Die Sache mit dem Verzeichnis

11

In diesem Kapitel

- Verstehen eines Verzeichnisdienstes
- Vorstellen des Windows 2000 Active Directories
- Planen für Active Directory
- Installieren von Active Diretory
- Umgehen mit mehreren Domänen

In diesem Kapitel sehen wir uns die einzige große Änderung in Windows 2000 an: die Implementierung eines Active Directory genannten Verzeichnisdienstes. Sie werden herausfinden, was ein Verzeichnisdienst ist und warum Sie einen haben wollen, außerdem wie Sie die Installation vom neuen Active Directory planen und durchführen. Es mag zwar nicht die größte Sache seit der Erfindung geschnittenen Brotes sein, aber es ist mindestens so gut wie gesalzene Kartoffelchips!

Viele von Ihnen sind bereits mit den auf NetBIOS basierenden Domänen von Windows NT vertraut. Möglicherweise fühlen Sie sich sogar sicher in deren Benutzung und und Implementierung. Aber wie das alte Microsoft-Sprichwort so schön sagt: »Es ist Zeit, all das neu zu lernen, was Sie bereits wissen.«

Was ist ein Verzeichnisdienst?

Sie werden es vielleicht nicht wissen, aber Sie nutzen Verzeichnisdienste schon die ganze Zeit. Wenn Sie hungrig nach Pizza sind, schnappen Sie sich ein Telefonbuch und schlagen unter P nach. Das Telefonbuch ist eine Art Verzeichnisdienst, denn es beinhaltet die Informationen, die Sie brauchen, und offeriert einen Weg, diese Informationen zu finden (In diesem Fall ist es eine alphabetische Sortierung). Ein computerisierter Verzeichnisdienste arbeitet auf vielen Wegen genauso: Er beinhaltet Informationen über zahlreiche Aspekte Ihres Unternehmens, organisiert diese Informationen und offeriert ein oder mehrere Werkzeuge, die beim Erforschen dieser Informationen helfen.

Windows 2000 ist nicht das ersten Betriebssystem, das Verzeichnisdienste anbietet. Novells NetWare beinhaltet die *Novell Directory Services* (NDS) bereits seit 1993, beginnend mit NetWare 4. Tatsächlich ist eine Version der NDS sogar für Windows NT und Windows 2000 verfügbar. Windows 2000 ist allerdings die erste Version eines Windows-Betriebssystems, das über einen eingebauten Verzeichnisdienst verfügt, nämlich Active Directory. Microsoft baut

die gesamte Windows 2000-Domänenstruktur rund um Active Directory auf, statt sie einfach als Add-On für vorangegangene Domänenimplementatierungen anzubieten.

Wenn es um Namen geht, ist Microsoft irgendwie besessen von dem Wort *Active*. Da gibt es Active Desktop, Active X und jetzt Active Directory. Aber der Name ist zutreffend, denn schließlich ist Active Directory aktiv (wenn es denn korrekt eingesetzt wird).

Treffen Sie Active Directory

Um seinen Job korrekt auszuführen, muss ein Verzeichnisdienst drei primäre Anforderungen erfüllen:

- ✔ Er muss eine Struktur zur Organisation und Speicherung der Verzeichnisdaten beinhalten.
- ✔ Er muss der Abfrage und dem Management der Daten eine Bedeutung geben.
- ✔ Er muss eine Methode zur Verfügung stellen, um Verzeichnisdaten sowie Netzwerk- und Serverressourcen, die mit diesen Daten korrespondieren, zu finden. Wenn die Verzeichnisdaten beispielsweise Zeiger (Pointer) auf eine Datei und einen Drucker beinhalten, muss der Verzeichnisdienst wissen, wo sich diese Dinge befinden und wie darauf zugegriffen wird.

Active Directory erfüllt diese Anforderungen mit verschiedenen Technologien. Für weitere Informationen über Active Directory schnappen Sie sich eine Exemplar von *Active Directory für Dummies* von Marcia Loughry.

Daten speichern und organisieren

Die Struktur ist unter Verwendung des *ISO X.500-Protokolls* implementiert (ISO steht für *International Organization for Standardization*). Abbildung 11.1 zeigt die hierarische Struktur eines X.500-Verzeichnisses. Es handelt sich dabei um einen sehr üblichen Standard, der in den meisten Verzeichnisdiensten verwendet wird, einschließlich Microsofts Active Directory, aber auch in Novells NDS, in Netscape-Produkten und anderen Implementierungen. X.500 hat sich als sehr nützlich für diese Applikation erwiesen, weil es Daten hierarchisch organisiert und die Verzeichnisinformationen einer Organisation auf zahlreiche nützliche Container oder Behälter aufteilt, beispielsweise Länder, Organisationseinheiten, Untereinheiten und Ressourcen. Unser Beispiel in Abbildung 11.1 organisiert das Verzeichnis runter zu den Benutzerobjekten.

Heute werden üblicherweise zwei X.500-Standards eingesetzt: der 1988- und der 1993-X.500-Standard. Die Version 1993 beinhaltet eine Anzahl von Vorteilen gegenüber der älteren Version 1988. Glücklicherweise ist die Version 1993 die Version, auf deren Grundlage Microsoft ihr Active Directory gebaut hat.

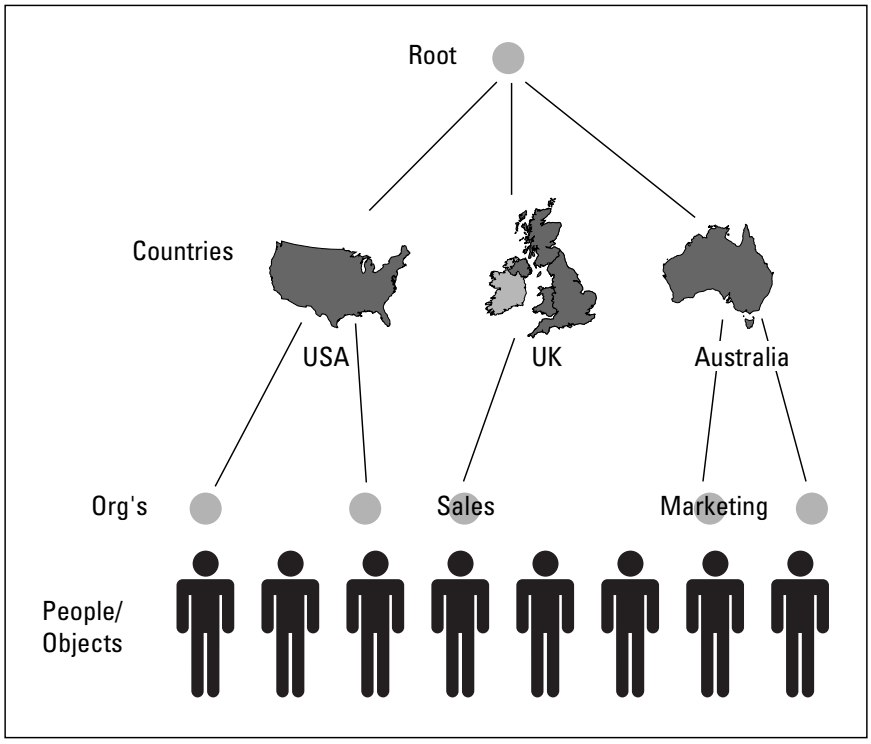

Abbildung 11.1: Die hierarchische Struktur eines X.500-Verzeichnisses

Daten managen

Ein spezielles, auf TCP/IP basierendes Protokoll, das *Lightweight Directory Access Protocol* (LDAP), bietet die zweite Zutat für den Active Directory-Dienst. Wie der lezte Teil seines Namens bereits vermuten lässt, ist LDAP speziell für die Abfrage von und den Zugriff auf Verzeichnisdaten entwickelt worden. Der Lightweight-Teil im Namen stammt von der Tatsache ab, dass es sich bei diesem Protokoll um eine gestrippte Version eines älteren, mächtigeren X.500-DAPs handelt.

Diese Terminologie ist sicher denen geläufig, die bereits mit dem Microsoft Exchange Server-Verzeichnisdienst herum experimentiert haben, weil der Active Directory-Dienst von Windows 2000 sich mit dem Exchange-Server-Verzeichnisdienst eine gemeinsame Technologie teilt.Tatsächlich steht im Windows 2000 Server ein Exchange-Konnektor zur Verfügung, um die beiden Verzeichnisdienste miteinander zu Verbinden und um Daten zwischen ihnen zu replizieren. Nicht überraschend heißt diese Komponente Active Directory Connector.

