

Kapitel 2

Active Directory für Exchange-Administratoren

In diesem Kapitel:

Ein kurzer Überblick über Active Directory	44
Weitere Active Directory-Komponenten	51
Exchange Server 2007 und Active Directory	55
DNS-Konfiguration	60
Zusammenfassung	61

In Kapitel 1, »Überblick über Microsoft Exchange Server 2007«, haben Sie etwas über die grundlegenden Komponenten einer Exchange-Organisation erfahren. Dieses Kapitel baut auf diesem Wissen auf und beschreibt, wie sich Exchange Server 2007 in Microsoft Windows Server 2003 einbindet und dessen Dienste zu seinem Vorteil nutzt. Wir beginnen mit einem kurzen Überblick über den Verzeichnisdienst Active Directory in Windows Server 2003 und beschreiben dann, wie er in Exchange Server 2007 verwendet wird. Schließlich behandeln wir noch einige der bedeutenderen Internetinformationsprotokolle.

Ein kurzer Überblick über Active Directory

Eine vollständige Beschreibung von Active Directory übersteigt zwar den Rahmen dieses Buches, aber ein kurzer Überblick ist an dieser Stelle sinnvoll. Da Exchange Server 2007 sehr stark von dem zugrunde liegenden Netzwerkbetriebssystem abhängt, müssen Sie die Grundlagen von Windows Server 2003-Active Directory kennen.

Weitere Informationen

Eine ausführliche Beschreibung von Active Directory und der übrigen Begriffe, die in diesem Kapitel behandelt werden, finden Sie in dem Handbuch *Microsoft Windows Server 2003 Administrator's Companion* von Charlie Russel, Sharon Crawford und Jason Gerend (Microsoft Press, 2006).

Die Verzeichnisstruktur in Active Directory

Bevor wir darauf eingehen, was Active Directory ist, sollten Sie zunächst wissen, was ein Verzeichnis ist. Stellen Sie sich dazu ein allgemeines Dateisystem vor. Darin haben Sie ein Laufwerk C: und auf diesem Laufwerk einen Stammordner namens **Memos**. In C:\Memos gibt es für jeden der 12 Monate eines Jahres jeweils einen Ordner, also auch einen mit dem Namen **Juli**. In C:\Memos\Juli befindet sich ein Ordner namens **Abteilungen**. Der vollständige Pfad zum Ordner **Abteilungen** lautet daher C:\Memos\Juli\Abteilungen. Dies ist eine Ordnerhierarchie in einem Dateisystem.

Ein Verzeichnis unterscheidet sich davon nur darin, dass die Hierarchie nicht aus Ordnern, sondern aus *Objekten* besteht. Ein Objekt ist eine Einheit, die durch einen eindeutigen benannten Satz von Attributen beschrieben wird. Außerdem verwenden wir nicht den Windows-Explorer, um diese Objekthierarchie zu durchsuchen, sondern ein Protokoll, das für diesen Zweck entwickelt wurde, nämlich das so genannte *Lightweight Directory Access Protocol (LDAP)*.

HINWEIS

Das ursprüngliche Zugriffsprotokoll für Verzeichnisse wurde Directory Access Protocol (DAP) genannt, wies aber einen großen Overhead auf und war sehr langsam. LDAP ist eine verbesserte Version dieses Protokolls, die wesentlich schneller ist und weniger Overhead hervorruft.

Microsoft hat sich das Konzept des Verzeichnisses mit Active Directory zu Eigen gemacht und es gleichzeitig beträchtlich verbessert, beispielsweise durch die Einführung des dynamischen DNS. Das Wort »Active« in Active Directory steht für die Flexibilität und die Erweiterbarkeit, die dieser Verzeichnisdienst von Microsoft aufweist.

Die logische Struktur von Active Directory

Die logische Struktur von Active Directory bilden Domänen, Organisationseinheiten, Ordnerstrukturen und Gesamtstrukturen.

Domänen

Domänen sind die Kerneinheiten von Active Directory und bestehen jeweils aus einer Sammlung von Computern mit einer gemeinsamen Verzeichnisdatenbank. Die Computer, die diese gemeinsame Verzeichnisdatenbank nutzen, werden als Domänencontroller bezeichnet. Ein Domänencontroller ist ein Windows Server 2003-Computer, auf dem Active Directory installiert ist. Er kann Benutzer für seine eigene Domäne authentifizieren. Auf jedem Domänencontroller ist ein vollständiges Replikat der Domänennamenspartition der Domäne gespeichert, zu der er gehört, sowie vollständige Replikate der Konfigurations- und der Schemanamenspartition der Gesamtstruktur. Mit dem Dienstprogramm **Dcpromo.exe** können Sie einen Windows Server 2003-Computer zu einem Domänencontroller heraufstufen. Weitere Informationen über Partitionen finden Sie weiter hinten in diesem Kapitel.

