

Aktualisierung auf Windows Server 2003

Die erste Version von Active Directory für Windows 2000 war erstaunlich stabil und robust. Bewertet man die Fehlerfreiheit der ersten Produktversionen, steht Microsoft wohl nicht an der Spitze. Aber für Windows 2000 Active Directory hat sich Microsoft Lob verdient, was den Funktionsumfang und die Zuverlässigkeit betrifft. Active Directory war allerdings so komplex und von so weit reichender Bedeutung, dass es natürlich noch viel Raum für Verbesserungen gab. Es traten gewisse Probleme mit der Skalierbarkeit auf, wie zum Beispiel die unrühmliche 5000-Mitglieder-Begrenzung für Gruppen oder die Begrenzung auf 300 Standorte, aus denen sich unter Umständen künstliche Beschränkungen für die Art und Weise ergaben, in der Sie Active Directory anwenden. Beide Probleme wurden in Windows Server 2003 gelöst. Die Vorgaben für die Konfiguration der Sicherheit waren bei Windows 2000 Active Directory nicht so gut, wie sie hätten sein sollen. Signierter LDAP-Verkehr und andere Verbesserungen der Sicherheit wurden seitdem in Service-Packs aufgenommen und sind nun im Lieferumfang von Windows Server 2003 enthalten. Die Verwaltung war ein weiterer Bereich, in dem Active Directory noch überarbeitet werden musste. In Windows Server 2003 sind zahlreiche Befehlszeilenprogramme hinzugekommen, und die Snap-Ins zur AD-Verwaltung wurden beträchtlich verbessert.

Wir haben einige Schlüsselbereiche genannt, in denen Active Directory in Windows Server 2003 verbessert wurde, und im nächsten Abschnitt beschreiben wir weitere neue Funktionen. Wenn Sie bereits mit Windows 2000 Active Directory arbeiten, wird sich Ihre nächste größere Entscheidung um die Frage drehen, ob und wann Sie auf Windows Server 2003 umsteigen. Zum Glück ist der Übergang zu Windows Server 2003 eher ein evolutionärer Schritt und kein revolutionärer wie beim Umstieg von Windows NT auf Active Directory. Microsoft hat sich zum Ziel gesetzt, den Wechsel zu Windows Server 2003 so nahtlos wie möglich zu gestalten. Das ist im Wesentlichen auch gelungen. Sie können so viele Windows Server 2003-Domänen-Controller in Ihre vorhandene Active Directory-Umgebung aufnehmen, wie Sie es für richtig halten. Diese sind vollständig mit Windows 2000-Domänen-Controllern kompatibel.

Bevor Sie aber Windows Server 2003-Domänen-Controller einführen können, müssen Sie die Gesamtstruktur und die Domänen mit dem Werkzeug ADPrep vorbereiten. Es bereitet die Gesamtstruktur auf die neuen Funktionen vor, die verfügbar werden, sobald Sie die Funktionsebene der Domäne oder der Gesamtstruktur heraufsetzen. Funktionsebenen lassen sich mit den Domänenmodi von Windows 2000 Active Directory vergleichen. Sie erlauben die Konfiguration von unterschiedlichen Funktionalitätsebenen, die in der Domäne oder der Gesamtstruktur verfügbar sind, je nachdem, welche Betriebssysteme auf den Domänen-Controllern laufen.

Bevor wir den Umstieg auf Windows Server 2003 besprechen, möchten wir kurz auf einige der wichtigsten neuen Funktionen von Windows Server 2003 eingehen und auf einige der Funktionsunterschiede zu Windows 2000 hinweisen. Anhand dieser Informationen sollte es Ihnen leichter fallen, die Notwendigkeit oder Dringlichkeit des Umstiegs einzuschätzen.

Neue Features in Windows Server 2003

Auch wenn Windows Server 2003 eher als evolutionärer Schritt angesehen wird, gibt es doch eine ganze Reihe von neuen Features, die den Umstieg attraktiv machen.



Mit »Feature« meinen wir eine neue Funktionalität, die nicht nur eine kleine Änderung gegenüber der Art und Weise darstellt, in der die betreffende Aufgabe unter Windows 2000 gelöst wurde. In diesem Sinn ist ein Feature etwas, das man explizit implementieren oder benutzen muss. Funktionsunterschiede zu Windows 2000 werden im nächsten Abschnitt besprochen.

Wir empfehlen, jedes dieser Features sorgfältig zu prüfen und nach folgenden Kategorien zu bewerten:

1. Sie würden das Feature sofort einsetzen.
2. Sie würden das Feature später einsetzen.
3. Sie würden das Feature niemals einsetzen, oder es ist nicht wichtig.

Die Bewertung jedes Features wird Ihnen bei der Überlegung helfen, welchen Vorteil Sie von einem Umstieg hätten. In der folgenden Liste werden die neuen Features in zufälliger Reihenfolge aufgeführt:

Anwendungspartitionen

Sie können Partitionen anlegen, die auf jeden Domänen-Controller in der Gesamtstruktur repliziert werden können.

Gleichzeitige LDAP-Bindungen

Gleichzeitige LDAP-Bindungen (Concurrent LDAP binds) generieren kein Kerberos-Ticket und kein Sicherheitstoken und sind daher viel schneller als eine einfache LDAP-Bindung.

Gesamtstrukturübergreifende Vertrauensstellung

Dies ist eine transitive Vertrauensstellung, die es allen Domänen aus zwei verschiedenen Gesamtstrukturen ermöglicht, sich gegenseitig zu vertrauen, obwohl nur eine einzige Vertrauensstellung zwischen den beiden Stammdomänen der Gesamtstrukturen definiert wurde.

Umbenennung eines Domänen-Controllers

Zur Umbenennung eines Domänen-Controllers ist ein einfacher Neustart erforderlich.

Umbenennung einer Domäne

Domänen können nun einen anderen Namen erhalten, allerdings nicht ohne beträchtliche Auswirkungen auf die Benutzer (alle Mitgliedscomputer müssen zweimal neu gestartet werden). Weitere Informationen finden Sie unter: <http://www.microsoft.com/windowsserver2003/downloads/domainrename.mspx>.

Dynamische Erweiterungsklassen

Es ist nun möglich, dynamische Erweiterungsklassen auf Standardbasis zu implementieren. Unter Windows 2000 werden Erweiterungsklassen als »statisch« angesehen, weil sie im Schema statisch definiert werden. Dynamische Erweiterungsklassen lassen sich bei der Erstellung eines Objekts einbinden, ohne im Schema als Erweiterungsklasse für die objectClass des Objekts definiert zu sein.

Dynamische Objekte

Bisher blieben Objekte so lange in Active Directory gespeichert, bis sie explizit gelöscht wurden. Dynamische Objekte können mit einer Lebensdauervorgabe (Time To Live, TTL) angelegt werden, nach deren Ablauf sie automatisch gelöscht werden, sofern die Lebensdauer nicht verlängert wird.

Installation von Medien

Dieses oft benötigte Feature ermöglicht es, Domänen-Controller-Replikate, die aus einem Backup eines anderen Domänen-Controllers eingerichtet wurden, in eine Gesamtstruktur heraufzustufen. Besonders in großen Domänen kann dies eine beträchtliche Zeitersparnis bei der Heraufstufung von Domänen-Controllern bedeuten.

MMC und CLI-Erweiterungen

Das Programm Active Directory-Benutzer und -Computer (ADUC) wurde erweitert und lässt die Auswahl von mehreren Objekten zu. Andere Werkzeuge wie *repadmin* und *netdom* haben neue Optionen.

Neue DS CLI-Werkzeuge

Eine neue Gruppe von CLI-Werkzeugen bietet eine größere Flexibilität bei der Verwaltung von Active Directory von der Befehlszeile aus. Dazu gehören *dsadd*, *dsmod*, *dsrm*, *dsget* und *dsquery*.

Neue GPO-Werte

Es gibt über 100 neue GPO-Werte, so dass die Verwaltung der Active Directory-Clients flexibler wird.

GPO RSoP

RSoP (Resultant Set of Policy) wurde in ADUC aufgenommen und lässt sich mit der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) einsetzen. RSoP ermöglicht Administratoren die Festlegung, welche GPO-Werte für Endbenutzer und Computer angewendet werden.

TLS-Unterstützung

Von Windows 2000 wurde nur SSL zur Verschlüsselung von Datenübertragungen unterstützt. TLS, der neueste Lösungsansatz zur standardisierten Verschlüsselung des LDAP-Verkehrs, wird nun ebenfalls unterstützt.