Daten und Ressourcen finden

Auch wenn Windows 2000 Verzeichnisdaten mit dem X.500-Protokoll strukturiert und auf diese Daten mit LDAP zugegriffen wird, muss es immer noch einen Weg geben, diese Daten zu finden. Zeit für die noch fehlende dritte Zutat! Wie entspricht Active Directory der dritten und letzten Anforderung für einen funktionierenden Verzeichnisdienst? Wir freuen uns, dass Sie gefragt haben. Active Directory stützt sich auf einen sehr gut bekannten und weit verbreiteten Internetstandard mit dem Namen *Domain Name System* (DNS), den es als Locatordienst verwendet.

Von Domänen und Controllern

Hinter jeder großartiger Domäne verbirgt sich ein großartiger Domänencontroller (so geht der Song von Aretha Franklin), aber bevor Sie sich ansehen, wie Windows 2000 Domänencontroller verwendet, steht ein kurzer Blick auf die Windows NT 4.0-Verwendung im Programm. Denken Sie aber daran, dass sich die Art und Weise, in der Windows NT mit Domänencontrollern umgeht, ein ganzes Stück von der Art und Weise unterscheidet, in der Windows 2000 die Dinge angeht. Das liegt hauptsächlich an Active Directory.

Am Anfang war...

Bei Windows NT 4.0 repräsentieren 15 Zeichen lange NetBIOS-Namen Domänen. Tatsächlich ist bei diesen Namen ein sechzehntes Zeichen ein unsichtbares Spezialzeichen <1C>, das besagt, dass es sich um den Namen einer Domäne handelt. Solche Domänen drehen sich um eine gemeisame Benutzer/Gruppen/Richtlinien-Datenbank, die in einem schreibbaren Format auf einem einzelnen, primären Server gespeichert ist, der als *primärer Domänencontroller* (PDC) bekannt ist.

Jedes Modell, das auf einem einzelnen Domänencontroller basiert, führt einen *Single Point of Failure* (einen einzelnen Fehlerpunkt) ein. Da aber der Zugriff auf die Domänendatenbank notwendig ist, um auf die Ressourcen der Domänen zuzugreifen, fügt Microsoft einen zweiten Servertypen hinzu, der als *Sicherungsdomänencontroller* (BDS) bekannt ist, um die Verfügbarkeit und Zuverlässigkeit der Domänen zu verbessern. Ein BDC speichert eine Nur-Lesen-Version der Domänendatenbank, die manchmal *Security-Accounts-Manager*-(SAM-)Datenbank oder Sicherheitskontenmanager-Datenbank genannt wird. Benutzer können auf einen BDC zugreifen, um sich anzumelden und um Benutzer, Gruppen und Kontoinformationen zu erforschen, aber Änderungen der Datenbank können ausschließlich auf dem PDC durchgeführt werden.

Bei dieser Variante einer Domänenumgebung muss der PDC periodisch die SAM-Datenbank auf allen BDCs in seiner Domäne aktualisieren, um sie synchron zu halten. Sollte ein PDC jemals ausfallen, kann ein BDC zum PDC mit einer beschreibbaren Kopie der SAM-Datenbank promotet werden. Es existiert jedenfalls eine nicht brechbare Master/Slave-Beziehung zwi-

schen PDCs und BDCs, da Änderungen der SAM-Datenbank auf dem PDC durchgeführt werden müssen und der PDC sie zu allen BDCs zu kopieren hat. Deshalb können keine Änderungen der SAM-Datenbank durchgeführt werden, wenn der PDC ausfällt, bis er wieder hergestellt ist oder ein BDC seine Rolle übernommen hat. Wow! Haben Sie's?

Obwohl das wie eine Form von Unterjochung klingt, bedeutet eine Master/Slave-Beziehung in Computerspeak »Alle Änderungen auf dem Master werden auf alle Slaves kopiert« und »Nur der Master kann Änderungen akzeptieren und sie zu den Slaves kopieren.«

Windows 2000 verwendet nicht länger NetBIOS, um seine Domänen mit Namen zu versehen; stattdessen verwendet es das Domain Name System (DNS), Sehen Sie sich bitte Kapitel 14 für weitere Informationen über DNS an.) Deshalb haben Sie statt des familiären »Dummies«-Domänennamen so etwas wie `sales.dummies.com` als legalen Domänennamen. Das Konzept der SAM wird in Windows 2000-Domänen auch nicht mehr verwendet. Alle Informationen über Benutzer, Kennwörter und Gruppen werden im Active Directory gespeichert. Statt Server, die in die SAM schreiben und daraus lesen können, müssen Server nun den LDAP-Dienst verwenden, der als Schnittstelle zu Active Directory dient.

In einem Windows 2000-Netzwerk sind die Server, die den LDAP-Dienst beheimaten, die Domänencontroller. Genau wie in Windows NT-basierten Netzwerken sind diese Server für die Authentisierung und andere Domänenaktivitäten verantwortlich. In Windows 2000-Netzwerken verwenden Server allerdings Active Directory zur Bereitstellung der Dienste, die ihre älteren Gegenstücke über die SAM-Datenbank angeboten haben.

Was ist aus PDCs und BDCs geworden?

Das Konzept der PDCs und BDCs ist aus Windows 2000 entfernt worden. In dieser tollen neuen Welt sind alle Domänencontroller gleich (obwohl einige tatsächlich etwas gleicher sind als andere). Wie wird diese Gleichheit gepflegt? Ein als *Multimaster-Replikation* bekannter Prozess stellt sicher, dass Änderungen auf einem Domänencontroller auf alle anderen Domänencontroller dieser Domäne repliziert werden. Statt der alten Master/Slave-Beziehung haben Sie es nun mit einer Peer-to-Peer-Beziehung zwischen allen Domänencontrollern in einer Windows 2000-Domäne (und dahinter) zu tun, in der Vertrauensstellungen existieren. Eine Vertrauensstellung ist ein spezielles Inter-Domänen-Zugriffsarrangement, dass Sie definieren, wenn Benutzer einer Domäne Zugriff auf Ressourcen einer anderen Domäne benötigen.

Offensichtlich werden Sie nicht dazu in der Lage sein, alle Domänencontroller von Windows NT 4.0 auf Windows 2000 in einem Rutsch aufzurüsten. Darum erlaubt Ihnen der Windows 2000 Server Domänen im *gemischten Modus* zu betreiben. Das erlaubt Windows NT-BDCs (aber keinem PDC) in einer Windows 2000-Domäne mitzuspielen. Die Idee, die dahinter steckt: Sie beginnen mit der Aktualisierung oder Aufrüstung der PDCs und machen dann mit der Aktualisierung der BDCs weiter, bis alle Domänencontroller konvertiert sind.Damit ein Windows NT 4.0-BDC funktioniert, muss er Updates von einem PDC beziehen können. Darum

übernimmt in Domänen im gemischten Modus ein einzelner Windows 2000-Domänencontroller die Aufgaben eines Windows NT 4.0-PDCs, wodurch Änderungen zu jedem Windows NT 4.0-BDC der Domänen repliziert werden können.

In Domänen im gemischten Modus können Clients NetBIOS-Namen für den Zugriff auf altmodische Domänendienste verwenden, oder sie nutzen Active Directory für den Zugriff auf Windows 2000-Domänendienste. Um einen Windows 2000-Domänencontroller zu finden, müssen die Clients von einem DNS-Server einen Service-Record anfordern, der die generelle Form `ldap_.tcp-<Domänenname>` hat, wobei beispielsweise `ldap.tcp.dummies.com` einen Domänencontroller für die Domäne `dummies.com` repräsentieren würde.

Windows 2000-Domänencontroller brauchen den DNS-Dienst nicht selbst ausführen. Die einzige Anforderung ist, dass die benutzten DNS-Server den Service-Record-Typen unterstützen, damit solche Domänen gefunden werden.

Wie funktioniert Active Directory?