Alle Active Directory-Domännennamen werden durch einen DNS-Namen und durch einen NetBIOS-Namen bezeichnet. Im Folgenden sehen Sie ein Beispiel für diese beiden Arten von Namen:

- DNS-Domänenname: contoso.com
- NetBIOS-Name: CONTOSO

Im Allgemeinen ist der NetBIOS-Name mit der ersten Komponente des DNS-Namens identisch. Er kann allerdings maximal 15 Zeichen lang sein, während jeder Name in der DNS-Namenskonvention bis zu 64 Zeichen umfassen darf. Sie können beide Namen während der Installation Ihrem Bedarf entsprechend einrichten. In der ersten Ausgabe von Windows Server 2003 konnten Active Directory-Namen verändert werden. Obwohl es Werkzeuge zum Ändern eines Domännennamens gibt, ist dies doch ein umfangreiches Unterfangen. Es ist besser, bei der ursprünglichen Erstellung Ihres Namensschemas vorsichtig zu sein.

Weitere Informationen

Um mehr über die Umbenennungswerkzeuge für Windows Server 2003 Active Directory zu erfahren und sie herunterzuladen, besuchen Sie die Seite <http://www.microsoft.com/technet/downloads/winsrvr/domainrename.msp>.

Die Domäne bildet in Active Directory auch eine Sicherheitsgrenze. Administratoren verfügen über die erforderlichen Berechtigungen und Rechte, um die nötigen Verwaltungsaufgaben in ihrer Domäne durchzuführen. Da jede Domäne jedoch ihre eigenen Sicherheitsbeschränkungen hat, müssen auch Administratoren explizit die erforderlichen Berechtigungen erhalten, wenn sie Verwaltungsaufgaben in anderen Domänen übernehmen sollen. Mitglieder der Gruppe Organisations-Admins haben jedoch die Rechte, um Verwaltungsaufgaben in allen Domänen einer Gesamtstruktur auszuführen. So gibt es neben den Domänenadministratoren auch eine höhere Ebene der Verwaltung, nämlich die der Organisationsadministratoren.

Windows Server 2003 Active Directory-Domänen können sich im gemischten oder im einheitlichen Modus befinden. Standardmäßig werden sie im gemischten Modus installiert, wobei sich ein Windows Server 2003-Domänencontroller wie ein Microsoft Windows NT 4.0-Domänencontroller verhält. Die Sicherheitskontendatenbanken von Active Directory-Domänen im gemischten Modus unterliegen

denselben Einschränkungen wie die von Windows NT 4.0-Domänencontrollern. So ist in diesem Modus beispielsweise die Größe des Verzeichnisses ebenso wie unter Windows NT 4.0 auf 40.000 Objekte begrenzt. Daher können auch Windows NT 4.0-Domänencontroller im Netzwerk existieren, Verbindungen zu den Windows Server 2003-Domänencontrollern herstellen und mit ihnen synchronisiert werden.

HINWEIS Exchange Server 2007 erfordert, dass sich Active Directory vor der Installation im einheitlichen Modus befindet. Mehr darüber erfahren Sie in Kapitel 6, »Exchange Server 2007 installieren«.

Der PDC-Emulator bildet eine der fünf FSMO-Rollen (Flexible Single Master Operation), und zwar diejenige, durch die ein Windows Server 2003-Computer wie ein Windows NT 4.0-PDC wirkt. Nur jeweils ein einziger Windows Server 2003-Domänencontroller kann als PDC-Emulator dienen. Wie alle anderen FSMO-Rollen wird auch diese auf einem Domänencontroller der Domäne installiert, und zwar standardmäßig auf dem ersten. (Die FSMO-Rollen werden in Kürze behandelt.) Sie sollten Windows Server 2003 nur dann im einheitlichen Modus ausführen, wenn kein Grund dafür besteht, eine Verbindung zu einem Windows NT 4.0-Sicherungsdomänencontroller (Backup Domain Controller, BDC) aufzunehmen und dies auch für die Zukunft nicht geplant ist. Mit anderen Worten: Wenn Sie Windows Server 2003 im einheitlichen Modus ausführen, können Sie in Ihrem Netzwerk niemals wieder einen Windows NT-BDC einsetzen, und keine Anwendung in Ihrem Netzwerk wird in der Lage sein, weiterhin Windows NT zu benutzen. Der Wechsel in den einheitlichen Modus ist eine einmalige Entscheidung, die Sie nicht rückgängig machen können. Im einheitlichen Modus können Ihre Windows Server 2003-Domänencontroller Millionen von Objekten in einer Domäne unterhalten. Außerdem wird die Verschachtelung von Gruppen möglich, was von großem Vorteil ist, wenn in Exchange Server 2007 große Verteilergruppen auftreten.