Kontingente

Wenn Benutzer unter Windows 2000 Objekte anlegen durften, dann konnten sie so viele Objekte erzeugen, wie sie wollten. Es gab keine Möglichkeit, die Menge zu beschränken. Nun lassen sich Kontingente (Quotas) für die Anzahl der Objekte festlegen, die ein Benutzer oder eine Benutzergruppe anlegen darf. Durch entsprechende Kontingente lässt sich auch festlegen, wie viele Objekte von einer bestimmten objectClass angelegt werden dürfen.

Gruppen auf Abfragebasis

Wird für die Autorisierung auf Rollenbasis benutzt. Der neue Autorisierungs-Manager ermöglicht die Definition von flexiblen Gruppen anhand von Informationen, die unter den Benutzerdaten gespeichert werden (zum Beispiel die Abteilung).

Umlenkung von Benutzern und Computern

Sie können den Standardort zur Speicherung von neuen Benutzern und Computern mit den Befehlen *redirusr* und *redircmp* umlenken.

Schemaänderung

Sie können Attribute und Klassen im Schema außer Kraft setzen und dann neu definieren.

Universelle Gruppenzwischenspeicherung

Durch die Freischaltung der universellen Gruppenzwischenspeicherung (Universal Group Caching) können Sie es vermeiden, dass bei der Anmeldung ein Server mit dem Globalen Katalog verfügbar sein muss. Diese Zwischenspeicherung wird auf Standortebene freigeschaltet und gilt für alle Clients, die sich bei den Domänen-Controllern dieses Standorts anmelden.

Zeitstempelattribut für die letzte Anmeldung

Ein klassisches Problem in einer NOS-Umgebung ist die Bestimmung des letzten Zeitpunkts, zu dem sich ein Benutzer oder ein Computer angemeldet hat. Das neue Attribut *lastLogonTimestamp* wird repliziert. Das bedeutet, dass Sie zum Beispiel mit einer einfachen Abfrage alle Benutzer oder Computer ermitteln können, die sich in einem bestimmten Zeitraum nicht angemeldet haben.

WMI-Filterung von GPOs

Neben den OU-, Standort-, Domänen- und Sicherheitsgruppenkriterien, nach denen man GPOs filtern kann, können Sie nun auch die WMI-Informationen auf der Maschine des Clients benutzen, um herauszufinden, ob ein GPO eingesetzt werden soll.

WMI-Provider für Vertrauensstellungen und Überwachung der Replikation

Dieser neue WMI-Provider bietet die Möglichkeit, Vertrauensstellungen und die Replikation per Programmcode zu überwachen.

Wenn Sie zu der Überzeugung kommen, dass Sie mehr als vier oder fünf der Features sofort einsetzen würden oder irgendwann vier oder fünf der Features benutzen wollen, könnte der Vorteil hinreichend groß sein, um in der nächsten Zeit auf Windows Server 2003 umzusteigen. Können Sie dagegen nicht viel mit den neuen Features anfangen, hilft Ihnen der nächste Abschnitt vielleicht bei der Entscheidung weiter. Dort geht es um die Funktionsunterschiede zu Windows 2000.

Unterschiede zu Windows 2000

Active Directory war zwar bereits so gut skalierbar, dass die meisten Organisationen zufrieden waren, aber nach einigen Jahren Erfahrung im Praxiseinsatz zeigte sich natürlich ein gewisser Bedarf an Verbesserungen. Viele der Funktionsunterschiede zu Windows 2000 sind das direkte Ergebnis von Erfahrungen, die AD-Administratoren gesammelt haben.

Wie bei den neuen Features empfehlen wir, die Unterschiede genau zu überprüfen und nach folgenden Kategorien zu bewerten:

1. Es würde meine Umgebung wesentlich verbessern.
2. Es würde meine Umgebung ein wenig verbessern.
3. Es würde meine Umgebung beeinträchtigen.

Beim größten Teil der Unterschiede handelt es sich um Verbesserungen, die sich für Sie positiv auswirken dürften. In manchen Situationen ist dadurch allerdings anfangs etwas mehr Arbeit erforderlich, wie zum Beispiel bei den sicherheitsbezogenen Änderungen.

Speicherung nur einer Instanz

Eindeutige Sicherheitsbeschreibungen werden nur einmal gespeichert, und zwar unabhängig davon, wie oft sie benutzt werden. Es wird also nicht für jede Instanz ein separater Deskriptor angelegt. Das allein spart nach der Umstellung schon 20 bis 40 Prozent Platz in Ihrer DIT. Beachten Sie bitte, dass eine Offline-Defragmentierung erforderlich wird, um den unnötig belegten Laufwerksplatz freizugeben.

Verbesserte Kontensperrung

Einige Fehler, die in Windows 2000 fälschlich zu Kontensperrungen führten, wurden beseitigt. Eine neue Eigenschaftenseite für Active Directory-Benutzer und -Computer namens Erweiterte Konteninformationen (Additional Account Info)

und das Programm *lockoutstatus.exe* sind gute Werkzeuge für die Diagnose von Kontensperrungsproblemen.

Verbesserte Ereignisprotokollnachrichten

Es gibt einige neue Ereignisprotokollnachrichten für die Replikation, DNS, FRS und so weiter, die sich bei der Fehlersuche als hilfreich erweisen.

Verknüpfungswertreplikation (Link value replication, LVR)

Die Replikation erfolgt in Active Directory auf Attributebene. Wenn also ein Attribut geändert wird, so wird das gesamte Attribut repliziert. Bei einigen Attributen ergaben sich daraus Probleme, wie zum Beispiel beim Mitgliedsattribut von Gruppenobjekten, das immerhin rund 5000 Mitglieder aufnehmen konnte. LVR-Replikation bedeutet, dass bestimmte Attribute (zum Beispiel member) nach jeder Änderung nur die Änderungen im Attribut replizieren und nicht den Inhalt des gesamten Attributs.

Standortinterne Replikationsfrequenz auf 15 Sekunden geändert

Der alte Vorgabewert war 5 Minuten und wurde nun auf 15 Sekunden geändert.

Keine Synchronisation des Globalen Katalogs für PAS-Addition

Wenn ein Attribut in den Teilattributsatz (Partial Attribute Set, PAS) aufgenommen wird, so wird keine Synchronisation des Globalen Katalogs mehr vorgenommen, wie es unter Windows 2000 der Fall war. Besonders für die Administratoren von großen, über den ganzen Globus verteilten Windows 2000-Domänen war dies unheimlich lästig.

Signierter LDAP-Verkehr

Statt den LDAP-Datenverkehr mit Werkzeugen wie ADUC und ADSI Edit im Klartext (Plain ASCII) durch die Übertragungsleitung zu schicken, werden die Daten nun signiert und bei der Gelegenheit auch verschlüsselt.

Verbesserte ISTG- und KCC-Skalierbarkeit

Die Algorithmen zur Generierung der Verbindungen zwischen den Standorten wurden so weit verbessert, dass die bisherige Beschränkung auf 300 bis 400 Standorte weggefallen ist und nun bei etwa 3000 bis 5000 Standorten liegt.

Schnellere Entfernung des Globalen Katalogs

Wenn Sie unter Windows 2000 den Globalen Katalog auf einem DC sperren, kann der Entfernungsprozess für den Globalen Katalog in 15 Minuten nur ungefähr 500 Objekte entfernen. Das wurde so geändert, dass der Vorgang nun wesentlich schneller läuft.

Die Überwachung verteilter Verknüpfungen (Distributed Link Tracking, DLT) ist standardmäßig ausgeschaltet

Der DLT-Dienst kann die Quelle von Tausenden, wenn nicht Millionen link-TrackOMTEntry-Objekten sein, die im System-Container einer Domäne liegen. Auf Windows Server 2003-Domänen-Controllern ist der DLT-Dienst daher normalerweise ausgeschaltet.

Änderungen beim kompatiblen Zugriff auf Systeme, die älter als Windows 2000 sind

Zur Verbesserung der Sicherheit steht der Sicherheitsprinzipal Jeder nicht mehr für jeden nichtauthentifizierten und jeden authentifizierten Benutzer. Stattdessen repräsentiert er nur authentifizierte Benutzer. Wenn Sie in Windows Server 2003 so etwas wie einen anonymen Zugriff ermöglichen möchten, sollten Sie das Konto Anonyme Anmeldung in die Gruppe für »Prä-Windows 2000 kompatiblen Zugriff« aufnehmen.