Um die Dinge in einer Art Techno-Nussschale zusammenzufassen: Active Directory ist unter Verwendung einer X.500-Struktur für Verzeichnisdaten implementiert, nutzt eine LDAP-Schnittstelle für den Zugriff auf Verzeichnisdaten und DNS als Locatormechanismus für Verzeichnisdaten. So, jetzt wo Sie dieses ganze Zeug über Active Directory wissen, was bringt Ihnen das? Die folgende Liste zeigt einige der Hauptfeatures und Vorteile von Active Directory:

- ✔ **Sicherheit:** Informationen sind in einer sicheren Form gespeichert. Jedes Objekt im Active Directory besitzt eine *Access Control List* (ACL) oder *Zugriffssteuerungsliste*, die eine Liste der Ressourcen enthält, die auf sie zugreifen können, und die Zugriffsprivilegien jeder dieser Ressourcen.
- ✔ **Abfragefähigkeiten:** Active Directory generiert einen *globalen Katalog*, um einen flexiblen Mechanismus für die Bearbeitung von Abfragen anzubieten. Jeder Client, der Active Directory unterstütz, kann diesen Katalog abfragen, um Verzeichnisdaten anzufordern.
- ✔ **Replikation:** Die Replikation des Verzeichnisses auf alle Domänencontroller bedeutet einfacheren Zugriff, höhere Verfügbarkeit und verbesserte Fehlertoleranz.
- ✔ **Erweiterbarkeit:** Active Directory ist *erweiterbar*, was bedeutet, dass einem Verzeichnis neue Objekttypen hinzugefügt oder existierende Objekte *erweitert* werden können. Sie könnten beispielsweise sehr einfach einem Benutzerobjekt eine Angestellten-ID oder ein Gehaltsattribut hinzufügen.
- ✔ **Mehrere Protokolle:** Die Kommunikation zwischen Verzeichnisservern oder über Verzeichnisse verschiedener Hersteller kann zahlreiche Netzwerkprotokolle verwenden, weil Active Directory auf einem X.500-Fundament aufbaut. Diese Protokolle beinhalten aktuell LDAP Version 2 und 3 sowie das *Hypertext Transfer Protocol* (HTTP). Dritthersteller können diese Fähigkeit für die Verwendung weiterer Protokolle erweitern, falls sie es brauchen.

✔ **Partitionierung:** In einer Active Directory-Umgebung können Informationen auf Domänen partitioniert werden, um die Replikation großer Mengen von Verzeichnisdaten zu vermeiden. Jede solche Domäne wird *Tree* bzw. *Baum* genannt, was an der Art und Weise liegt, in der X.500 Verzeichnisdaten in eine untereinander verbundende Hierarchie mit einer einzigen Wurzel (Root) strukturiert. Eine Sammlung von Domänen formt eine Gruppe von Trees, die man – richtig geraten – *Forest* nennt. Für die deutsche Sprache hat Microsoft den weniger schönen Begriff *Gesamtstruktur* erfunden.

Wenn Sie Active Directory-Daten in verschiedene (Domänen-)Bäume partitionieren, bedeutet das nicht, dass Active Directory nicht nach Informationen anderer Domänen abgefragt werden kann. *Globale Kataloge* beinhalten eine Untermenge von Informationen über jedes Objekt der kompletten Gesamtstruktur, wodurch Abfragen in der Gesamtstruktur durchführbar sind, unterstützt durch Ihren freundlichen lokalen Domänencontroller.

Was Replikation bedeutet

In einer Windows 2000-Domäne sind alle Domänencontroller gleich. Wenn Sie Änderungen auf irgendeinem Domänencontroller durchführen, müssen deshalb die gesamten Verzeichnisse aller anderen Domänencontroller aktualisiert werden, damit sie die Änderungen übernehmen. Das wird mit Hilfe eines *Multimaster-Replikation* genannten Prozesses durchgeführt.

So funktioniert die Sache: Jedes Objekt im Active Directory auf jedem Domänencontroller besitzt ein Attribut, das *Update Sequence Number* (USN) genannt wird. Jedesmal, wenn eine Änderung an Active Directory-Daten durchgeführt wird, erhöht der Server, auf dem die Änderung durchgeführt wird, seine USN um 1, gemeinsam mit den USNs jedes geänderten Objekts. Diese Änderungen müssen dann auf alle Domänencontroller der Domäne repliziert werden. Hier bietet die USN den Schlüssel für die Multimaster-Replikation.

USN-Erhöhungen sind *atomare Operationen*. Auf Deutsch heißt das, dass die Erhöhung des Wertes einer USN (und die aktuelle Änderung von Verzeichnisdaten) zur gleichen Zeit erfolgt. Schlägt ein Teil fehl, dann schlägt die gesamte Änderung fehl. Deshalb ist es nicht möglich, ein Active Directory-Objekt zu ändern, ohne dessen USN zu erhöhen. So geht eine Änderung niemals verloren. Jeder Domänencontroller verfolgt die höchsten USNs der anderen Domänencontroller, mit denen er repliziert. Dies erlaubt dem Domänencontroller zu berechnen, welche Änderungen während jedes Replikationskreislaufs zu replizieren sind. Mit den einfachsten Worten: Die höchste USN gewinnt immer!

Am Anfang jedes Replikationskreislaufs prüft jeder Domänencontroller seine eigene USN-Tabelle und fragt alle anderen Domänencontroller, mit denen er repliziert, nach deren letzten USNs ab. Tabelle 11.1 zeigt als Beispiel die USN-Tabelle des Servers A.

Domänencontroller	USN
DC B	54
DC C	23
DC D	53

Tabelle 11.1: Die USN-Tabelle von Server A

Server A fragt die Domänencontroller auf deren aktuelle USNs ab und erhält die in Tabelle 11.2 gezeigten Resultate.

Domänencontroller	USN
DC B	58
DC C	23
DC D	64

Tabelle 11.2: Aktuelle USNs der anderen Domänencontroller

Mit diesen Daten berechnet Server A die Änderungen, die er von jedem Server benötigt, wie in Tabelle 11.3 gezeigt.

Domänencontroller	USN
DC B	55, 56, 57, 58
DC C	zu erneuern
DC D	54 – 64

Tabelle 11.3: Die Änderungen, die Server A von jedem anderen Server benötigt

Nun würde Server A die benötigten Änderungen von den anderen Servern anfordern.

Da Objekte Eigenschaften haben, haben sie auch *Property Version Numbers* (PVNs) (Eigenschaftsversionsnummern). Jede Eigenschaft eines Objekts hat eine PVN und jedesmal, wenn eine Eigenschaft modifiziert wird, wird auch die PVN um 1 erhöht. Klingt das irgendwie bekannt? Diese PVNs werden zum Erkennen von Kollisionen verwendet, die vorkommen, wenn mehrere Änderungen derselben Eigenschaft zur gleichen Zeit durchgeführt werden. Falls es zu einer Kollision kommt, besitzt die Änderung mit der höchsten PVN die höchste Priorität.

Sind die PVNs identisch, löst eine *Zeitmarke* (Time Stamp) einen solchen Konflikt. Zeitmarken sind eine großartige zweite Verteidigungslinie zur Bekämpfung von Kollisionen, da sie exakt kennzeichnen, wann jede Änderung der Verzeichnisdaten durchgeführt wurde. Dadurch wird dem System ermöglicht zu entscheiden, welche Änderung höchste Priorität besitzt und durchzuführen ist. Denken Sie aber daran, dass Zeitmarken nur dann ihren Job korrekt erledigen können, wenn die Domänencontroller in Ihrem Netzwerk genau miteiander

synchronisiert sind. Übernehmen Sie also einen Tipp aus alten Kriegsfilmen und synchronisieren Sie ihre Domänencontroller!

In dem höchst unwahrscheinlichen Fall, dass sowohl die PVNs als auch die Zeitmarken identisch sind, wird ein binärer Puffervergleich durchgeführt, aus dem der größte Puffer als Sieger hervorgeht. PVNs werden nur durch das originale Schreiben und nicht durch das Replikationsschreiben erhöht (anders als USNs). PVNs sind nicht Server-spezifisch, reisen aber gemeinsam mit der Objekteigenschaft.