Eigenständige Windows NT 4.0-Server oder Mitgliedserver mit diesem Betriebssystem können jedoch in ein Windows Server 2003-Netzwerk im einheitlichen Modus aufgenommen werden. Damit Windows NT 4.0-Arbeitsstationen an Active Directory teilhaben können, müssen sie auf Windows 2000 Professional, Windows XP Professional oder Windows Vista aktualisiert oder mit dem Verzeichnisdienstclient ausgestattet werden. Windows Server 2003 implementiert Active Directory nach einem Multimastermodell, sodass die Active Directory-Objekte auf jedem Domänencontroller bearbeitet werden können. Aus diesem Grund wird auf die Verzeichnisreplikation zwischen den Domänencontrollern so großer Wert gelegt. Es gibt jedoch einige Rollen, die als Multimasterfunktionen entweder ein zu hohes Sicherheitsrisiko darstellen oder zu schwer durchzuführen sind, weil sie möglicherweise zu Konflikten beim Replikationsverkehr führen könnten. Das Verständnis dieser Rollen ist sehr wichtig: Wenn ein Domänencontroller, der eine bestimmte Rolle ausführt, nicht erreichbar ist, steht diese Funktion auch in Active Directory nicht zur Verfügung. Es handelt sich um die Rolle des Schemamasters, des Domänennamenmasters, des RID-Masters, des PDC-Emulators und des Infrastrukturmasters.

Schemamaster

Das *Schema* ist der Satz von Objektklassen (wie Benutzer und Gruppen) und ihrer Attribute (wie der volle Name und die Telefonnummer), die Active Directory bilden. Der Schemamaster steuert alle Aspekte der Aktualisierung und Änderung dieses Schemas. Um es aktualisieren zu können, benötigen Sie Zugriff auf den Schemamaster. In einer Gesamtstruktur kann es jeweils nur einen Schemamaster geben.

Domänennamenmaster

Der Domänennamenmaster steuert das Hinzufügen und Entfernen von Domänen in einer Gesamtstruktur. Er ist der einzige Domänencontroller, auf dem Sie Domänen erstellen und löschen können. In einer Gesamtstruktur kann es jeweils immer nur einen Domänennamenmaster geben.

RID-Master (Relative Identifier Master)

Der RID-Master weist jedem Domänencontroller in seiner Domäne RID-Sequenzen zu. Während der Schemamaster und der Domänennamenmaster ihre Funktionen in der ganzen Gesamtstruktur ausüben, ist der RID-Master jeweils nur für eine Domäne zuständig, sodass jeder Domäne ein RID-Master zugewiesen ist. Da jeder Domänencontroller Objekte in Active Directory erstellen kann, weist der RID-Master ihm dafür einen Pool von 500 RIDs zu. Sobald ein Domänencontroller mehr als 400 RIDs verbraucht hat, erhält er vom RID-Master weitere 500.

Jedes Mal, wenn ein neuer Benutzer, eine neue Gruppe oder ein neues Computerobjekt erstellt wird, erbt dieses Objekt die Sicherheitskennung (Security Identifier, SID) der Domäne. An das Ende der Domänen-SID wird die RID angehängt, und auf diese Weise erhält jedes Objekt eine eindeutige SID. Wenn ein Objekt in eine andere Domäne verschoben wird, erhält es eine neue SID (bestehend aus der Zieldomänen-SID und der RID). Die Eindeutigkeit der SIDs in Windows Server 2003 auch über die Domänengrenzen hinweg wird dadurch sichergestellt, dass nur der RID-Master Objekte von einer Domäne in eine andere verschieben darf. Für jedes Objekt wird der Verlauf der SID-Änderungen gepflegt, sodass für Sicherheit beim Zugriff auf die Ressourcen gesorgt ist.

PDC-Emulator

Jede Domäne in einer Gesamtstruktur muss einen Domänencontroller aufweisen, der als PDC-Emulator fungiert. Wenn Active Directory im gemischten Modus ausgeführt wird, weil sich auch Windows NT 4.0-Domänencontroller im Netzwerk befinden, ist der PDC-Emulator dafür zuständig, die Kennwortänderungen und die Aktualisierungen der Sicherheitskonten zwischen den Windows NT 4.0-Servern und den Windows Server 2003-Computern zu synchronisieren. Darüber hinaus fungiert der PDC-Emulator für untergeordnete Clients wie Windows 95, Windows 98 und Windows NT 4.0 als PDC für die Domäne. Er dient außerdem als Hauptsuchdienst der Domäne, ist verantwortlich für die Replikation auf die BDCs und schreibt Verzeichniseinträge in die Sicherheitsdatenbank der Windows NT 4.0-Domäne.

Im einheitlichen Modus empfängt der PDC-Emulator die dringenden Aktualisierungen der Active Directory-Sicherheitskontendatenbank, beispielsweise Kennwortänderungen und Kontosperrungen. Sie werden augenblicklich auf den PDC-Emulator repliziert, unabhängig davon, auf welchem Computer in der Domäne sie durchgeführt wurden. Wenn bei einem Anmeldeversuch an einem Domänencontroller die Authentifizierung fehlschlägt, werden die Anmeldeinformationen zunächst zur Authentifizierung an den PDC-Emulator weitergegeben, bevor die Anmeldung verweigert wird.