Wenn Sie zu dem Schluss kommen, dass mehr als zwei oder drei dieser Punkte für Ihre Umgebung von Vorteil wären und weniger als ein oder zwei einen negativen Effekt haben, ist dies ein weiterer Hinweis darauf, dass der Umstieg auf Windows Server 2003 so viele Vorteile bringt, dass Sie ihn näher ins Auge fassen sollten. Natürlich ist das keine absolute Regel, denn manche Dinge sind vielleicht wichtiger als andere. Wenn Sie zum Beispiel über 300 oder 400 Standorte mit Domänen-Controllern haben, könnte die Verbesserung im KCC für Sie von Bedeutung sein. Müssen Sie sich dagegen in der nahen Zukunft mit der Aufnahme neuer Attribute in den Teilattributsatz beschäftigen und haben Sie es mit Globalen-Katalog-Servern zu tun, die praktisch über den gesamten Globus verteilt sind, dann könnte Ihnen das geänderte Verhalten bei der Synchronisation des Globalen Katalogs so manches lange Wochenende ersparen, an dem Sie sonst Babysitter für die Replikation spielen müssten. Vielleicht sehen Sie auch andere Features als Vorteil, wie zum Beispiel die MMC-Verbesserungen, aber deren Bedeutung dürfte nicht an die beiden gerade beschriebenen heranreichen. Sie kommen nicht umhin, bei Ihren Überlegungen jeden Punkt sorgfältig zu gewichten.

Funktionsebenen erklärt

Nachdem wir nun kurz skizziert haben, welche neuen Features Active Directory zu bieten hat und welche Verbesserungen es gegenüber Windows 2000 gibt, möchten wir beschreiben, wie man diese Features unter Windows Server 2003 tatsächlich verfügbar macht. Wenn Sie bereits mit Windows 2000 Active Directory gearbeitet haben, kennen Sie wahrscheinlich das Konzept des Domänenmodus. In Windows 2000 Active Directory gab es den gemischten und den einheitlichen Modus. Der Domänenmodus schrieb einfach vor, welche Betriebssysteme auf den Domänen-Controllern laufen durften, und weiter nichts. Mit dem Wechsel in den einheitlichen Modus wurden neue Features verfügbar, wie universelle Gruppen und die Schachtelung von Gruppen, um einige zu nennen. Stellen Sie sich Funktionsebenen wie Domänenmodi vor, aber einen Schritt weiter entwickelt.

Die Funktionsebenen von Windows Server 2003 lassen sich mit den Domänenmodi von Windows 2000 vergleichen, weil sie ebenfalls vorschreiben, welche Betriebssysteme auf den Domänen-Controllern laufen dürfen. Außerdem können sie nur heraufgesetzt werden, aber niemals herabgesetzt. Allerdings wird der Punkt oft falsch verstanden, dass sich Domänenmodi praktisch nicht auf die Clients und deren eingerichtete Betriebssysteme auswirken. Zum Beispiel können Sie in Windows 2000-Domänen, die im gemischten

oder im einheitlichen Modus betrieben werden, mit Windows 9x-Clients arbeiten, und auch in Domänen, die auf der Funktionsebene Windows 2000 oder Windows Server 2003 laufen.



Informationen darüber, welche Betriebssysteme in den verschiedenen Funktionsebenen erlaubt sind, finden Sie im Abschnitt »Windows Server 2003-Funktionsebenen« in Kapitel 2.

Ein wichtiger Unterschied ist allerdings, dass Funktionsebenen auf der Ebene der Domäne und der Gesamtstruktur gelten. Dafür gibt es einen einfachen Grund: Manche Features von Windows Server 2003 Active Directory setzen voraus, dass alle Domänen-Controller in einer Domäne mit Windows Server 2003 laufen oder dass alle Domänen-Controller in der ganzen Gesamtstruktur mit Windows Server 2003 laufen.

Sehen wir uns zur Verdeutlichung zwei Beispiele an. Beginnen wir mit dem neuen Attribut »Zeitstempel der letzten Anmeldung«. Dieses Feature sorgt dafür, dass ein neues Attribut namens `lastLogonTimestamp` einen Wert erhält, wenn sich ein Benutzer oder ein Computer bei einer Domäne anmeldet, und es wird auf alle Domänen-Controller in der Domäne repliziert. Mit diesem Attribut können Sie herausfinden, ob sich ein Benutzer oder Computer in der letzten Zeit angemeldet hat, und zwar auf einfachere Weise als mit dem Attribut `lastLogon`, das nicht repliziert wird und daher auf jedem Domänen-Controller der Domäne abgefragt werden muss. Damit `lastLogonTimestamp` von Nutzen ist, müssen alle Domänen-Controller in der Domäne wissen, wie der Wert aktualisiert wird, wenn sie eine Anmeldung von einem Benutzer oder Computer erhalten. Domänen-Controller von anderen Domänen brauchen sich nur um die Objekte in ihren eigenen Domänen zu kümmern. Deswegen gilt dieses Feature nur domänenweit. Windows 2000-Domänen-Controller wissen nichts über `lastLogonTimestamp` und aktualisieren dieses Attribut nicht. Damit dieses Attribut wirklich von Nutzen sein kann, sollten alle Domänen-Controller in der Domäne mit Windows Server 2003 laufen. Alle Domänen-Controller müssen darüber informiert werden, dass die anderen Domänen-Controller Windows Server 2003 benutzen. Das erfahren sie durch die Abfrage der Funktionsebene, die für die Domäne gilt. Sobald sie herausfinden, dass die Domäne auf einer bestimmten Funktionsebene läuft, können sie die Features benutzen, die zu dieser Funktionsebene gehören.

In vergleichbarer Weise können sich Situationen ergeben, in denen alle Domänen-Controller in einer Gesamtstruktur Windows Server 2003 benutzen müssen, damit ein bestimmtes Feature verfügbar wird. Die Verbesserungen bei der Replikation sind ein gutes Beispiel. Wenn einige der ISTGs die alten Algorithmen für die Standorttopologie benutzen und andere die neuen, könnte sich eine Art Replikations-Chaos ergeben. Alle Domänen-Controller in der Gesamtstruktur müssen Windows Server 2003 benutzen, damit die neuen Algorithmen freigeschaltet werden. Bis es so weit ist, werden die Windows 2000-Algorithmen benutzt.

So wird die Funktionsebene heraufgestuft

Um die Funktionsebene einer Domäne oder Gesamtstruktur heraufzustufen, können Sie das MMC-Snap-In Active Directory-Domänen und -Vertrauensstellungen verwenden. Wenn Sie die Funktionsebene einer Domäne heraufstufen möchten, öffnen Sie das Snap-In, suchen die Domäne, die Sie heraufstufen möchten, klicken Sie auf der linken Fensterseite mit der rechten Maustaste an und wählen *Domänenfunktionsebene heraufstufen...* Dann öffnet sich ein Dialogfeld wie in Abbildung 14-1.

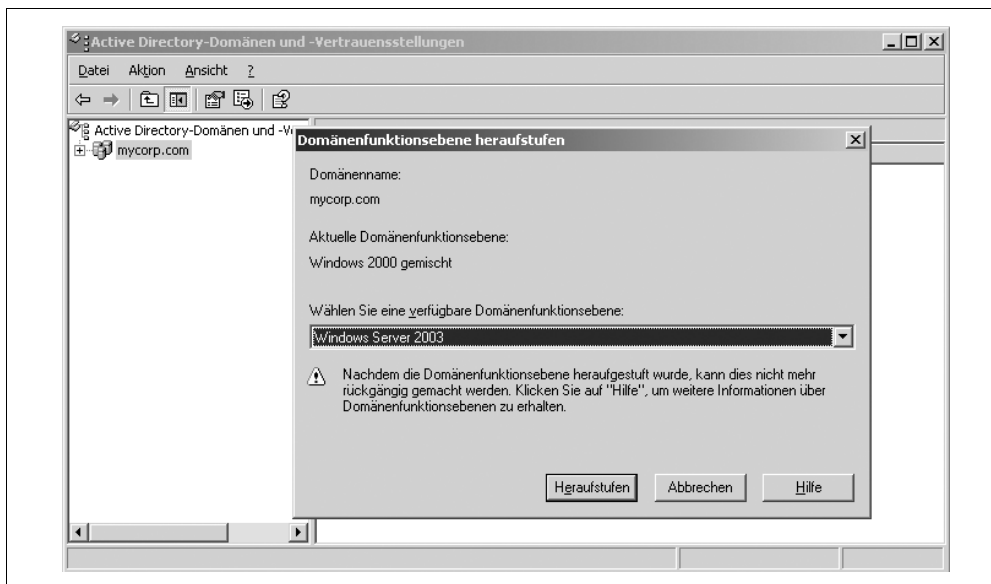


Abbildung 14-1: Heraufstufung der Domänenfunktionsebene

Wählen Sie die neue Funktionsebene aus, und klicken Sie auf die Schaltfläche *Heraufstufen*. Anschließend erhalten Sie eine Bestätigung, dass die Heraufstufung erfolgreich war, oder eine Fehlermeldung mit einer Begründung, warum die Funktionsebene nicht heraufgestuft werden konnte. Abbildung 14-2 zeigt die Meldung, die nach der erfolgreichen Heraufstufung der Funktionsebene erscheint. In ähnlicher Weise lässt sich die Funktionsebene einer Gesamtstruktur heraufstufen. Dazu klicken Sie in der linken Fensterfläche mit der rechten Maustaste auf *Active Directory-Domänen und -Vertrauensstellungen* und wählen *Gesamtstrukturfunktionsebene heraufstufen...*

Sie können die Funktionsebene einer Domäne oder Gesamtstruktur auch mit zwei anderen Verfahren festlegen. Erstens können Sie sich für Domänen das msDS-Behavior-Version-Attribut im Domännennamenskongext (zum Beispiel `dc=mycorp,dc=com`) ansehen oder für die Gesamtstruktur den Partitions-Container im Konfigurationsnamenskongext (d.h. `cn=partitions,cn=configuration,dc=mycorp,dc=com`). Der Wert 0 steht für die Funktionsebene Windows 2000, 1 für die Windows-Interimsfunktionsebene und 2 für Windows Server 2003.