Ein spezielles Schema wird verwendet, um zu vermeiden, dass Änderungen wiederholt zu anderen Servern gesendet werden. Dieses von Windows 2000 genutzte Schema verhindert logische Loops (Kreisläufe) in der Active Directory-Struktur, die zur endlosen Wiederbelebung von Updates führen, und redundante Übertragungen von Updates zu bereits aktualisierten Servern zur Folge haben könnten. Konsequenterweise führt jeder Server eine Tabelle mit Up-to-Date-Vektoren, welche die höchsten von jedem Domänencontroller empfangenen Writes (sinngemäß Schreibungen) repräsentieren. Diese Vektoren besitzen folgende Form:

```
<Änderungsinformation >, <Name des Domänencontrollers, der die
        Originaländerung durchgeführt hat>, <USN für die Änderung>
```

Ein Beispiel dazu:

```
<object savillj>, property Password xxx>, Titanic,54
```

Dies repräsentiert eine Änderung des Kennwortwertes für das Objekt `savillj` auf dem Domänencontroller `Titanic` mit einer USN von 54.

Domänencontroller senden solche Informationen mit ihren USNs, so dass sie berechnen können, ob sie die Änderung bereits durchgeführt haben, die ein andere Domänencontroller versucht zu replizieren.

Die großen Schema-Dinge

Jedes Objekt in einer Domäne besitzt ein *Schema*, das eine Art Diagramm der Objektcharakteristika ist. Mit anderen Worten: Wenn Objekte erzeugt werden, werden ihnen automatisch bestimmte Attribute zugeordnet. Ein Benutzerobjekt besitzt beispielsweise Attribute wie Name, Adresse und Telefonnummer. Die Sammlung dieser Attribute und deren Definitionen wird Schema genannt. Sie können sich das Schema eines Objekts auch als Wäscheliste oder als Checkliste seiner Fähigkeiten vorstellen. Das Defaultschema stellt Definitionen für Benutzer, Computer, Domänen und mehr zur Verfügung. Sie können pro Domäne und Objekt nur ein Schema haben und sie können nicht mehrere Definitionen für dasselbe Objekt haben.

Die Default-Schemadefinition ist in der Schema.Ini-Datei definiert, die außerdem die initiale Struktur der Ntds.Dit-Datei enthält, die Active Directory-Daten speichert. Die Schema.Ini-Datei befindet sich im Verzeichnis `%systemroot%\ntds`. Es handelt sich um eine ASCII-Datei, die sich am Bildschirm anzeigen und drucken lässt.

Standardmäßig kann das Active Directory-Schema nicht editiert werden. Wenn Sie das Schema erweiterbar machen wollen, müssen Sie zuerst die Registry editieren, um anzugeben, dass das Schema nun erweiterbar sein soll. Nachdem Sie die Registry editiert haben ist das Schema erweiterbar, das heißt, dass Sie nun Ihre eigenen Attribute hinzufügen oder sogar komplett neue Objekttypen definieren können. Beispielsweise könnten Sie dem Benutzerobjekt leicht ein Gehaltsattribut oder eine Angestellten-ID hinzufügen.

Eine komplette Unternehmensgesamtstruktur (eine Sammlung von Active Directory-Bäumen in einem einzigen organisatorischen Container) teilt sich ein gemeinsames Schema und betrifft jeden Domänencontroller in jeder verbundenen Domäne. Stellen Sie deshalb immer sicher, dass alle Änderungen die Sie durchführen sowohl korrekt als auch gewünscht sind. Das Schema sollte nur durch erfahrene Programmierer oder Schema-Administratoren geändert werden. Für weitere Informationen über die Erweiterung eines Schemas durchsuchen Sie die Microsoft-Website (`www.microsoft.com`) nach dem »Active Directory Programmers Guide.«

Sie sollten das Schema nur dann erweitern, wenn das Objekt nicht das Attribut besitzt, das Sie benötigen. Um dem Schema ein Attribut hinzuzufügen, führen Sie folgende Schritte aus:

Diese Aktivität sollte nur von einem Schema-Administrator oder einem Programmierer durchgeführt werden.

1. **Starten Sie den Registrierungseditor mit Start, Ausführen und Eingabe von Regedit32.Exe.**
2. **Gehen Sie zu HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.**
3. **Wählen Sie Bearbeiten, Wert hinzufügen und erzeugen Sie einen neuen Werteintrag mit dem Namen Schema Update Allowed (vom Typ REG_DWORD).**
4. **Setzen Sie den Wert dieses neuen Werteschlüssels auf 1.**
5. **Klicken Sie auf Ok.**
6. **Schließen Sie den Registrierungseditor.**

Globale Kataloge

Der globale Katalog beinhaltet einen Eintrag für jedes Objekt der Gesamtstruktur (die eine Kollektion von Bäumen ist, die sich nicht explizit einen einzelnen, benachbarten Namensraum teilen), aber er enthält lediglich eine begrenzte Zahl von Eigenschaften für jedes Objekt. Die komplette Gesamtstruktur teilt sich einen globalen Katalog. Mehrere Server enthalten Kopien des gesamten Katalogs.

Abfragen in der kompletten Gesamtstruktur können nur nach solchen Objekteigenschaften durchgeführt werden, die aktuell im globalen Katalog erscheinen. Abfragen im Domänenbaum eines Benutzers können nach jeder Eigenschaft durchgeführt werden, wenn eine so genannte *tiefe Suche* nach Eigenschaften ausgeführt wird, die sich nicht im globalen Katalog befinden. Nur Verzeichnisdienste (oder Domänencontroller) können für den Besitz einer Kopie des globalen Katalogs konfiguriert werden.

Konfigurieren Sie nicht zu viele globale Kataloge für eine Domäne, weil die zur Pflege solcher Kataloge notwendige Replikation Netzwerkbandbreite beansprucht. Ein globaler Katalogserver pro Domäne innerhalb jedes physikalischen Standorts ist ausreichend. Der Windows 2000 Server richtet Server für globale Kataloge so ein, wie sie benötigt werden, weshalb Sie die Defaultauswahl nicht ändern sollten, ausser Benutzer beschweren sich über lange Antwortzeiten bei Verzeichnisanfragen.

Da vollständige Suchen Abfragen des gesamten Domänenbaums statt des globalen Katalogs nach sich ziehen, verbessert die Gruppierung des Unternehmens in einen einzelnen Baum die Suchzeiten, weil dadurch die Abfrage von Objekten möglich ist, die sich nicht im globalen Katalog befinden. Die Einrichtung Ihres Unternehmens als einzelnen Domänenbaum produziert einen größeren Suchraum und gibt den Benutzern Zugriff auf die gesamte Verzeichnisdatenbank mit einer einzigen tiefen Suche (statt tiefe Suchen für jeden Baum in der Gesamtstruktur anzufordern).

Planen für Active Directory

Falls Sie irgendeine Version von Windows NT ausführen, haben Sie möglicherweise mehrere Domänen mit verschiedenen Vertrauensstellungen zwischen individuellen Teilen der Domänen. Theoretisch könnten Sie einfach jede Domäne aktualisieren, die Vertrauensstellungen beibehalten und keine Änderungen durchführen. Wenn Sie das aber tun, verlieren Sie die Vorteile des Active Directory.

Bevor Sie einen einzelnen Domänencontroller aktualisieren, sollten Sie einen Plan für Ihre Domänen erstellen. Dann sollten Sie diesen Plan zum Bestimmen der Reihenfolge und Methode der Migration von Windows NT-Domänen zu Windows 2000-Active Directory einsetzen.

Was steckt in einem Namensraum?

Ein Namensraum ist eine logisch abgegrenzte Region, die auf einer standardisierten Konvention basierende Namen zur symbolischen Repräsentation von Objekten oder Informationen enthält. Spezifische Regeln bestimmen die Konstruktion von Namen innerhalb eines Namensraums und wie einem Objekt ein Name zugeordnet werden kann. Viele Namensräume sind hierarchischer Natur, beispielsweise das DNS oder Active Directory. Andere Namensräume, beispielsweise NetBIOS, sind flach und unstrukturiert.

In Windows 2000 verwenden Domänen voll aufgeblasene DNS-Namen statt NetBIOS-Namen. Das erzeugt zwischen den Domänen Eltern/Kind-Beziehungen (Parent-Child-Relationships), in denen eine Domäne als Kind einer anderen erzeugt werden kann – eine Sache, die Windows NT nicht unterstützt. Beispielsweise ist `sales.dummies.com` ein Kind der Domäne `dummies.com`. Eine Kinddomäne beinhaltet grundsätzlich immer den vollständigen Namen der Elterndomäne.