Infrastrukturmaster

Der Infrastrukturmaster zeichnet alle Verweise zwischen Gruppen und Benutzern auf, die verschiedenen Domänen angehören. Das Objekt in der Remotedomäne wird über seinen GUID und seine SID angesprochen. Wenn ein Objekt von einer Domäne in eine andere verschoben wird, erhält es eine neue SID. Der Infrastrukturmaster repliziert diese Änderung an die Infrastrukturmaster der anderen Domänen.

Organisationseinheiten

Eine *Organisationseinheit* ist ein Containerobjekt, mit dessen Hilfe andere Objekte in einer Domäne gruppiert werden. Eine Organisationseinheit kann Benutzerkonten, Drucker, Gruppen, Computer und andere Organisationseinheiten enthalten.

Weitere Informationen

Der Entwurf von Active Directory beruht auf dem X.500-Standard, den Sie von www.itu.org beziehen können. Die Dokumentation ist ziemlich kurz – sie umfasst lediglich 29 Seiten –, aber ihre Lektüre wird Ihnen nützliches Hintergrundwissen für das Verständnis von Active Directory und Novell Directory Services geben.

Organisationseinheiten dienen ausschließlich zur Erleichterung der Verwaltung. Für den Endbenutzer sind sie vollkommen unsichtbar und haben keinerlei Einfluss auf seine Fähigkeit, auf die Ressourcen im Netzwerk zuzugreifen. Mithilfe von Organisationseinheiten lassen sich Abteilungsgrenzen bzw. geografische Grenzen nachbilden. Außerdem können mit ihrer Hilfe einzelne Benutzer dazu autorisiert werden, bestimmte administrative Aufgaben zu erledigen. Sie können beispielsweise eine Organisationseinheit für alle Drucker erstellen und dann einem Druckeradministrator die vollständige Kontrolle darüber geben.

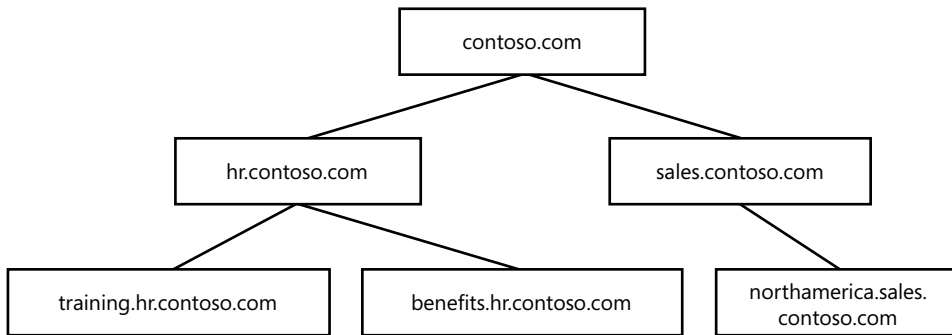
Sie können mithilfe von Organisationseinheiten auch den Einfluss von Administratoren einschränken. So können Sie den Mitarbeitern am Helpdesk z.B. die Berechtigung geben, bei allen Benutzerobjekten in einer Organisationseinheit das Kennwort zu ändern, ohne dass sie gleichzeitig die Berechtigung zum Ändern anderer Attribute der Benutzer – beispielsweise deren Gruppenzugehörigkeit oder Namen – erhalten.

Da eine Domäne in Active Directory Millionen von Objekten umfassen darf, können Unternehmen, die auf Windows Server 2003 aktualisieren, ihre bisherigen mehreren Domänen in eine einzige umwandeln und die Verwaltungsaufgaben für die verschiedenen Ressourcen mithilfe von Organisationseinheiten verteilen.

Strukturen und Gesamtstrukturen

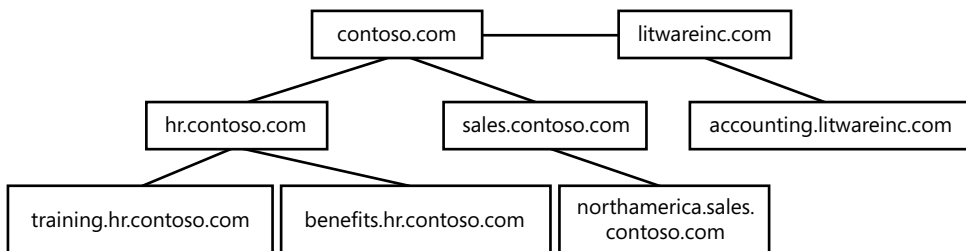
Die erste Windows Server 2003-Domäne, die Sie erstellen, ist die Stammdomäne, die auch die Konfiguration und das Schema der Gesamtstruktur enthält. Anschließend können Sie der Stammdomäne weitere Domänen beifügen, die dann die Struktur bilden. Wie Sie in Abbildung 2.1 sehen können, ist eine *Struktur* eine hierarchische Gruppierung von Windows Server 2003-Domänen, die zu einem gemeinsamen, zusammenhängenden Namespace gehören. Einen zusammenhängenden Namespace erkennen Sie daran, dass alle Domänen in der Struktur denselben Stammnamen erhalten.