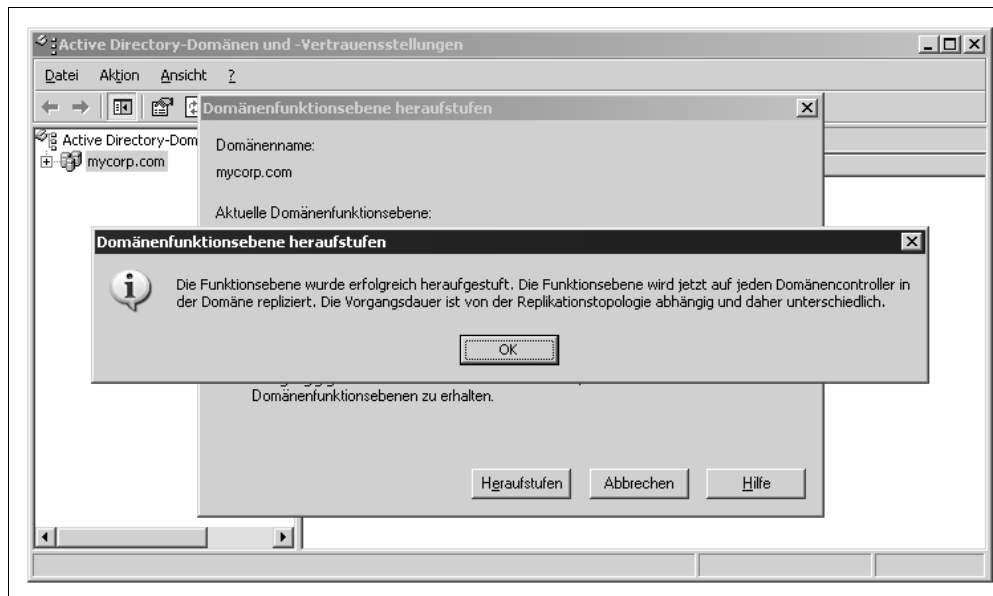


Abbildung 14-2: Die Domänenfunktionsebene wurde erfolgreich heraufgestuft

Als Alternative bietet sich noch an, diese Informationen im RootDSE eines Domänen-Controllers nachzusehen. Auf Windows Server 2003-Domänen-Controllern enthält RootDSE zwei neue Attribute, die die aktuelle Funktionsebene beschreiben:

domainFunctionality

Dieser Wert spiegelt den msDS-Behavior-Version-Wert aus dem Domänennamens-kontext.

forestFunctionality

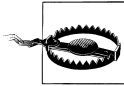
Dieser Wert spiegelt den msDS-Behavior-Version-Wert aus dem Partitions-Contai-ner.

Vorbereitung für ADPrep

Bevor Sie die Funktionsebenen freischalten können, müssen Sie die vorhandene Infra-struktur auf Windows Server 2003 aktualisieren. Der erste Schritt vor der Heraufstufung Ihres ersten Windows Server 2003-Domänen-Controllers ist die Vorbereitung der Ge-samtstruktur mit dem Hilfsprogramm ADPrep.

Wenn Sie in Ihrer Active Directory-Gesamtstruktur Exchange 2000 installiert haben, kennen Sie sicher die Exchange-Schalter *setup.exe /forestprep* und */domainprep*. Diese Schalter werden unabhängig von der Exchange-Server-Installation benutzt, damit sich Active Directory-Administratoren um die AD-bezogenen Vorbereitungen für Exchange kümmern können. Der Exchange-Befehl */forestprep* erweitert das Schema und fügt einige Objekte in den Konfigurationsnamenskontext ein. Der Exchange-Befehl */domain-*

prep fügt Objekte in den Domänennamenskontext der Domäne ein, auf der er läuft, und setzt einige ACLs. Der ADPrep-Befehl folgt derselben Logik und führt ähnliche Aufgaben durch, um die Aktualisierung auf Windows Server 2003 vorzubereiten.



Microsoft empfiehlt, vor dem Start von ADPrep zumindest das Service Pack (SP) 2 auf den Domänen-Controllern zu installieren. SP 2 behebt einen kritischen internen AD-Fehler, der bei der Erweiterung des Schemas auftreten kann. Außerdem gibt es einige Korrekturen zur Verbesserung der Replikationsverzögerung, die sich bei der Indizierung von Attributen zeigt. Wenn Sie vorhaben, über längere Zeit eine Umgebung mit Windows 2000 und Windows Server 2003 einzusetzen, empfiehlt Microsoft, auf den Windows 2000-Domänen-Controllern SP3 zu installieren.

Weitere Informationen zu den Microsoft-Empfehlungen finden Sie im Microsoft Knowledge Base-Artikel 331161 unter <http://support.microsoft.com>.

Der Befehl ADPrep ist auf der Windows Server 2003-CD im Verzeichnis `\i386` zu finden. ADPrep ist auf mehrere Dateien angewiesen, die in diesem Verzeichnis liegen, und lässt sich daher nicht einfach auf eine Diskette oder CD kopieren. Den Befehl ForestPrep geben Sie folgendermaßen:

```
X:\i386\adprep /forestprep
```

Dabei stellt `X:` ein CD-Laufwerk mit der Windows Server 2003-CD dar, sei es auf der lokalen Maschine oder auf dem Netzwerk abgebildet. Auf ähnliche Weise wird der Befehl DomainPrep gegeben:

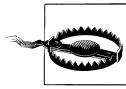
```
X:\i386\adprep /domainprep
```

Die detaillierte Ausgabe des ADPrep-Befehls können Sie sich in den Protokolldateien ansehen, die im Verzeichnis `%SystemRoot%\system32\debug\adprep\logs` abgelegt werden. Bei jeder Ausführung von ADPrep wird eine neue Protokolldatei mit allen Aktionen generiert, die bei dem betreffenden Aufruf durchgeführt wurden. Die Namen der Protokolldateien werden aus Datum und Uhrzeit des ADPrep-Aufrufs gebildet.

Sehen wir uns nun genauer an, was ForestPrep und DomainPrep tun.

ForestPrep

Der Befehl `ADPrep /forestprep` erweitert das Schema um einige neue Klassen und Attribute. Diese neuen Schema-Objekte sind für die neuen Features von Windows Server 2003 erforderlich. Sie können sich die Schema-Erweiterungen in den `.ldf`-Dateien ansehen, die im Verzeichnis `\i386` der Windows Server 2003-CD liegen. Diese Dateien enthalten LDIF-Einträge für die Aufnahme und Änderung neuer und vorhandener Klassen und Attribute.



Microsoft rät von manuellen Erweiterungen des Schemas mit den LDIF-Dateien von ADPrep ab. Lassen Sie stattdessen ADPrep die Arbeit für Sie tun.

ForestPrep verschärft einige Standard-Sicherheitsbeschreibungen und ändert einige der ACLs in den Containern des Configuration-NCs. Neue displaySpecifier-Objekte werden hinzugefügt und einige vorhandene geändert, um die administrativen Active Directory-Snap-Ins an die neuen Features anzupassen. Ein NTDS Quotas-Container wird in den Stamm des Configuration-Containers aufgenommen. Das ist ein neuer Container für die Kontingentobjekte, mit denen festgelegt wird, wie viele Objekte ein Benutzer oder eine Benutzergruppe in einem Container oder einer OU einfügen kann.

