Windows Server 2008 nicht mehr über die Supporttools, sondern direkt mit Windows ausgeliefert wird, können Sie Adhoc-Suchen im Verzeichnis durchführen. Nach dem Start führen Sie zunächst per "Verbinden" und "Gebunden" die Verbindung und Authentifizierung am Verzeichnis durch. Im Menü "Optionen" befinden sich unter "Steuerelemente" alle verfügbaren Controls. Hier wählen Sie das Steuerelement "Search Stats"aus und laden es, um die Suchstatistik zu aktivieren. Anschließend rufen Sie über das Menü "Durchsuchen" den Dialog "Suchen" auf. Dieser verlangt bereits die genannten, für die Suche erforderlichen Informationen. Zusätzlich lassen sich die Attribute definieren, die für die Suchergebnisse zurückgeliefert werden sollen. Bevor Sie die Suche starten können, sollten Sie über den Button "Optionen" den Aufruftyp auf "Erweitert" festlegen – nur durch diese Auswahl wird das LDAP-Control für die Suchstatistik ausgewählt. Wenn die Suche anschließend gestartet wird, zeigt LDP recht interessante Suchstatistiken an.

Lange Suchen optimieren

Nur selten befindet sich der Administrator im glücklichen Umstand, den Quelltext der Applikation zu besitzen oder die Entwickler zu einer Änderung des Programms bewegen zu können. Stellen Applikationen suboptimale Anfragen an das Verzeichnis, ist die IT-Abteilung dem oft hilflos ausgeliefert. In einem solchen Fall kann es sinnvoll sein, sich die suboptimale Anfrage genauer anzusehen. So lässt sich möglicherweise zumindest die Datenbasis an das Programm angleichen. Als Datenbanksystem verfügt das Active Directory über eine Indexfunktion, die Indizes über konfigurierte Attribute anlegt. Stößt der Verzeichnisdienst bei einer Suchanfrage auf eines der konfigurierten Attribute, wird es anstelle aller Objekte den angelegten Attribut-Index durchsuchen und somit den deutlichen kürzen Weg zu seinen Suchergebnissen nehmen. Von Haus aus werden einige wichtige Attribute, die sowohl vom System als auch von anderen Anwendungen genutzt werden, in Indizes gespeichert.

Indizes über Attribute werden als eigene Tabellen in der Active Directory-Datenbank realisiert. Das AD analysiert die Suchfilter und entscheidet, welches der im Filter verwendeten Attribute die Suche am besten einschränkt. Besitzt eines der Attribute einen eigenen Attributindex, wird die Indextabelle für die Suche verwendet – sie schränkt die potentiellen Suchergebnisse deutlich ein. Die Liste der Attribute, für die das AD bereits einen Index vorhält, finden Sie mit einer LDAP-Abfrage heraus:

```
(&(objectCategory=attributeSchema)
  (search-Flags:1.2.840.113556.1.4.
  803:=1))
```

Zu beachten ist allerdings, dass für diese Abfrage nicht die Domänenpartition als Startzweig ausgewählt werden darf, sondern die Schemapartition: "CN=Schema,CN=Configuration,DC=contoso,DC=com". LDP gibt, wie im vorherigen Beispiel, die zu dieser Suche beste Auskunft. Bei näherer Betrachtung des Suchfilters fällt auf, dass nach einem Attribut namens "searchFlags" gesucht wird, das unter Verwendung eines Operators den Wert 1 erhalten soll. Das Attribut ist eine Bitmaske, in der jedes Bit eine AD-Funktion ein- oder ausschaltet. Der Operator "1.2.840.113556.1.4.803" bildet hierbei das logische UND, das dazu verwendet wird, den Status der Bits in searchFlags zu prüfen. Da das erste Bit 0 bei "nicht gesetzt" und 1 bei "gesetzt" trägt, wird mit dem Wert "1" gefiltert. Die einzelnen Bits und ihre Funktionen sind in [4] beschrieben.

Befindet sich ein für Anwendungen wichtiges Attribut nicht im Index, kann ein Aufnehmen in den Index die Abfragedauer verkürzen. Das Aufnehmen von Attributen geschieht dabei ähnlich wie die Abfrage: über das Setzen des ersten Bits des searchFlags-Attributes. Hierzu bietet sich das Schema-MMC-Snap-In an, das Sie nach einer Neuinstallation von Windows Server erst registriert müssen. Über die Datei *regsvr32 schmmgmt.dll* schalten Sie das Snap-In frei und fügen es in der MMC als "Active Directory-Schema" hinzu. Im geöffneten Zustand zeigt das Snap-In zwei Knoten: Klassen und Attribute. Die Auswahl von "Attribute" öffnet in der rechten Spalte eine Übersicht aller Attribute des Verzeichnisses. In den Eigenschaften des gesuchten Attributes befindet sich dann die Option "Dieses Attribut indizieren", die