Abbildg. 2.1 Fiktive Struktur von contoso.com



Mehrere Strukturen, die nicht zu einem gemeinsamen Namespace gehören, können in einer Gesamtstruktur zusammengefasst werden. Auf diese Weise haben sie dann eine gemeinsame Konfiguration, ein gemeinsames Schema und einen gemeinsamen globalen Katalog. Standardmäßig wird der Name der Stammdomäne auch als Name der Gesamtstruktur verwendet, auch wenn die anderen Strukturen andere Namen tragen.

Zwischen den Stammdomänenservern der verschiedenen Strukturen werden automatisch transitive Vertrauensbeziehungen hergestellt, wenn sie alle zu derselben Gesamtstruktur gehören, selbst wenn sie verschiedene Namen tragen. In Abbildung 2.2 sind zwei Strukturen – **contoso.com** und **trainsbydave.com** – dargestellt, die sich in derselben Gesamtstruktur befinden.

Abbildg. 2.2 Eine Gesamtstruktur aus **contoso.com** und **litwareinc.com**

Die Schema- und die Konfigurationspartition von Active Directory werden auf alle Domänencontroller in jeder Domäne repliziert. Eine Domäne bildet eine Grenze für die Sicherheitsfunktionen und die logische Gruppierung von Objekten, eine Gesamtstruktur dagegen für Active Directory und die Exchange Server 2007-Organisation.

Sie können auch keine neuen Domännennamen verwenden, die dem ersten Domännennamen übergeordnet sind. Wenn Ihr Stammdomänenname beispielsweise **sales.contoso.com** lautet, können Sie niemals eine Domäne mit dem Namen **contoso.com** in derselben Gesamtstruktur einrichten. Andere Domännennamen, z.B. **litwareinc.com**, können Sie in die Gesamtstruktur aufnehmen, solange sie zu einem anderen Namespace gehören.

Gruppen

In Windows Server 2003 werden Gruppen zur Verringerung des administrativen Aufwands genutzt, da sich damit viele Benutzerkonten gleichzeitig verwalten lassen. Außerdem werden Gruppen verwendet, um die Zahl der Objekte, die direkt verwaltet werden müssen, möglichst gering zu halten.

Es gibt in Windows Server 2003 zwei grundlegende Arten von Gruppen. Beide haben bestimmte Vorteile und auch Einschränkungen, die Sie berücksichtigen müssen, wenn Sie sie verwenden wollen. Exchange Server 2007 verwendet beide Arten von Gruppen aus Windows Server 2003:

- **Sicherheitsgruppen** Sicherheitsgruppen enthalten die Sicherheitsprinzipale in Active Directory. Mit ihrer Hilfe werden Benutzer und Computer in Gruppen zusammengefasst, um die Anzahl der Verwaltungspunkte zu reduzieren und um Berechtigungen für Netzwerkressourcen zuzuweisen.
- **Verteilerguppen** Verteilerguppen sind für die Ausführung von Verteilungsfunktionen vorgesehen. Sie können nicht zum Zuweisen von Berechtigungen für Netzwerkressourcen verwendet werden.

Globale Gruppen

Im gemischten Modus können globale Gruppen nur Benutzer aus der Domäne enthalten, in der sie sich selbst befinden, im einheitlichen Modus aber auch Benutzer und globale Gruppen aus der lokalen Domäne, in der sie erstellt wurden. Sie können mit ihrer Hilfe jedoch Berechtigungen für Ressourcen in allen Domänen vergeben. Globale Gruppen können Benutzer, Computer und globale Gruppen aus der lokalen Domäne enthalten. Sie selbst können in alle anderen Arten von Gruppen aufgenommen werden.

In der Regel werden globale Gruppen zur Verwaltung von mehreren Benutzern verwendet, die alle die Berechtigung zur Verwendung einer Netzwerkressource haben. Die Gruppe selbst wird als Teil des globalen Katalogs repliziert, die Mitgliedschaft in der Gruppe jedoch nicht. Das bedeutet, dass durch das Hinzufügen oder Entfernen von Benutzerkonten aus einer globalen Gruppe nicht automatisch eine Replikation des globalen Katalogs ausgelöst wird. Globale Gruppen lassen sich in universelle Gruppen (siehe unten) umwandeln, wenn sie keine anderen globalen Gruppen enthalten und wenn sich die Domäne im einheitlichen Modus befindet.

Lokale Domänengruppen

Im einheitlichen Modus können lokale Domänengruppen andere lokale Domänengruppen sowie Benutzer, globale Gruppen und universelle Gruppen aus allen anderen Domänen innerhalb der Gesamtstruktur enthalten, es können ihnen jedoch nur in ihrer eigenen Domäne Berechtigungen zugewiesen werden. Im gemischten Modus können sie lediglich Konten von Benutzern und globalen Gruppen enthalten.