Es ist wichtig daran zu denken, dass Eltern/Kind-Beziehungen nur innerhalb einer Elterndomäne unter Verwendung des Domänencontroller-Erstellungsassistenten erzeugt werden können. Die Elterndomäne muss also existieren, um ein Kind dieser Eltern erzeugen zu können. Deshalb ist die Reihenfolge, in der Sie Domänen erzeugen, so wichtig!

Im nächsten Abschnitt finden Sie weitere Gründe dafür, warum es so wichtig ist, Domänen in einer bestimmten Reihenfolge zu erzeugen. Bevor Sie sich mit Standortfragen auseinandersetzen, sollten Sie sich bewusst sein, dass Sie immer erst die Unternehmens-Wurzel-(Root-) Domäne erzeugen sollten, bevor Sie weitere Domänen erstellen. Wenn Sie beispielsweise mit der Wurzeldomäne `dummies.com` beginnen, können Sie anschließend die Domäne `sales.dummies.com` und weitere abhängige Domänen als Kinder der Wurzeldomäne erzeugen. Diese Struktur hilft bei der Suche anderer Domänen und macht das Verschieben von Domänen in zukünftigen Windows 2000-Versionen möglich.

Eine reine Standortfrage

Sites oder Standorte im Active Directory sind Gruppierungen von Servern in Containern oder Behältern, die das physikalische Layout Ihres Netzwerks widerspiegeln. Diese Organisation erlaubt Ihnen die Konfiguration der Replikation zwischen Domänencontrollern. Eine Anzahl von TCP/IP-Subnetzen kann ebenfalls Standorten zugeordnet werden, was es neuen Servern ermöglicht, sich abhängig von ihren IP-Adressen sofort den richtigen Standorten anzuschließen. Dieses Adressierungsschema erleichtert es außerdem Clients, den nächstgelegenen Domänencontroller zu finden.

Wenn Sie den ersten Domänencontroller erzeugen, wird automatisch ein Standardstandort mit dem Namen Default-First-Side erstellt und der Domänencontroller wird diesem Standort zugeordnet. Weitere Domänencontroller werden diesem Standort hinzugefügt, aber sie können verschoben werden. Sie können den Standort außerdem umbenennen.

Standorte werden mit dem Active Directory-Standorte und -Dienste-MMC-Snap-In erzeugt und verwaltet. Um einen neuen Standort zu erzeugen, führen Sie folgende Aktionen durch:

1. **Starten Sie das Active Directory-Standorte und -Dienste-MMC-Snap-in über Start, Programme, Verwaltung, Active Directory-Standorte und -Dienste.**
2. **Klicken Sie mit der rechten Maustaste auf Sites und selektieren Sie dann im Kontextmenü Neuer Standort.**

3. **In der Dialogbox Objekt neu erstellen (Standort) geben Sie den Namen des neuen Standortes ein, beispielsweise Ennepetal.**
4. **Der Name darf bis zu 63 Zeichen lang sein; er darf keine Punkte und Leerzeichen enthalten. Sie müssen außerdem eine Standortverknüpfung selektieren. In der Standardeinstellung gibt es nur einen DEFAULTSITELINK vom Typ IP.**
5. **Selektieren Sie eine Standortverknüpfung für den neuen Standort und klicken Sie dann auf Ok.**

Nachdem der Standort erstellt ist, können Sie ihm verschiedene IP-Subnetze, auf deutsch auch IP-Teilnetze oder Teilnetzwerke genannt, zuordnen. Um das zu tun, führen Sie folgende Schritte aus:

1. **Starten Sie das Active Directory-Standorte und -Dienste-MMC-Snap-In über Start, Programme, Verwaltung, Active Directory-Standorte und -Dienste.**
2. **Erweitern Sie Sites.**
3. **Klicken Sie mit der rechten Maustaste auf Subnets und selektieren Sie dann im Kontextmenü Neues Teilnetz.**
4. **In der Dialogbox Objekt neu erstellen (Teilnetz) geben Sie den Namen des Teilnetzes im Format `<Netzwerk>/<maskierte Bits>` ein. Beispielsweise bezeichnet 200.200.201.0/24 das Netzwerk 200.200.201.0 mit der Subnetzmaske 255.255.255.0. Selektieren Sie den Standort, dem das Subnetz zugeordnet werden soll, beispielsweise Entenhausen.**
5. **Klicken Sie auf Ok.**

Sie haben nun ein Subnetz mit einem Standort verknüpft. Wenn Sie wollen, können Sie einem Standort mehrere Subnetze zuordnen. Für weitere Informationen über Subnetze sehen Sie sich bitte Kapitel 14 an. Noch detailliertere Informationen finden Sie im Windows 2000-Hilfemenü für Subnetze.

Oh Du Organisationseinheit (OU), Du!

Die Organisationseinheit (OU für Organizational Unit) ist eine Schlüsselkomponente des X.500-Protokolls. Wie der Name bereits vermuten lässt, beinhalten Organisationseinheiten Objekte einer Domäne, die in logischen Behältern organisiert sind, was eine feinere Abstufung und Kontrolle innerhalb einer Domäne erlaubt. Organisationseinheitenbehälter können weitere Organisationseinheiten, Gruppen, Benutzer und Computer beinhalten.

OUs lassen sich zum Erstellen einer Hierarchie, die der Struktur Ihres Unternehmens oder Ihrer Organisation entspricht, verschachteln. Durch Verwendung von OUs vermeiden Sie den Einsatz der schwerfälligen, für Windows NT-Server-basierte Netzwerke entwickelten Domänenmodelle (Beispielsweise das Master-Domänenmodell, in dem verschiedene Ressourcen-

domänen die Konten einer zentralen Benutzerdomäne nutzen.) Mit Active Directory können Sie eine einzige große Domäne erzeugen und Ressourcen sowie Benutzer in mehrere getrennte OUs gruppieren.

Der größte Vorteil von OUs ist, dass sie eine Delegation der Autorität erlauben. Sie können bestimmten Benutzern oder Gruppen die administrative Kontrolle einer OU zuweisen, wodurch sie Kennwörter ändern und Konten in dieser OU erzeugen können, aber keine Kontrolle über den Rest der Domäne erhalten. Diese Fähigkeit ist eine der größten Verbesserungen gegenüber der Windows NT-Domänenadministration, die eher eine Alles-oder-Nichts-Lösung war.

Installieren von Active Directory

In vorangegangenen Windows NT-Versionen richteten Sie den Typen jedes Servers während der Installation ein. Die Funktion des Servers konnte eine der folgenden Rollen sein:

- ✔ Standalone/Mitgliedserver
- ✔ PDC
- ✔ BDC

Mit Ausnahme des Austausches der PDC/BDC-Rollen konnte die Rolle eines Servers nicht geändert werden, ohne die Software neu zu installieren. Es war beispielsweise nicht möglich, einen Mitgliedserver zu einem Domänencontroller zu machen, ohne Windows NT neu zu installieren.

Windows 2000 hat all das hinter sich gelassen und erlaubt Ihnen nun, alle Server als normale Server zu installieren. Sie können einen Assistenten benutzen (im folgenden Abschnitt beschrieben), um normale Server in Domänencontrollern zu konvertieren oder Domänencontroller in normale Server. Diese Einrichtung ermöglicht Ihnen außerdem, Domänencontroller von einer Domäne in eine andere zu »verschieben«, indem Sie den Domänencontroller in der alten Domäne zu einem Mitgliedserver und in der neuen Domäne wieder zu einem Domänencontroller machen. Unter Windows NT waren für einen solchen Vorgang Betriebssystem-Neuinstallationen erforderlich.

Domänencontroller promoten

Windows 2000 erlaubt Ihnen die Konvertierung normaler Server in Domänencontroller und umgekehrt. Dazu verwenden Sie den Active Directory-Assistenten, den Sie durch Öffnen der Dcpromo.Exe-Datei starten. Es gibt keine Verknüpfung dafür im administrativen Ordner. Sie müssen das Programm also direkt über eine Eingabeaufforderung oder den Ausführen-Dialog im Start-Menü starten. Um einen Standalone/Mitgliedserver zu einem Domänencontroller aufzurüsten, führen Sie folgende Aktionen durch:

1. **Klicken Sie auf Start, Ausführen.**
2. **Geben Sie in der Ausführen-Dialogbox Dcpromo ein, um den Active Directory-Installationsassistenten zu starten.**

Bevor Sie versuchen Dcpromo.Exe auszuführen und damit den Active Directory-Installationsassistenten starten, müssen Sie sicherstellen, dass in der Windows 2000-Domäne, die Sie erzeugen wollen, eine DNS-Zone konfiguriert ist. Die DNS-Zone unterstützt Service-Records und ist für dynamische Updates eingeschaltet. Ohne diese Informationen kann der Assistent seinen Job nicht erledigen.