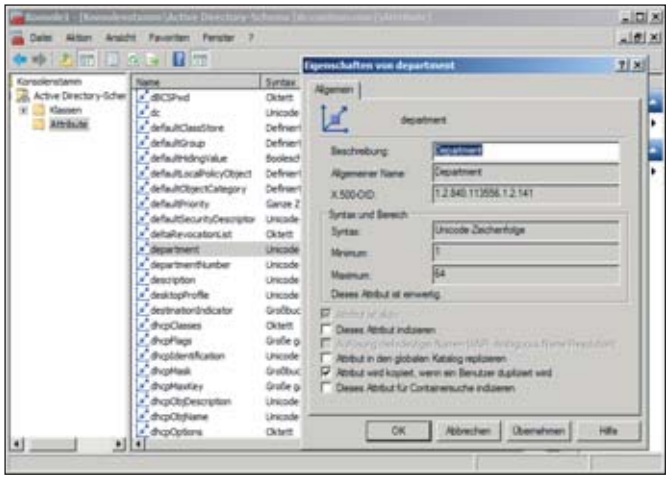


Bild 3: LDP liefert auf Wunsch nützliche Informationen bei der Optimierung von LDAP-Suchanfragen

beim Aktivieren oder Deaktivieren das entsprechende Bit im searchFlags-Attribut setzt.

Neben "Dieses Attribut indizieren" finden Sie noch weitere Optionen, die sonst in der searchFlags-Bitmaske gespeichert werden. Die Einstellung "Attribut in den globalen Katalog replizieren" bestimmt, ob ein Attribut für domänenübergreifende Suchen mit Globalen Katalogen verfügbar sein soll. "Attribut wird kopiert, wenn ein Benutzer dupliziert wird" weist das Snap-In "Active Directory-Benutzer und -Computer" an, beim Kopieren eines Objektes dieses Attribut mit zu berücksichtigen.

Domänenübergreifendes suchen

In Infrastrukturen mit mehreren Domänen im AD-Forest kommt eine weitere Komponente des Active Directory zum Zug, die für Suchen eingesetzt wird: der Globale Katalog. In dieser Rolle besitzt ein DC neben seiner eigenen, schreibbaren Domänenpartition auch eine Nur-Lesen-Kopie jeder anderen Domänenpartition der Gesamtstruktur.

So ist der Domänencontroller mit Globalem Katalog in der Lage, Suchergebnisse aus anderen Domänen anzuzeigen, wenn er danach gefragt wird. Der Unterschied zwischen der domänen- und gesamtstrukturweiten Suche beim Globalen Katalog liegt in einem kleinen Detail – nämlich dem Port, mit dem der Client die Verbindung zum DC aufbaut. Während normale LDAP-Suchen am Port 389 entgegengenommen werden, bearbeitet ein DC mit GC Anfragen zusätzlich auf dem Port 3268 und verwendet als Suchbasis alle lesbaren Domänenpartitionen.

Sind Applikationen so geschrieben, dass sie eine domänenübergreifende Suche anstoßen, wird der LDAP-Client nach einem Globalen Katalog suchen. Findet er keinen in der lokalen Site, muss er standortübergreifend auf einen verfügbaren Globalen Katalog zugreifen. Dies kann über Standortgrenzen hinweg die Performanz beeinträchtigen – gerade wenn die Verbindungen zwischen den Standorten nicht ausreichend genug ausgebaut ist. Andere Anwendungen wie etwa Microsoft Exchange setzen Globale Kataloge voraus, um Funktionen wie globale Adressbücher bereitstellen zu können.

Die Erreichbarkeit von GCs ist somit in vielerlei Hinsicht notwendig und lässt sich mit mehreren Bordmitteln von Windows testen – unter anderem mit LDP. Im Fenster "Verbinden" verwenden Sie anstelle des Standard-Ports 389 den GC-Port 3286. Nach der Authentifizierung kann wie zuvor nach Objekten gesucht werden. Der Ergebnissatz enthält nun nicht mehr nur Objekte aus der Domäne des verbundenen Domänencontrollers, sondern Objekte aller Domänen der Gesamtstruktur.

Sind nicht überall Globale Kataloge verfügbar, etwa weil nicht jeder Standort mit einem DC ausgerüstet ist, versuchen Clients, den nächsten Globalen Katalog im Verzeichnis zu erreichen. Der "nächste" Globale Katalog wird anhand der Kostenkonfiguration in "Active Directory-Standorte und -Dienste" bestimmt. Aufgrund dieser Konfiguration entscheiden DCs, ob sie durch Registrierung ihrer DNS-SRV-Einträge den DC-losen Standort abdecken müssen. Welcher Domänencontroller letztlich kontaktiert wird, entscheidet der DC-Locator-Prozess. Auch hier kann das Werkzeug "nltest" gute Arbeit bei der Fehlersuche leisten. *(dr)*

Nicht immer ist es sinnvoll, Attribute in den Index aufzunehmen. Da Attribute verschiedene Datentypen besitzen oder an eine besondere Syntax gebunden sind, gibt es Situationen, in denen von einer Indizierung abgesehen werden sollte. Folgend ein paar wenige Regeln, die bei der Erstellung von Indizes näher betrachtet werden müssen:

- Vor der Indizierung sollte ein grober Überblick über die im Attribut gespeicherten Daten gewonnen werden. Wenn ein Attribut nur wenige verschiedene Werte annimmt (etwa "Bürogebäude": Ost, West, Haupt), wird ein Index nicht effizient arbeiten.
- Ein Index ist nur dann sinnvoll, wenn er die Suchergebnisse über ein Attribut signifikant (im Verhältnis zur gesamten Suchbasis, ganzes Verzeichnis, alle Benutzer et cetera) einschränken kann.
- Leere Felder werden nicht indiziert – verfügt ein Attribut bei vielen Objekten über keinen Wert, ist der Index klein.
- Mehrwertige Attribute können zwar indiziert werden, verbessern aber nicht zwingend das Suchergebnis, wenn der Filter schlecht geformt wurde oder die Datenbasis schlecht ist. Objekte mit mehrwertigen Attributen werden nur einmal in der Suchergebnisliste angezeigt.
- Beim Betrachten der Datenbasis ist es vielleicht nicht notwendig, einen Index für ein verwendetes Attribut zu erstellen – eventuell lässt sich ein bereits indiziertes Attribut mit in den Filter aufnehmen, das die Suche einschränkt und beschleunigt.
- Das Erstellen eines Indexes erzeugt eine neue Tabelle in der AD-Datenbank, so dass sie stetig wächst. Je größer die Datenbasis des indizierten Attributes, desto größer der Zuwachs durch den Index.
- Es mag nicht immer logisch erscheinen, welchen Index das Active Directory für die Verarbeitung der Suche wählt. Sind mehrere Indizes mögliche Kandidaten, wägt AD über eine Schätzung der möglichen Resultate ab, welcher Index der geeignete ist. Das Statistik-Steuerelement listet den benutzten Index auf einer Suche auf.

Tipps zur Attributindizierung

Das nächste Sonderheft des IT-Administrator erscheint Ende März 2011

Thema:

Netzwerkanalyse & Troubleshooting

Ethernet, WLAN und VoIP fehlerfrei betreiben

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion
John Pardey (jp), *Chefredakteur*
verantwortlich für den redaktionellen Inhalt
john.pardey@it-administrator.de

Daniel Richey (dr), *Stellv. Chefredakteur*
daniel.richey@it-administrator.de

Lars Nitsch (ln),
Schlussredakteur
lars.nitsch@it-administrator.de

Autor dieses Sonderhefts
Klaus Bierschenk, Florian Frommherz,
Nils Kaczenski, Ulf B. Simon-Weidner

Anzeigen
Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

Druck
EUROPRINT, a.s.
Pod Kotlárkou 3
150 00 Praha 5
Tschechien

Vertrieb
Anne Kathrin Heinemann
Vertriebsleitung
kathrin@it-administrator.de
Tel.: 089/4445408-20

Abo- und Leserservice
Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Eltville
leserservice@it-administrator.de
Tel.: 06123/9238-251
Fax: 06123/9238-252

Internet
www.it-administrator.de

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel.: 089/4445408-0
Fax: 089/4445408-99
(zugleich Anschrift aller Verantwortlichen)

Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

Geschäftsführung / Anteilsverhältnisse
Geschäftsführende Gesellschafter zu gleichen Teilen sind Anne Kathrin und Matthias Heinemann.

ISSN
1614-2888

So erreichen Sie den Leserservice
Leserservice IT-Administrator
Stephan Orgel
65341 Eltville
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

Bankverbindung für Abonnenten
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

So erreichen Sie die Anzeigenabteilung
Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

Kompetentes Schnupperabo sucht neugierige Administratoren

Sie wissen, wie man Systeme und Netzwerke am Laufen hält. Und das Magazin IT-Administrator weiß, wie es Sie dabei perfekt unterstützt:

mit praxisnahen Workshops, aktuellen Produkttests und nützlichen Tipps und Tricks für den beruflichen Alltag.

Damit Sie sich Zeit, Nerven und Kosten sparen.

Teamwork in Bestform. Überzeugen Sie sich selbst!

6 Monate lesen

3 Monate bezahlen

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München
Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Bleiben Sie in Verbindung!

Folgen Sie uns auf Twitter

twitter.com/ita_blog

Werden Sie ein Fan auf Facebook

www.facebook.de/itanet

Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet

Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

Auf Facebook haben wir ein eigenes Profil. Neben ausgesuchten Informationen rund um das Magazin und Veranstaltungshinweisen finden Sie hier auch Gewinnspiele oder Wissenstests. Oder wollen Sie den IT-Administrator in 140 Zeichen täglich begleiten? Verfolgen Sie unser „Gezwitscher" über die interessantesten Neuigkeiten, besten Downloads und Tipps auf Twitter. Wenn Sie aber den direkten Austausch suchen, sind Sie in unserer Xing-Gruppe genau richtig. Lernen Sie dort Ihre Kollegen aus der IT und die Heftmacher des IT-Administrators persönlich kennen und nehmen Sie Einfluss auf Ihr Praxismagazin. Immer gut informiert bleiben Sie auch über unseren RSS-Feed.

Treten Sie unserer Community bei. Wir freuen uns auf Sie.