Sie weisen lokalen Domänengruppen nur Berechtigungen für die Objekte in der lokalen Domäne zu. Das Vorhandensein der Gruppe wird an den Server mit dem globalen Katalog repliziert, die Mitgliedschaft darin jedoch nicht. Die Flexibilität einer lokalen Domänengruppe besteht darin, dass Sie darin (im einheitlichen Modus) jede beliebige Sicherheitsrichtlinie anwenden können, um die Verwaltung zu erleichtern. Wenn die lokale Domänengruppe keine anderen gleichartigen Gruppen umfasst, können Sie sie im einheitlichen Modus in eine universelle Gruppe umwandeln.

Universelle Gruppen

Universelle Gruppen können Benutzer, globale Gruppen und andere universelle Gruppen aus allen Windows Server 2003-Domänen innerhalb der Gesamtstruktur enthalten. Die Domäne muss allerdings im einheitlichen Modus ausgeführt werden, damit Sicherheitsgruppen mit universellem Bereich erstellt werden können. Einer universellen Gruppe können Sie Berechtigungen für Ressourcen zuweisen, die überall in der Gesamtstruktur verteilt liegen.

Die Mitgliedschaft in einer universellen Gruppe muss zum Zeitpunkt der Anmeldung ermittelt werden. Da ihr Bereich universell ist, werden Informationen über diese Art von Gruppe durch den globalen Katalog weiterverbreitet. In diesem Fall wird also nicht nur die Gruppe selbst, sondern auch ihre Mitgliedschaft verbreitet. Eine universelle Gruppe mit einer großen Mitgliederzahl ruft bei Änderungen der Mitgliedschaft zusätzlichen Replikationsaufwand hervor. Universelle Gruppen stehen als Sicherheitsgruppen nur im einheitlichen Modus zur Verfügung. Die Regeln für die Mitgliedschaft in den verschiedenen Gruppen sind in Tabelle 2.1 zusammengefasst.

Tabelle 2.1 Vergleich zwischen den verschiedenen Arten von Gruppen

Gruppenbereich	Mögliche Mitglieder im gemischten Modus	Mögliche Mitglieder im einheitlichen Modus	Mögliche eigene Mitgliedschaft in folgenden Gruppen	Mögliche Berechtigungen für folgende Domänen
Lokale Domäne	Benutzerkonten und globale Gruppen aus allen Domänen	Benutzerkonten, globale und universelle Gruppen aus allen Domänen der Gesamtstruktur sowie lokale Domänengruppen aus derselben Domäne	Lokale Domänengruppen in derselben Domäne	Die Domäne, in der sich die lokale Domänengruppe befindet
Global	Benutzerkonten	Benutzerkonten und globale Gruppen aus derselben Domäne	Universelle Gruppen und lokale Domänengruppen in allen Domänen sowie in globalen Gruppen derselben Domäne	Alle Domänen in der Gesamtstruktur
Universell	–	Benutzerkonten, globale Gruppen und andere universelle Gruppen aus allen Domänen in der Gesamtstruktur	Lokale Domänengruppen und universelle Gruppen in allen Domänen	Alle Domänen in der Gesamtstruktur

Weitere Active Directory-Komponenten

Active Directory ist ein komplexes Gesamtsystem, das weit mehr umfasst als nur die zuvor beschriebene grundlegende logische Struktur. In diesem Abschnitt werden noch einige weitere ausgewählte Komponenten kurz erläutert, die in Active Directory eine wichtige Rolle spielen.

Namenspartitionen

Sie können sich Active Directory als in drei Teile gegliedert vorstellen: in die Domänen, die Konfiguration und das Schema. Jeder Teil ist ein unabhängiger Abschnitt von Active Directory mit eigenen Eigenschaften, beispielsweise mit eigener Replikationskonfiguration und einer eigenen Struktur von

Berechtigungen. Ein Windows Server 2003-Domänencontroller speichert in seiner Datenbankdatei (Ntds.dit) immer die folgenden drei Namenspartitionen. Die standardmäßigen LDAP-Pfade für diese Partitionen lauten wie folgt:

- **Konfiguration:** cn=configuration,dc=sales,dc=contoso,dc=com
- **Schema:** cn=schema,cn=configuration,dc=sales,dc=contoso,dc=com
- **Domäne:** dc=sales,dc=contoso,dc=com

In einer Struktur mit mehreren Domänen gehören die Domänencontroller verschiedenen Domänen an. Diese Server haben dann zwar eine gemeinsame Konfigurations- und eine gemeinsame Schemanamenspartition, aber jeweils eine unterschiedliche Domänennamenspartition. Exchange Server 2007 speichert die meisten Informationen in der Konfigurationsnamenspartition, die innerhalb der Gesamtstruktur weitergegeben wird.