ADPrep speichert seinen Fortschritt in Active Directory. Diese clevere Lösung ermöglicht eine elegante Wiederaufnahme nach Fehlern, die irgendwo in der Mitte der Arbeit auftreten. Außerdem kann man schnell ermitteln, ob alle erforderlichen Operationen durchgeführt wurden und ob ADPrep erfolgreich war. Die Speicherung der Operationen in Active Directory ist zum Beispiel auch dann von Vorteil, wenn Sie auf Probleme stoßen und die Microsoft Support Services anrufen müssen. Dann können Sie sich diesen Container ansehen und alle Operationen auflisten, die erfolgreich durchgeführt wurden. Die Support Services können dann nachsehen, welche Operation fehlgeschlagen ist.

Direkt unter dem Configuration-Container wird ein ForestUpdates-Container angelegt. In diesem ForestUpdates-Container liegen zwei weitere Container mit den Namen Operations und Windows2003Update. Der Container Operations enthält weitere Container, die jeweils eine bestimmte Aufgabe darstellen, die ADPrep abgeschlossen hat. Eine dieser Operationen könnte zum Beispiel die Erstellung von neuen displaySpecifier-Objekten sein. Die Namen der Operationscontainer sind GUIDs, und die Objekte selbst enthalten keine Informationen, die von Interesse wären. Insgesamt sollte es nach dem Abschluss der ForestPrep-Arbeiten 36 dieser Operationscontainer geben.

Das andere Objekt im Container ForestUpdates heißt Windows2003Update. Dieses Objekt wird angelegt, wenn ADPrep fertig ist. Sofern dieses Objekt vorhanden ist, bedeutet es, dass ADPrep erfolgreich ForestPrep abgeschlossen hat. Wenn Sie also herausfinden möchten, wann ForestPrep in einer Gesamtstruktur abgeschlossen wurde, sehen Sie sich einfach das Attribut whenCreated des Windows2003Update-Objekts an. Abbildung 14-3 zeigt, wie dieser Container im Snap-In ADSI Edit aus den Windows Support Tools aussieht.

Sie brauchen ForestPrep nur einmal auszuführen. Sie können den Befehl zwar mehrfach geben, aber da er seinen Fortschritt in Active Directory im Container ForestUpdates vermerkt, wird eine Wiederholung nur dann etwas bewirken, wenn eine Operation zuvor nicht erfolgreich abgeschlossen wurde.

Da das Schema erweitert wird und an zahlreichen Stellen im Configuration-NC Objekte angelegt werden, muss der Benutzer, der ForestPrep startet, ein Mitglied der Gruppen Schema-Admins und Enterprise-Admins sein. Außerdem sollten Sie den Befehl direkt auf

dem Schema-Master der Gesamtstruktur geben. Der Import der Schema-Erweiterungen ist recht ressourcenintensiv und sollte daher auf dem Schema-Master erfolgen. Außerdem kann die Ausführung von ForestPrep einige Zeit dauern, wenn Sie große Domänen mit vielen Objekten haben. ForestPrep indiziert einige Attribute. Das erfordert einige Rechenzeit bei der Aktualisierung der AD-Datenbank.

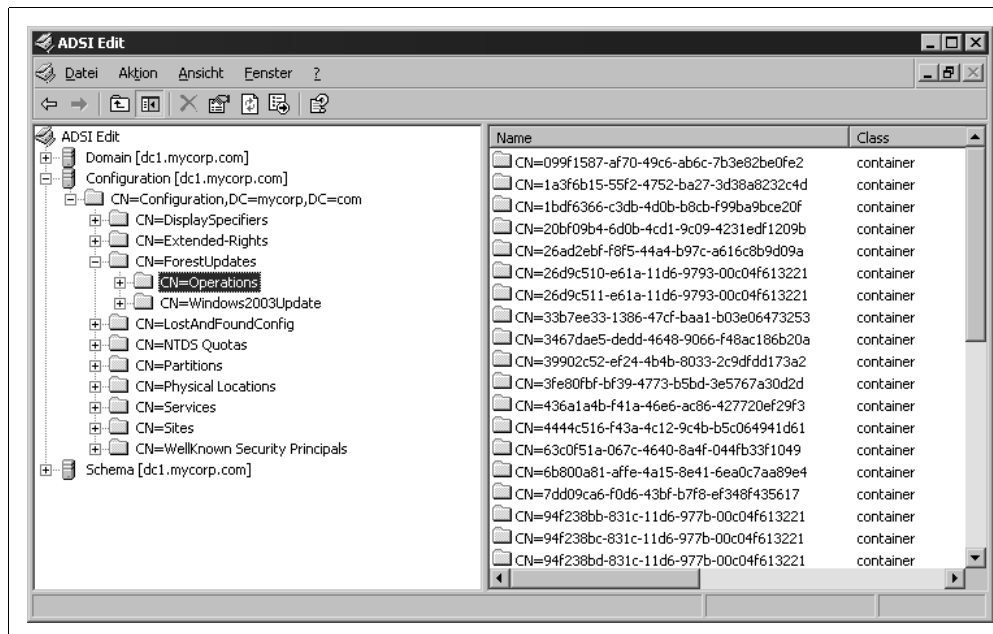


Abbildung 14-3: ADPrep-Operationen zur Aktualisierung der Gesamtstruktur

DomainPrep

Bevor Sie den Befehl `ADPrep /domainprep` geben, müssen Sie sicher sein, dass die Änderungen von ForestPrep auf alle Domänen-Controller der Gesamtstruktur repliziert wurden. DomainPrep muss auf dem Infrastruktur-Master einer Gesamtstruktur und mit den Rechten eines Mitglieds der Domänen-Admins-Gruppe gestartet werden. Wenn Sie versuchen, DomainPrep zu starten, bevor ForestPrep gelaufen ist und alle Änderungen repliziert wurden, erhalten Sie eine Fehlermeldung. Falls Sie nicht sicher sind, was die Meldung zu bedeuten hat, empfiehlt es sich auch in diesem Fall, die ADPrep-Protokolle im Verzeichnis `%SystemRoot%\system32\debug\adprep\logs` auszuwerten.

DomainPrep erstellt neue Container und Objekte, ändert die ACLs einiger Objekte und ändert die Bedeutung des Sicherheitsprinzips Jeder.

Anders als der Befehl ForestPrep, der sehr ressourcenintensiv ist, läuft DomainPrep relativ schnell ab. Im Vergleich mit ForestPrep sind die Änderungen gering. In der obersten Ebene werden zwei neue Container angelegt: einer namens NTDS Quotas, wie der, den

ForestPrep in den Configuration-Container eingebaut hat, und ein weiterer Container namens Program Data. Er ist als Ausgangspunkt zur Speicherung von Anwendungsdaten vorgesehen, damit sich nicht jeder Provider seine eigene OU-Struktur ausdenken muss.

Wie ForestPrep speichert auch DomainPrep den Stand der Arbeit in Active Directory ab. Unter dem Container System wird ein Container namens DomainUpdates angelegt. In diesem Container entstehen zwei weitere Container mit den Namen DomainUpdates und Windows2003Update. Die Speicherung erfolgt nach dem gleichen Prinzip wie bei ForestPrep. Jede Operation, die von DomainPrep durchgeführt wird, wird als Objekt im Container Operations gespeichert. Für DomainPrep gibt es 52 Operationen. Nach dem Abschluss der Operationen wird das Objekt Windows2003Update geschrieben. Es zeigt an, dass DomainPrep fertig ist. Abbildung 14-4 zeigt ein Beispiel dafür, wie diese Containerstruktur in ADSI Edit aussieht.

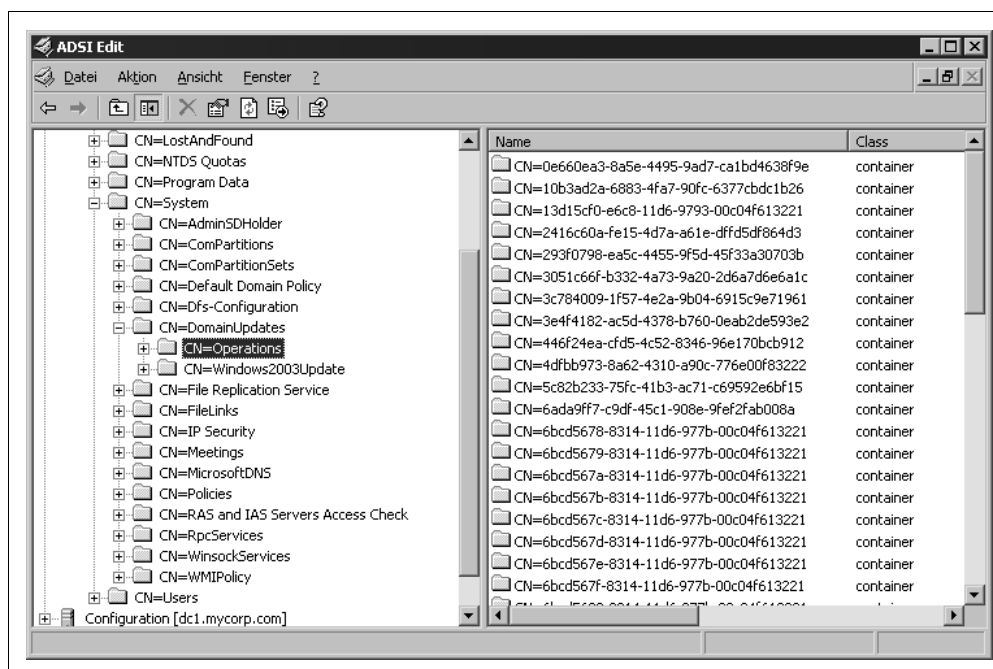


Abbildung 14-4: ADPrep-Operationen zur Domänenaktualisierung

Nachdem Sie die Befehle ForestPrep und DomainPrep gegeben haben und hinreichend Zeit für die Replikation auf alle Domänen-Controller verstrichen ist, können Sie damit beginnen, Ihre Domänen-Controller auf Windows Server 2003 umzustellen oder neue Windows Server 2003-Domänen-Controller zu installieren.