3. **Klicken Sie im Einführungsbildschirm auf die Schaltfläche Weiter.**
4. **Es erscheinen zwei Wahlmöglichkeiten:**
   - Domänencontroller für eine neue Domäne
   - Zusätzlicher Domänencontroller für eine bestehende Domäne

Es existiert kein BDC-Konzept beim Windows 2000 Server. Alle Domänencontroller sind mehr oder weniger gleich.

Selektieren Sie für dieses Beispiel Domänencontroller für eine neue Domäne und klicken Sie dann auf Weiter.

5. **Windows 2000 beinhaltet das neue Konzept der Bäume (oder Domänenstrukturen), das die Erzeugung von Kinddomänen (oder untergeordneten Domänen) ermöglicht.**

   Falls Sie eine neue Top-Level-Domäne erstellen wollen, selektieren Sie Eine neue Domänenstruktuir erstellen, sonst Eine neue untergeordnete Domäne in einer bestehenden Domänenstruktur.

   Klicken Sie auf die Schaltfläche Weiter.

6. **Falls Sie die Erzeugung einer neuen Domänenstruktur (eines neuen Baums) gewählt haben, werden Sie nun gefragt, ob Sie eine neue Gesamtstruktur (einen Forest) aus der Domänenstruktur erstellen oder ob Sie diese Domänenstruktur in eine bestehende Gesamtstruktur eingliedern wollen.**

   Gesamtstrukturen erlauben Ihnen eine Anzahl separater Domänenstrukturen zu verbinden und Vertrauensstellungen zwischen ihnen einzurichten. Falls es sich hier um Ihren ersten Windows 2000-Domänenbaum handelt, sollten Sie eine neue Gesamtstruktur erzeugen.

   Klicken Sie auf die Schaltfläche Weiter.

7. **Sie werden nach dem DNS-Namen für Ihre Domäne gefragt.**

   Der Name `savilltech.com` ist beispielsweise ein gültiger Domänenname. Es ist wichtig, dass der Name der Konfiguration auf dem DNS-Server entspricht.

   Geben Sie den DNS-Namen ein und klicken Sie dann auf Weiter.

8. **Nun werden Sie nach einem NetBIOS-Domänennamen gefragt, der in der Voreinstellung aus dem linken Teil des DNS-Domänennamens besteht (bis zu 15 Zeichen), beispielsweise** `savilltech`**. Die Voreinstellung lässt sich natürlich ändern. Klicken Sie auf die Schaltfläche** Weiter**, um fortzufahren.**

9. **Jetzt müssen Sie Speicherplätze für Active Directory und die Active Directory-Protokolldatei angeben. Übernehmen Sie die Voreinstellungen und klicken Sie einfach auf Weiter.**

10. **Schließlich müssen Sie einen Bereich der NTFS-Partition für das System-Volume (SYSVOL) selektieren, auf dem die Public-Dateien des Servers gespeichert werden. Die Voreinstellung lautet** `%systemroot%\SYSVOL`**. Klicken Sie auf** Weiter**.**

Das gemeinsame System-Volume (SYSVOL), das Login/Logoff-Skripts speichert, muss sich auf einem NTFS-5.0-Volume befinden, weil es den *File Replication Service* für die Replikation seines Inhalts zu anderen Domänencontrollern verwendet.

11. **Sie erhalten nun die Option, die Sicherheit für die Verwendung von Windows NT 4.0-RAS-Servern herabzusetzen, was Sie wahrscheinlich nicht tun wollen. Treffen Sie ihre Wahl und klicken Sie dann auf** Weiter**.**

12. **Eine Zusammenfassung erscheint. Klicken Sie auf** Weiter**, um die Aufrüstung zu starten.**

    Der Assistent stellt die Sicherheit ein und erzeugt den Verzeichnisserver-Schemabehälter. Informationen aus der Standard-Verzeichnisdienstedatei und der alten SAM werden eingelesen, falls es sich bei der Maschine um einen aufgerüsteten PDC handelt.

13. **Klicken Sie auf** Fertig stellen **und starten Sie dann die Maschine neu.**

Sie haben nun einen Windows 2000-Domänencontroller. Weitere Domänencontroller lassen sich durch eine Wiederholung der vorangegangenen Schritte mit Selektion von Zusätzlicher Domänencontroller für eine bestehende Domäne in Schritt 2 hinzufügen. Der Assistent fragt Sie dann für die Replikation nach dem Namen der Domäne.

Falls Sie einen existierenden Domänencontroller auf Windows 2000 aktualisieren und dann das Dcpromo-Programm ausführen, werden Sie die Möglichkeit zur Änderung des NetBIOS-Namen nicht erhalten, aber Sie werden nach wie vor einen neuen DNS-Domänennamen wählen können.

Die Active Directory-Datenbank und das gemeinsame System-Volume

Obwohl Sie sich Active Directoty als Informationsblase vorstellen sollten, ist es in Form einer Datei auf jedem Domänencontroller als `%systemroot%\NTDS\ntds.dit` gespeichert. Diese Datei ist immer geöffnet und kann deshalb nicht mit einer einfachen Copy-Operation gesi-

chert werden. Das neue NTBACKUP-Programm von Windows 2000 beinhaltet aber eine Option, mit der sich ein Schnappschuss des Active Directory zum Backup dieser Informationen erstellen lässt. Es gibt einen speziellen *Directory-Restauration-Modus*, in den Sie zum Zurückkopieren eines Active Directory-Backups booten müssen. Kapitel 17 behandelt Backups im Detail.

Das *gemeinsame System-Volume* (oder SYSVOL) ist die Replikationswurzel für jede Domäne. Sein Inhalt wird mit dem File Replication Service zu jedem Domänencontroller innerhalb der Domäne repliziert. Das SYSVOL muss sich auf einem NTFS-5.0-Volume befinden, weil dies eine Anforderung des File Replication Service ist.

SYSVOL ist auch eine Freigabe, die in der Voreinstellung auf `%systemroot%\SYSVOL\sysvol` zeigt, wo sich Domänen-spezifische Bereiche, beispielsweise Anmeldeskripts, befinden. Die Anmeldefreigabe NETLOGON für die Domäne savilltech.com zeigt beispielsweise auf `%systemroot%\SYSVOL\sysvol\savilltech.com\SCRIPTS`. Sie können einfach Dateien, die zum An- und Abmelden benutzt werden, in dieses Verzeichnis kopieren und die Änderungen werden mit dem nächsten Replikationsintervall (in der Voreinstellung alle 15 Minuten) zu allen anderen Domänencontrollern repliziert.

Domänenoperationsmodi

Windows 2000 Server-Domänen arbeiten in zwei Modi: gemischter und einheitlicher (natürlicher) Modus. Domänen im *gemischten Modus* erlauben Windows NT 4.0-BDCs die Teilnahme in Windows 2000-Domänen.

Im *einheitlichen Modus* können nur Windows 2000-Domänencontroller in der Domäne arbeiten und Windows NT 4.0-BDCs werden nicht länger als Domänencontroller unterstützt.

Der Wechsel vom gemischten in den einheitlichen Modus kann nicht rückgängig gemacht werden. Wechseln Sie also nicht in diesen Modus, bevor alle Domänencontroller zu Windows 2000 konvertiert sind. Sie sollten sich außerdem sicher sein, dass keine auf Windows NT 4.0 basierenden BDCs hinzugefügt werden sollen, nachdem der Wechsel durchgeführt ist.

Der Wechsel in den einheitlichen Modus erlaubt die Verwendung von *Universalgruppen*, die, anders als Globale Gruppen, ineinander verschachtelt werden können. Ältere NetBIOS-basierte Clients werden auch im einheitlichen Modus noch NetBIOS-Domänennamen verwenden können.