Standorte

Ein *Standort* in Active Directory ist eine Sammlung mehrerer IP-Subnetze, die permanent und über Leitungen mit hoher Bandbreite miteinander verbunden sind. Active Directory geht davon aus, dass alle Computer eines Standorts ständige Hochgeschwindigkeitsverbindungen untereinander unterhalten. Oftmals bilden Standorte die physische Struktur eines Netzwerks ab: Langsame WAN-Verbindungen gehören meist nicht zu den Standorten, da diese von Hochgeschwindigkeitsleitungen gebildet werden.

Die Topologien von Standorten und Domänen sind vollständig unabhängig voneinander. Eine Domäne kann mehrere Standorte umschließen, es können aber auch mehrere Domänen an einem Standort untergebracht sein. Da die Bandbreite zwischen verschiedenen Standorten oft langsam oder unzuverlässig ist, muss zur Verbindung zweier Standorte in der Regel ein Connector eingesetzt werden, der die Bezeichnung *Standortverknüpfung* trägt.

Standortverknüpfungen werden vom Administrator manuell erstellt und bilden die physische Topologie eines Netzwerks. In Windows Server 2003 wird die Konsistenzprüfung (Knowledge Consistency Checker, KCC) verwendet, um über die Standortverknüpfungen Replikationspfade zwischen den Domänencontrollern einzurichten. Die Konsistenzprüfung wird automatisch ausgeführt, kann aber manuell konfiguriert werden. Sie erstellt auf jedem Domänencontroller in der Konfigurationsnamenspartition *Verbindungsobjekte*. Diese bilden die Replikationstopologie, über die die Active Directory-Informationen repliziert werden. Die Konsistenzprüfung ist ein Dienst, der auf jedem Domänencontroller ausgeführt wird, um dessen Verbindungsobjekte zu erstellen.

Dienstesuche

In Windows Server 2003 übernimmt DNS diese Funktion und hilft den Clients dabei, die von ihnen benötigten Dienste im Netzwerk zu finden. Windows Server 2003 umfasst das dynamische DNS, das standardmäßig zu einer Installation von Active Directory gehört. Mit seiner Hilfe fragen die Clients auf der Suche nach Diensten im Netzwerk SRV-Einträge (Service) von DNS ab und können auch DNS-Einträge aktualisieren, wenn sich ihr eigener Standort ändert.

Globale Katalogserver

In einer Umgebung mit mehreren Domänen kann man davon ausgehen, dass manche Benutzer auch auf Objekte außerhalb ihrer eigenen Domäne zugreifen müssen. Beispielsweise muss ein Benutzer aus Domäne A vielleicht Zugriff auf einen Farbdrucker in Domäne B haben. Da die Domänencontroller nur ein Replikat der Objekte in ihrer eigenen Domäne pflegen, muss innerhalb einer Gesamtstruktur ein besonderer Dienst vorhanden sein, der den Benutzern Zugriff auf Objekte in anderen Domänen verschafft. Dieser Dienst wird vom globalen Katalogserver bereitgestellt. Auf ihm sind Replikate aller Objekte in der Gesamtstruktur zusammen mit einem begrenzten Satz ihrer Attribute gespeichert. Welche Attribute der Objekte im globalen Katalog aufgelistet werden, bestimmt das Schema. Der globale Katalog ist keine eigenständige Datei, sondern in der Datei **Ntds.dit** enthalten, und umfasst ca. 40% des Umfangs von Active Directory oder der **Ntds.dit**-Datei auf einem Domänencontroller ohne globalen Katalog.

HINWEIS Standardmäßig gibt es in einer Gesamtstruktur nur einen globalen Katalogserver, nämlich den ersten Domänencontroller, der in der ersten Domäne der ersten Struktur installiert ist. Jeder weitere globale Katalogserver muss manuell eingerichtet werden. Sie können dies erreichen, in dem Sie das Snap-In **Active Directory-Standorte und Dienste** öffnen und darin die NTDS-Einstellungen des Servers suchen, auf dem Sie den Dienst installieren wollen. Klicken Sie dann mit der rechten Maustaste auf **NTDS Settings** (NTDS-Einstellungen), wählen Sie **Eigenschaften** und aktivieren Sie das Kontrollkästchen **Globaler Katalog**.

Neben den Benutzern, die Zugriff auf Dienste außerhalb ihrer eigenen Domäne benötigen, gibt es auch Anwendungen, die auf eine Liste aller Objekte innerhalb der Gesamtstruktur angewiesen sind. Exchange Server 2007 ist eine solche Anwendung. Wenn ein Benutzer zum Beispiel die globale Adressliste durchsuchen will, wird diese Liste vom globalen Katalogserver erstellt. Der Server führt alle E-Mail-aktivierten Objekte auf und gibt diese Liste in der Adressbuchschnittstelle an den Benutzer zurück.