Der Aktualisierungsprozess

Die Aktualisierung auf Windows Server 2003 dürfte in den meisten Fällen keinen großen Aufwand erfordern. Es ist keine Umstrukturierung der Gesamtstruktur erforderlich. Sofern Sie die neusten Service Packs und Hotfixes verwenden, sind auch keine Änderungen der Benutzerprofile oder Arbeitsstationen erforderlich, und es gibt eigentlich keinen Grund für irgendwelche politischen Auseinandersetzungen über den Gebrauch von Namensräumen und über Besitzverhältnisse, wie es vielleicht bei Windows 2000 noch der Fall war.

Wir möchten nun fünf Schritte skizzieren, die Sie bei der Umstellung auf Windows Server 2003 befolgen sollten. Dazu gehört eine Bestandsaufnahme Ihrer Domänen-Controller und Clients, um herauszufinden, ob sich irgendwelche Kompatibilitätsprobleme ergeben. Anschließend sind Sie für einen Probelauf bereit und können sich in ausführlichen Tests vergewissern, welche Auswirkungen die Aktualisierung auf die Funktionalität haben wird. Dann müssen Sie Ihre Gesamtstruktur und Domänen mit ADPrep vorbereiten, das wir bereits besprochen haben. Und schließlich stellen Sie Ihre Domänen-Controller auf Windows Server 2003 um. Im Abschnitt »Nach der Aktualisierung« beschreiben wir, was nach der Aktualisierung der Domänen-Controller zu tun ist, sofern die Überwachung, die Heraufstufung der Funktionsebenen und der Einsatz der neuen Features betroffen sind.

Bestandsaufnahme Domänen-Controller

Ein guter Vorbereitungsschritt vor dem Start des Aktualisierungsprozesses ist eine vollständige Bestandsaufnahme der Hardware und Software auf Ihren Domänen-Controllern. Wahrscheinlich werden Sie auch Ihre Lieferanten kontaktieren, um herauszufinden, ob diese sich bereits mit Kompatibilitätstests beschäftigt haben und Unterstützung für Windows Server 2003 zur Verfügung stellen können. Wer möchte schon den Aktualisierungsprozess starten und auf halbem Wege feststellen, dass eine kritische Überwachungsanwendung oder eine wichtige Backup-Software, die auf den Domänen-Controllern laufen soll, nicht mehr richtig funktioniert. Einen großen Teil dieser Tests können Sie in Ihren eigenen Labors durchführen. Aber es ist nie verkehrt, Kontakt mit den Lieferanten aufzunehmen und deren Zustimmung einzuholen. Sollten sich Probleme ergeben, möchten Sie ja davon ausgehen können, dass Ihre Lieferanten die neue Plattform beherrschen und unterstützen und Sie nicht im Regen stehen lassen.

Anschließend sollten Sie überprüfen, ob Sie alle erforderlichen Hotfixes und Service Packs installiert haben. Im Microsoft Knowledge Base-Artikel 331161 finden Sie eine gute Übersicht über die Empfehlungen aus dem Hause Microsoft. Was Sie installieren müssen, hängt davon ab, wie lange Sie noch Windows 2000-Domänen-Controller einsetzen wollen. Falls Sie eine schnelle Umstellung planen, brauchen Sie nur die Mindestmenge an Korrekturen vorzunehmen. Erstreckt sich die Umstellung aber über einen längeren Zeitraum, sollten Sie in Betracht ziehen, alle aktuellen Fixes und Service Packs zu installieren.

Wenn Sie sich davon überzeugt haben, dass Ihre Hardware und die Software auf einem aktuellen Stand ist und unter Windows Server 2003 funktioniert, sollten Sie Ihre aktuellen Domänen-Controller sorgfältig überprüfen und dafür sorgen, dass sie fehlerfrei arbeiten. Werten Sie die Ereignisprotokolle aus, und beseitigen Sie alle Fehler und alle Ursachen für Warnungen. Die Befehle *dcdiag* und *netdiag* sind bei der Suche nach potenziellen Problemen sehr nützlich. Außerdem müssen Sie damit beginnen, Daten für die CPU- und Speicherstatistik zu erfassen, falls Sie das nicht schon längst tun. Der Grund für diese Datensammlung besteht darin, dass Sie bei Problemen, die sich nach der Umstellung auf Windows Server 2003 zeigen, mit den entsprechenden Daten leichter herausfinden können, ob es sich um ein altes Problem handelt oder um ein neues, das vielleicht durch die Aktualisierung entstanden ist. Wenn Sie diese Daten nicht erfassen und sammeln, handeln Sie sich vielleicht unnötige Schwierigkeiten ein.

Ein guter Kompatibilitätstest ist der Aufruf des Windows Server 2003-Installers (*winnt32.exe*) mit dem Schalter */checkupgradeonly*.

```
X:\> i386\winnt32.exe /checkupgradeonly
```

Dieser Befehl durchläuft alle Schritte wie bei der richtigen Umstellung, überprüft aber nur die installierten Anwendungen und den Zustand der Gesamtstruktur. Wenn Sie ADPrep noch nicht benutzt haben, erhalten Sie eine entsprechende Fehlermeldung.

An diesem Punkt sollten Sie auch den Zustand Ihrer Backups überprüfen. Bevor Sie ADPrep starten, sollten Sie zumindest zwei einwandfreie Backups von mindestens zwei Domänen-Controllern aus jeder Gesamtstruktur und von jedem FSMO-Rolleninhaber vorliegen haben. Sorgen Sie außerdem dafür, dass Ihre Fehlerbeseitigungsprozeduren sorgfältig dokumentiert sind und tatsächlich auch getestet wurden.

Bestandsaufnahme der Clients

Die gute Nachricht, was Clients betrifft, lautet, dass sie nicht viele Anforderungen erfüllen müssen, um in einer Windows Server 2003-Gesamtstruktur arbeiten zu können. Tatsächlich sind auf Windows XP- und Windows 2000-Maschinen keine Änderungen erforderlich. Bei NT 4.0-Clients sollten Sie zumindest den Service Pack 3 installiert haben. Microsoft empfiehlt Service Pack 6a. Windows 98- und Windows 95-Clients setzen die Installation des DS-Client voraus, wie im Microsoft Knowledge Base-Artikel 323466 beschrieben, oder das OS muss auf Windows 2000 oder höher aktualisiert werden (das ist sowieso keine schlechte Idee, wenn Sie es so einrichten können).

Davon abgesehen, können Ihre Clients so bleiben, wie sie sind. Ein vorausschauender AD-Administrator wird natürlich trotzdem dafür sorgen, dass die Clients vor der Aktualisierung sorgfältig getestet werden. Insbesondere bei einer neuen Version von Active Directory warten zweifellos noch einige Probleme auf ihre Entdeckung, und Sie werden vermutlich nicht der Erste sein wollen, der sie erst nach der Aktualisierung bemerkt.