Um alle Domänencontroller zu ändern, führen Sie folgende Schritte aus:

1. **Starten Sie das MMC-Snap-In ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN in START, PROGRAMME, VERWALTUNG.**
2. **Klicken Sie mit der rechten Maustaste auf die Domänen, die Sie in den einheitlichen Modus konvertieren wollen, und selektieren Sie im Kontextmenü EIGENSCHAFTEN.**

3. **Klicken Sie auf die Schaltfläche Modus wechseln.**
4. **Eine Dialogbox erscheint und fragt Sie, ob Sie die Domänen wirklich im einheitlichen Modus betreiben wollen. Klicken Sie auf Ja, um die Frage zu beantworten.**
5. **Klicken Sie auf Übernehmen.**
6. **Es erscheint eine Meldung, dass die Aktion erfolgreich abgeschlossen wurde. Klicken Sie auf Ok.**
7. **Starten Sie die Maschine neu (obwohl uns gesagt wurde, dass ein Neustart nicht notwendig ist).**

Sie müssen nun die anderen Domänencontroller in der Domänen überprüfen. Falls der Domänenoperationsmodus der einheitliche Modus ist (statt des gemischten Modus), starten Sie den Domänencontroller neu, was 15 Minuten (oder länger, falls der Netzwerkzugriff auf andere Domänencontroller aus irgendeinem Grund fehlschlägt) dauern kann.

Falls ein Domänencontroller nicht kontaktiert werden kann, wenn Sie die Änderung durchführen (weil er sich beispielsweise an einem Remote-Standort befindet und sich nur gelegentlich mit dem Hauptstandort verbindet), wird der Domänencontroller umgestellt, sobald die nächste Replikation stattfindet.

Wenn sich Domänen multiplizieren

In diesem Abschnitt sehen Sie sich in Windows 2000 enthaltene neue Methoden zur Verbindung von Domänen an. In Windows NT 4.0 sind Sie auf einfache ein- oder bidirektionale Vertrauensstellungen zur expliziten Verbindung von zwei Domänen beschränkt. Windows 2000 besitzt ausführlichere, funktionellere Modelle zur Erzeugung von Beziehungen und Verbindungen zwischen seinen Domänen.

Vertrauensstellungen über Domänen

Die Vertrauensstellungen von Windows NT 4.0 sind nicht transitiv. Wenn beispielsweise Domäne A der Domäne B vertraut, und Domäne C der Domäne B, dann vertraut nicht automatisch Domäne C auch der Domäne A (siehe Abbildung 11.2).

Dieses Fehlen der Transitivität ist bei den Vertrauensstellungen für die Verbindung der Mitglieder eines Baums (oder einer Gesamtsruktur) in Windows 2000 nicht länger der Fall. Vertrauensstellungen in Windows 2000 sind 2-Wege-, transitive Vertrauensstellungen. Das bedeutet, dass jede Domäne im Baum implizit jeder anderen Domäne im Baum oder in der Gesamtstruktur vertraut. Das befreit von der Notwendigkeit einer zeitraubenden Administration individueller Vertrauensstellungen zwischen Domänenpaaren, weil solche Vertrauensstellungen automatisch erzeugt werden, wenn eine neue Domäne einem Baum hinzugefügt wird.

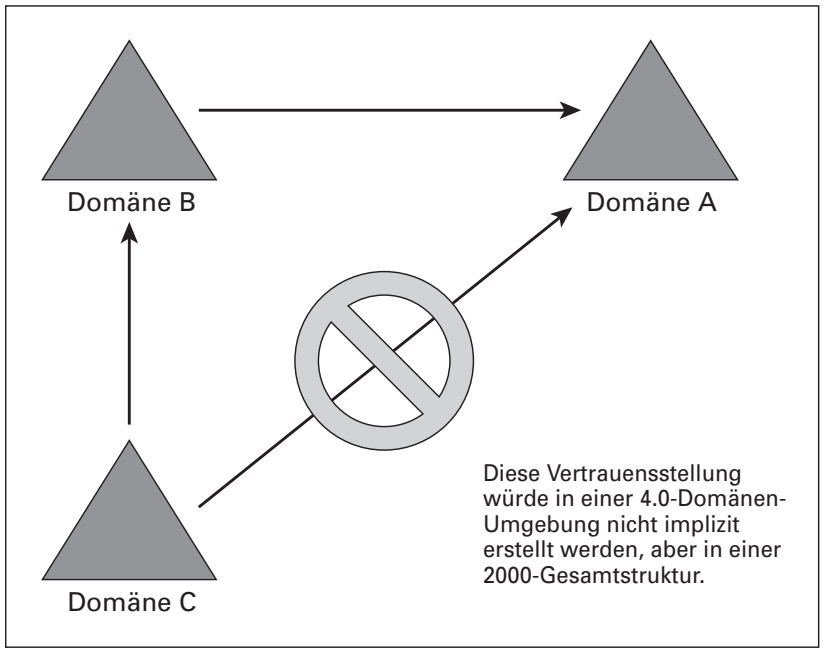

Abbildung 11.2: Ein Beispiel einer Vertrauensstellung in Windows NT 4.0

Die Sicherheit von Windows 2000-Vertrauensstellungen wird über Kerberos gewährleistet. Kerberos Version 5.0 ist das primäre Sicherheitsprotokoll von Windows 2000, aber es ist kein Microsoft-Protokoll. Kerberos ist ein am Massachusetts Institute of Technology (MIT) entwickeltes Sicherheitssystem. Es verifiziert sowohl die Identität eines Benutzers als auch die Identität aller Sitzungsdaten, während dieser Benutzer eingeloggt ist. Kerberos-Dienste werden auf jedem Domänencontroller und Kerberos-Clients auf jeder Windows 2000-Arbeitsstation und auf jedem Windows 2000 Server installiert. Die einleitende Kerberos-Authentisierung eines Benutzers bietet diesem Benutzer einen Single-Logon zu Unternehmensressourcen. Für weitere Informationen über Kerberos sehen Sie sich die Requests for Comments (RFCs) 1510 und 1964 der Internet Engineering Task Force (IETF) an. Diese Dokumente sind im Web unter `www.rfc-editor.org` verfügbar.

Bäume pflanzen

In Windows 2000 kann eine Domäne das Kind einer anderen sein. Beispielsweise ist `legal.savilltech.com` das Kind bzw. die untergeordnete Domäne vom `savilltech.com` (welches der Wurzel-Domänenname und damit auch der Name des Baums bzw. der Domänenstruktur ist). Eine untergeordnete Domäne (Kinddomäne) enthält immer den vollständigen Domänennamen der übergeordneten Domäne (Elterndomäne). Wie in Abbildung 11.3 dargestellt, kann `dev.savillCORP.com` nicht Kind von `savilltech.com` sein, weil sich die Domänennamen nicht entsprechen. Eine Kinddomäne und seine Elterndomäne sind über eine 2-Wege, tranistive Vertrauensstellung miteinander verbunden.

Wenn eine Domäne Kind einer anderen Domäne ist, wird ein Domänenbaum bzw. eine Domänenstruktur erzeugt. Das bedeutet, dass alle Namensräume eine gemeinsame Wurzel (oder dieselben Eltern) verwenden.

Da Domänennamen DNS-Namen sind und der Elternteil des Namens vererbt wird, werden bei einer Umbenennung eines Teils des Baums implizit alle Kinder umbenannt. Wird beispielsweise die Elterndomäne `ntfaq.com` des Kindes `sales.ntfaq.com` in `backoffice.com` umbenannt, dann wird das Kind automatisch in `sales.backoffice.com` umbenannt. (Diese Einrichtung fehlt tatsächlich aktuell in Windows 2000, wird aber in zukünftigen Versionen erscheinen.)