Probelauf

Wir könnten uns zwar den ganzen Tag darüber auslassen, wie einfach der Aktualisierungsprozess ist, aber den Beweis muss die Prozedur eben in der Praxis antreten. Wir halten es für einen sehr wichtigen Schritt, den man keinesfalls auslassen sollte, einen ausführlichen Test mit einer »produktionsähnlichen« Active Directory-Gesamtstruktur durchzuführen, bevor der erste Domänen-Controller aus der Produktionsumgebung auf Windows Server 2003 aktualisiert wird. Was ist mit »produktionsähnlich« gemeint? Das hängt davon ab, wie viel Zeit und Ressourcen Ihnen zur Verfügung stehen. Der beste Weg, Ihre Produktionsumgebung zu simulieren, besteht vielleicht darin, tatsächlich aus jeder Domäne der Gesamtstruktur einen Produktions-Domänen-Controller herauszunehmen und in ein privates Netzwerk einzubauen. Dann können Sie die Gesamtstruktur im privaten Netzwerk nachbilden, und die gesamten Daten aus der Produktionsumgebung befinden sich anschließend auch in der Testumgebung, die Sie gerade eingerichtet haben. Bevor wir diesen Gedanken weiter verfolgen, möchten wir aber darauf hinweisen, dass dies wohl die aufwändigste Option zur Erstellung einer Testumgebung ist, denn Active Directory heilt sich nicht von selbst, nachdem Sie die Domänen-Controller ins private Netz überstellt haben. So könnte es sich zum Beispiel als problematisch erweisen, einen DC überhaupt zum Laufen zu bringen, weil er anfangs keinen Kontakt zu einem der FSMO-Master herstellen kann. Microsoft hat zwar angekündigt, den Prozess vereinfachen zu wollen, und sogar vorgeschlagen zu dokumentieren, wie man es macht, aber zum Zeitpunkt der Veröffentlichung dieses Buchs war noch nichts in dieser Richtung verfügbar. Die Alternative besteht darin, die Test-Gesamtstruktur mit so vielen Daten aus der Produktionsumgebung zu versorgen wie möglich. Falls Sie Ihre Produktionsumgebung bereits durch entsprechende Skripten oder durch ein Metaverzeichnis mit Daten versorgen, können Sie denselben Prozess vielleicht auch für die Testumgebung einsetzen.

Sobald Sie eine Test-Gesamtstruktur mit einer Simulation der Produktionsumgebung eingerichtet haben, sollten Sie so viele Clients wie möglich hinzufügen, wobei alle Betriebssysteme vertreten sein sollten, die Sie auf den Clients einsetzen. Wenn Sie mit Exchange 2000 arbeiten, sollten Sie es ebenfalls installieren, wie auch alle anderen eingesetzten verzeichnisfähigen Anwendungen. Das klingt nach viel Arbeit? Es ist empfehlenswert, alle wichtigen Aspekte auszuprobieren, und zwar unabhängig davon, wie simpel die Aktualisierung nach der Aussage von Microsoft sein wird. Sie wollen ganz sicher nicht, dass es in der Produktionsumgebung ein größeres Desaster gibt und Sie Ihrem Chef dann erklären müssen, dass Sie keine ausführlichen Tests durchgeführt haben, weil Microsoft sagte, die Aktualisierung sei einfach.

Der entscheidende Punkt bei den Probelaufen ist, alles genau zu dokumentieren. Wenn Sie Anomalien entdecken, dokumentieren Sie alles, und versuchen Sie herauszufinden, ob sich daraus ein Problem entwickeln könnte. Wenn Sie mit den Probelaufen fertig sind, sollten Sie ein umfassendes Dokument haben, das beschreibt, wie Sie die Aktualisierung durchführen möchten, wie lange Sie mit der Heraufstufung der Funktionsebenen warten wollen und wann und in welcher Reihenfolge Sie die neuen Features verfügbar machen werden.

Vorbereitung der Gesamtstruktur und der Domänen

Wie bereits erwähnt, müssen Sie den Befehl ADPrep einsetzen, bevor Sie den ersten Windows Server 2003-Domänen-Controller in Ihrer Gesamtstruktur heraufstufen können. Sobald Sie mit der Bestandsaufnahme der DCs und Clients fertig sind und sich keine Hindernisse ergeben haben, sollten Sie ADPrep benutzen.

Zuerst starten Sie ADPrep mit dem Schalter /forestprep. Sobald die Änderungen in der ganzen Gesamtstruktur repliziert wurden, müssen Sie in jeder Domäne ADPrep mit dem Schalter /domainprep aufrufen. Ziemlich einfach, nicht wahr? Allerdings gibt es einige Stolpersteine, die man bei diesem Ablauf vermeiden sollte.

Exchange 2000

Wenn Sie in der Gesamtstruktur vor dem Start von ADPrep Exchange 2000 installieren, müssen Sie einige Fehler korrigieren, die von den Exchange 2000-Schema-Erweiterungen gemacht wurden. Genauer gesagt, ADPrep und Exchange 2000 definieren beide die Attribute labledURI, houseIdentifier und secretary, aber Exchange 2000 benutzt nicht die korrekten LDAP-Anzeigenamen (LDAPDisplayName), wie sie in RFC 2798 definiert werden. Wenn Sie ADPrep benutzen, nachdem Exchange 2000 installiert wurde, und diese Attribute nicht korrigieren, können sich Duplikate von Schema-Objekten ergeben, die verschiedene LDAPDisplayName-Attribute haben. Zur Lösung des Problems müssen Sie die Datei *inetorgpersonfix.ldf* aus dem Verzeichnis `\support\tools\support.cab` starten. Diese LDIF-Datei korrigiert die LDAPDisplayName-Attribute dieser drei Attribute.

Zuerst speichern Sie die Datei *inetorgpersonfix.ldf* und importieren sie dann mit dem Hilfsprogramm *ldifde*. Im folgenden Beispiel importieren wir die Datei in die Gesamtstruktur *mycorp.com*:

```
ldifde.exe /i /f inetOrgPersonFix.ldf /c "DC=X" "DC=mycorp,DC=com"
```

Beachten Sie bitte, dass *inetorgpersonfix.ldf* als Pfad für die Gesamtstruktur DC=X benutzt. Diesen Pfad ersetzen wir mit Hilfe des Schalters /c durch unseren eigenen Gesamtstrukturpfad.

SFU 2.0

Falls Sie in Ihrer Windows 2000-Gesamtstruktur die Microsoft Services for UNIX (SFU) 2.0 installiert haben, können sich ähnliche Probleme ergeben, wie gerade für Exchange 2000 beschrieben. Das Problem zeigt sich wieder an einem falsch definierten Attribut. In diesem Fall handelt es sich um das Attribut uid. Microsoft hat dafür einen Hotfix entwickelt, der im Microsoft Knowledge Base-Artikel 293783 beschrieben wird.



Das gilt nur für SFU 2.0. Wenn Sie mit SFU 3.0 arbeiten, tritt dieses Problem nicht auf.

Aktualisierung der Domänen-Controller

Nun kommt der einfache Teil. Vielleicht fragen Sie sich, wieso wir behaupten können, dass die Aktualisierung der einfache Teil sei. Wir sollten wohl Folgendes vorausschicken: Wenn Sie Ihre Hausaufgaben gemacht haben, wird dies der einfache Teil sein. Die harte Arbeit steckt in der Bestandsaufnahme der DCs und Clients, in der Abklärung der Kompatibilitätsfragen, der Überwachung, der Prüfung der Ereignisprotokolle, in der Ausarbeitung eines realistischen Zeitplans, in der Durchführung von Testaktualisierungen und so weiter. Wenn Sie dann endlich so weit sind, tatsächlich die Aktualisierungen in der Produktionsumgebung durchführen zu können, sollte der Ablauf Ihnen praktisch zur zweiten Natur geworden sein.

Sie können die Aktualisierung so schnell vorantreiben oder so langsam durchführen, wie Sie möchten. Windows Server 2003-Domänen-Controller sind zu Windows 2000-Domänen-Controllern vollständig kompatibel. Die Domänen-Controller können auch jede Rolle in der Gesamtstruktur übernehmen und zum Beispiel als Server für den Globalen Katalog dienen, als FSMO-Master, als ISTG oder als Bridgehead-Server.

Nach der Aktualisierung

Nachdem Sie einen oder mehrere Ihrer Domänen-Controller auf Windows Server 2003 umgestellt haben, müssen Sie zum Abschluss der Aktualisierung noch einige zusätzliche Arbeiten durchführen. Zuerst und vor allem müssen Sie die Domänen-Controller auf jedem Schritt des Wegs überwachen, insbesondere natürlich nach ihrer Aktualisierung. Sie öffnen Schwierigkeiten Tür und Tor, wenn Sie Active Directory nicht angemessen überwachen.

Überwachung

Die Bedeutung einer ausreichenden Überwachung lässt sich kaum genug betonen. Wie finden Sie heraus, ob etwas während der Aktualisierung falsch gelaufen ist, wenn Sie die Systeme nicht überwachen? Die folgende Liste nennt einige Punkte, die Sie überprüfen sollten, nachdem Sie den ersten Domänen-Controller in der Domäne oder einen FSMO-Rolleninhaber aktualisiert haben oder nachdem Sie die Aktualisierung aller DCs abgeschlossen haben:

Reaktion aller Dienste

Überprüfen Sie LDAP, Kerberos, GC (sofern installiert) und DNS (sofern installiert), und überzeugen Sie sich davon, dass die Authentifizierungen und Anmeldungen bearbeitet werden. Der Befehl `dcdiag` kann viele dieser Tests ausführen.

Prozessor- und Speicherauslastung

Erfassen Sie die Prozessor- und Speicherauslastung bereits vor der Aktualisierung, damit Sie nach der Aktualisierung Vergleichszahlen haben.

DIT-Wachstum

Die DIT sollten nur unwesentlich wachsen. Vielleicht führen Sie nach der Aktualisierung sowieso eine Offline-Defragmentierung durch, um den Speicherplatz zurückzugewinnen, der durch die Speicherung der ACLs in jeweils nur einer Instanz frei geworden ist.

Ereignisprotokolle

Das ist nicht schwierig, aber wichtig. Überprüfen Sie immer alle Ereignisprotokolle auf erfasste Fehler.

Registrierte DC-Ressourcendatensätze

Sorgen Sie dafür, dass die SRV-, CNAME- und A-Datensätze für die Domänen-Controller registriert sind. Diese Überprüfungen kann der Befehl *dcdiag* erledigen.

Funktioniert die Replikation?

Geben Sie die Befehle *repadmin /showreps* und *repadmin /replsum*, und achten Sie auf ungewöhnliche Anzeigen.

Werden Gruppenrichtlinien angewendet?

Vielleicht möchten Sie ein vorhandenes GPO mit neuen Werten versehen und überprüfen, ob diese Werte auf einem Client, der sie erhalten soll, auch tatsächlich angewendet werden.

Existieren NETLOGON und SYSVOL?

Dieser Test könnte zum Beispiel darin bestehen, ein Explorer-Fenster zu öffnen und auf dem Domänen-Controller zu den verfügbaren freigegebenen Verzeichnissen zu navigieren.

Repliziert FRS korrekt?

Das finden Sie heraus, indem Sie auf einem Domänen-Controller eine Testdatei im SYSVOL-Verzeichnis ablegen und überprüfen, ob die Datei auf andere Domänen-Controller repliziert wird.

Das ist keine vollständige Liste aller Punkte, die Sie überprüfen sollten, aber ein guter Anfang. Wenn über eine Woche hinweg keine ernsthaften Probleme auftreten, können Sie wahrscheinlich davon ausgehen, dass die Aktualisierung erfolgreich verlaufen ist. Solange Sie die Ereignisprotokolle gut im Auge behalten, sollten Sie eigentlich die meisten Probleme erkennen.

Erhöhung der Funktionsebenen

Sobald Sie überzeugt sind, dass die Aktualisierungen erfolgreich verlaufen sind, sollten Sie im nächsten Schritt damit beginnen, die Funktionsebenen zu erhöhen. Wenn Sie nur die Domänen-Controller in einer einzigen Domäne aktualisiert haben, können Sie die Funktionsebene für diese Domäne auf Windows Server 2003 erhöhen. Wenn Sie alle Domänen-Controller in der Gesamtstruktur aktualisiert haben, können Sie auch die Funktionsebene der Gesamtstruktur auf Windows Server 2003 erhöhen.



Falls Sie auf der sicheren Seite bleiben möchten und es mit mehreren Domänen zu tun haben, bietet es sich an, nur die Funktionsebene einer einzigen Domäne anzuheben und die Überwachung eine weitere Woche fortzuführen, bevor Sie die Funktionsebene der Gesamtstruktur erhöhen.

Nach der Erhöhung der Funktionsebene von einer Domäne oder der Gesamtstruktur sollten Sie bei der Überwachung der Systeme auch die neuen Features von Windows Server 2003 berücksichtigen. Zum Test der Domänenfunktionsebene Windows Server 2003 sollten Sie sich auf einem Domänen-Controller anmelden und sich das `lastLogonTimestamp`-Attribut Ihres Benutzerobjekts ansehen, über das wir in diesem Kapitel bereits gesprochen haben. Dieses neue replizierte Attribut gibt Ihre Anmeldezeit an. Falls Sie nach einer gewissen Zeit feststellen, dass das Attribut immer noch keinen gültigen Wert hat, müssen Sie wohl etwas tiefer graben und der Sache auf den Grund gehen.

Der vielleicht einfachste Test, mit dem man herausfinden kann, ob für eine Domäne oder eine Gesamtstruktur eine Funktionsebene festgelegt wurde, besteht darin, das `RootDSE` abzufragen und die Attribute `domainFunctionality` und `forestFunctionality` zu untersuchen. Der Wert 2 bedeutet, dass sich die Domäne oder die Gesamtstruktur auf der Funktionsebene Windows Server 2003 befindet.

Anpassung der Einstellungen

Nach der Definition der Funktionsebenen werden Sie vermutlich alle Einstellungen ändern, deren Werte bei den Tests von der gewünschten Konfiguration abweichen. Besonders wichtig ist die Konfiguration der Sicherheit und der Kontensperrung. Wenn Sie die SMB-Signatur abschalten möchten, können Sie das über die Gruppenrichtlinien unter *Domänen-Controller Sicherheitsrichtlinien* → *Windows-Einstellungen* → *Sicherheitseinstellungen* → *Lokale Richtlinien* → *Sicherheitsoptionen* → *Kommunikation digital signieren* tun.

Windows 2000 Active Directory-Administratoren hatten Probleme mit Kontensperrungen. Die Bugfixes aus den Service Packs 2 und 3 werden auch in Windows Server 2003 berücksichtigt. Sie sollten die Einstellungen für die Kontensperrung und den Verfall der Kennwörter überprüfen. Microsoft hat die entsprechenden Empfehlungen in einer Security Configuration Template-Datei zusammengefasst, die auf einem Windows Server 2003-Domänen-Controller unter `%SystemRoot%\security\templates\SECURED.C` zu finden ist.

Wenn Sie irgendwelche Werte in der Registrierung eines Domänen-Controllers abspeichern mussten, sollten Sie überprüfen, ob Sie diese Werte noch brauchen. Zum Beispiel haben viele Leute die standort-interne Replikationsfrequenz von 5 Minuten auf 15 bis 60 Sekunden erhöht. Unter Windows Server 2003 wurde die Standardfrequenz auf 15 Sekunden geändert.

Implementierung neuer Features

Nachdem Sie Ihre Domänen-Controller aktualisiert und die Funktionsebene einer Domäne oder Gesamtstruktur erhöht haben, können Sie damit beginnen, die neuen Features einzusetzen. Einige können Sie sofort benutzen, wie zum Beispiel die MMC- und CLI-Erweiterungen. Bei anderen sollten Sie genauer überlegen, wie sie implementiert werden, zum Beispiel bei Kontingenten. Außerdem empfiehlt es sich, solche Features genau zu dokumentieren und mit den Kollegen abzusprechen, bevor Sie damit arbeiten. Wenn Sie AD-integrierte DNS-Zonen benutzen, sollten Sie über den Umstieg auf Anwendungspartitionen zur Speicherung der DNS-Daten nachdenken. Diese Konvertierung lässt sich mit dem DNS MMC-Snap-In durchführen und ist relativ einfach. In manchen Fällen kann es erforderlich werden, die aktuelle Vorgehensweise völlig neu zu durchdenken. Wenn Sie zum Beispiel damit beginnen, mit dem Feature »Installieren von Medium« zu arbeiten, ändert sich vielleicht die Art und Weise, in der Sie Domänen-Controller aufbauen und einsetzen.

Zusammenfassung

In diesem Kapitel haben wir uns mit den neuen Features von Windows Server 2003 und mit einigen Unterschieden zu Windows 2000 beschäftigt, die sich meistens aus Praxisanforderungen ergeben haben. Dann haben wir besprochen, wie man die neuen Features mit Hilfe von Funktionsebenen freischalten kann und warum Funktionsebenen wichtig sind. Dann sind wir auf den ADPrep-Prozess eingegangen, der erforderlich ist, bevor Sie den ersten Windows Server 2003-Domänen-Controller heraufstufen können. Sobald die Gesamtstruktur und die Domänen vorbereitet sind, können Sie mit der Aktualisierung beginnen. Wir haben einige der Punkte beschrieben, die bei der Aktualisierung wichtig sind, und sind auch darauf eingegangen, was nach dem Abschluss der Aktualisierung noch zu tun ist.

Während sich dieses Kapitel auf die Aktualisierung einer vorhandenen Windows 2000 Active Directory-Infrastruktur konzentriert hat, besprechen wir im nächsten Kapitel die wichtigsten Probleme, die sich beim Umstieg von Windows NT auf Windows Server 2003 Active Directory ergeben können.