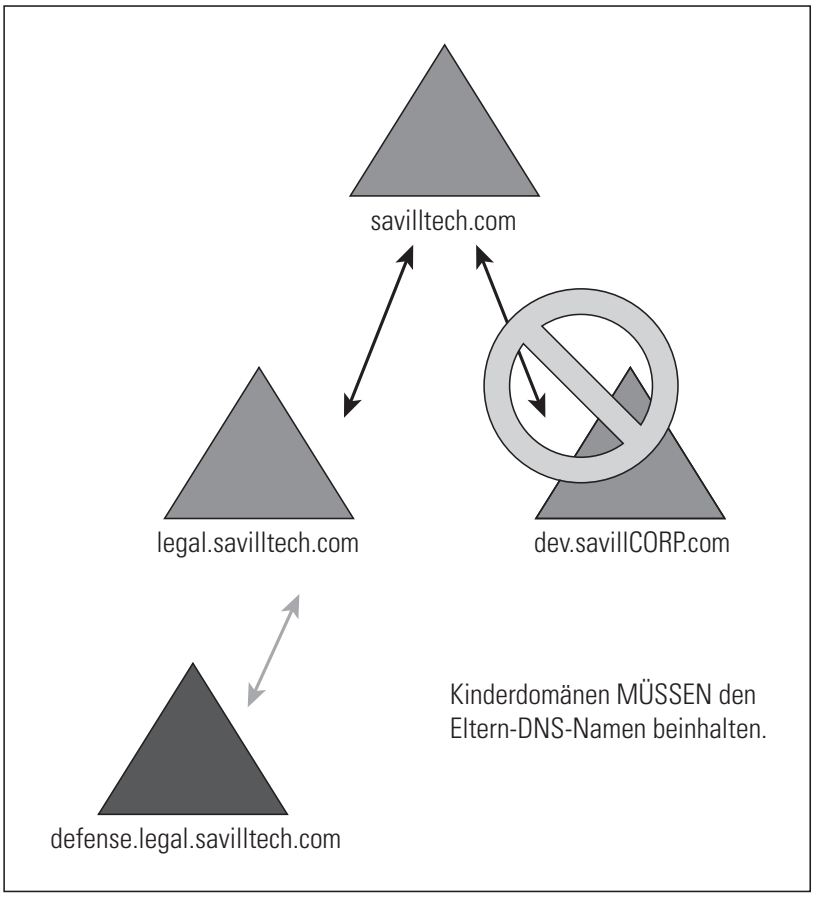

Abbildung 11.3: Ein Beispiel für eine Eltern/Kind-Vertrauensstellung

Domänenbaume können aktuell nur durch den Domänencontroller-Promotionsprozess mit dem Programm DCPROMO.EXE erzeugt werden – auch dies wird sich zukünftig ändern.

Es gibt zahlreiche Vorteile durch das Einordnen von Domänen in einen Domänenbaum bzw. in eine Domänenstruktur. Der erste und wichtigste Vorteil ist, dass alle Mitglieder eines Baums über transitive Kerberos-Vertrauensstellungen zwischen ihren Eltern und deren Kinder verfügen. Diese transitiven Vertrauensstellungen bedeuten auch, dass jedem Benutzer oder jeder Gruppe in einem Domänenbaum Zugriff auf jedes Objekt im gesamten Baum gewährt werden kann. Eine einzelne Netzwerkanmeldung kann auf jeder Arbeitsstation im Domänenbaum benutzt werden.

Den Wald trotz aller Bäume sehen

Möglicherweise haben Sie mehrere separate Domänenbäume in Ihrer Organisation, mit denen Sie Ressourcen gerne teilen würden. Sie können Ressourcen zwischen Domänenbäumen teilen, wenn Sie die Bäume in einer Gesamtstruktur (Forest) zusammenführen.

Eine *Gesamtstruktur* ist eine Sammlung von Domänenstrukturen (Domänenbäumen), die explizit einen einzelnen, abgegrenzten Namensraum benutzen. (Jeder Baum muss trotzdem seine Grenzen haben.) Die Erzeugung einer Gesamtstruktur kann dann nützlich sein, wenn Ihr Unternehmen über mehrere Wurzel-(Root-)DNS-Adressen verfügt.

Abbildung 11.4 zeigt beispielsweise zwei Wurzeldomänen, die über transitive, 2-Wege-Kerberos-Vertrauensstellungen miteinander verbunden sind (wie Vertrauensstellungen zwischen Eltern und Kind). Gesamtstrukturen enthalten immer den gesamten Domänenbaum jeder Domäne. Sie können keine Gesamtstruktur erzeugen, die nur einen Teil eines Domänenbaums enthält.

Gesamtstrukturen werden während der Domänencontroller-Promotion mit dem Programm Dcpromo.Exe erzeugt und können gegenwärtig nicht zu einer anderen Zeit erzeugt werden (was sich in Zukunft ändern soll).

Sie sind nicht auf zwei Domänenbäume in einer Gesamtstruktur beschränkt, sondern Sie können so viele Bäume hinzufügen wie Sie wollen, und alle Domänen innerhalb der Gesamtstruktur können jedem Benutzer innerhalb der Gesamtstruktur Zugriff auf Objekte gewähren. Damit müssen Vertrauensstellungen nicht mehr manuell verwaltet werden. Die Vorteile von Gesamtstrukturen sind folgende:

Alle Bäume besitzen einen gemeinsamen globalen Katalog, der spezifische Informationen über jedes Objekt in der Gesamtstruktur enthält.

Die Bäume enthalten alle ein gemeinsames Schema. Microsoft hat noch nicht bestätigt, was passiert, wenn zwei Bäume verschiedene Schemata haben, bevor sie zusammengeführt werden. Wir gehen davon aus, dass die Änderungen gemischt werden.

Suchabfragen in einer Gesamtstruktur sind tiefe Auchabfragen im gesamten Baum der Domäne, aus der die Anforderung stammt; sie verwenden die Einträge im globalen Katalog für den Rest der Gesamtstruktur.

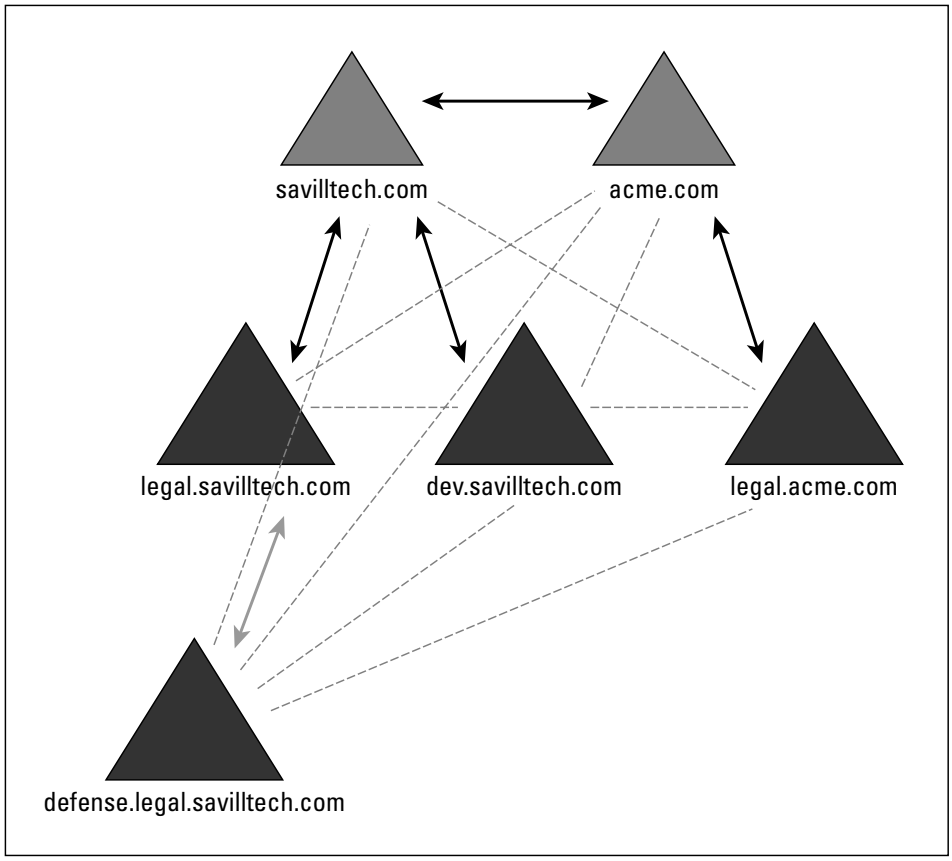

Abbildung 11.4: Ein Beispiel für eine Gesamtstruktur

Sie können sich natürlich auch dafür entscheiden, Domänenstrukturen bzw. Domänenbaume nicht in einer Gesamtstruktur zusammenzuführen. Stattdessen erstellen Sie dann normale Vertrauensstellungen zwischen individuellen Elementen der Bäume.

Wegen des gemeinsamen Schemas innerhalb der Gesamtstrukturen haben viele Organisationen zwei Gesamtstrukturen, damit sie Schemamodifikationen testen können, bevor sie diese in einer lebenden Gesamtstruktur implementieren.