Auch in einer Umgebung mit nur einer Domäne werden die Exchange-Clients an den globalen Katalogserver verwiesen, wenn sie Adressen abfragen wollen. Standardmäßig werden in einem solchen Szenario alle derartigen Abfragen an den Stammdomänencontroller weitergegeben. Sie sollten einen Anstieg des Netzwerkverkehrs zwischen den globalen Katalogen und den Exchange Server 2007-Computern einplanen. Dieser Anstieg kann beträchtlich sein, wenn Sie sämtliche Vorteile aller neuen Funktionen und Rollen in Exchange Server 2007 nutzen möchten.

Hier ist noch der Hinweis nützlich, dass ein globaler Katalogserver je nach dem TCP-Port, der für eine Abfrage verwendet wird, unterschiedliche Attribute zurückgibt. Bei einer Abfrage an Port 389 (dem standardmäßigen LDAP-Port) kann der Client beispielsweise nur innerhalb seiner Basisdomäne nach Objekten suchen, dafür wird der vollständige Satz von Attributen für das Objekt zurückgegeben. Bei einer Abfrage über Port 3268 dagegen kann der Client in der ganzen Gesamtstruktur nach Objekten suchen, auch in der Basisdomäne des globalen Katalogservers. Der Client erhält hierbei aber nur einen Teil der verfügbaren Attribute zurück, selbst wenn sich das Objekt in der Basisdomäne des globalen Katalogservers befindet.

Clientauthentifizierung

Wenn ein Client versucht, sich in einer Domäne anzumelden, fragt er DNS-SRV-Einträge ab, um einen Domänencontroller zu finden. DNS ordnet daraufhin die IP-Adresse des Clients einem Active Directory-Standort zu und gibt eine Liste der Domänencontroller zurück, die den Client authentifizieren können. Der Client wählt willkürlich einen der Domänencontroller aus der Liste und sendet zuerst ein Signal an ihn, bevor er die Anmeldeanfrage auf den Weg schickt. Im einheitlichen Modus leitet der authentifizierende Domänencontroller die Anmeldeinformationen des Clients an den lokalen Server mit dem globalen Katalog weiter, der die Zugriffsmöglichkeiten aufgrund der Mitgliedschaft in universellen Sicherheitsgruppen aufzählt.

Active Directory-Namen

Die Namenskonventionen, die in einem Verzeichnis befolgt werden, betreffen sowohl die Benutzer als auch die Anwendungen. Wenn Sie eine Ressource im Netzwerk suchen, müssen Sie ihren Namen oder eine ihrer Eigenschaften kennen. Active Directory unterstützt mehrere Namenskonventionen für die verschiedenen Formate, die auf den Verzeichnisdienst zugreifen können.

Definierter Name

Jedes Objekt im Verzeichnis besitzt einen *definierten Namen*, der den Speicherort des Objekts innerhalb der gesamten Objekthierarchie bezeichnet. Zum Beispiel:

```
cn=dhall,cn=users,dc=contoso,dc=com
```

Dieses Beispiel zeigt an, dass sich das Benutzerobjekt **dhall** im Container **users** befindet, der wiederum in der Domäne **contoso.com** angesiedelt ist. Wenn das Objekt **dhall** in einen anderen Container verschoben wird, ändert sich sein definierter Name entsprechend seiner neuen Position in der Hierarchie. Definierte Namen sind innerhalb einer Gesamtstruktur immer eindeutig. Es kann keine zwei Objekte mit demselben definierten Namen geben.

Relativ definierter Name

Der *relativ definierte Name* eines Objekts ist der Teil des definierten Namens, der als Attribut des Objekts fungiert. In dem oben genannten Beispiel lautet der relativ definierte Name des Objekts **dhall** und der relativ definierte Name der übergeordneten Organisationseinheit **users**. In Active Directory kann ein übergeordneter Container niemals zwei Objekte mit demselben relativ definierten Namen aufnehmen.

Benutzerprinzipalname

Der *Benutzerprinzipalname* wird für jedes Objekt im Format *benutzername@DNS_domäne* erstellt. Die Benutzer können sich mit diesem Namen anmelden, und Administratoren können bei Bedarf Suffixe dafür definieren. Benutzerprinzipalnamen müssen eigentlich eindeutig sein, doch wird diese Eindeutigkeit in Active Directory nicht durchgesetzt. Es ist jedoch vorteilhaft, wenn Sie eine Namenskonvention einführen, mit der mehrfach vorkommende Benutzerprinzipalnamen vermieden werden.

Global eindeutiger Bezeichner

Manche Anwendungen müssen Objekte anhand eines konstanten Bezeichners ansprechen können. Dies wird dadurch erreicht, dass die Objekte ein Attribut erhalten, das *global eindeutiger Bezeichner* (*Globally Unique Identifier, GUID*) genannt wird. Es handelt sich um eine 128-Bit-Zahl, die garantiert eindeutig ist. Der GUID wird einem Objekt bereits bei seiner Erstellung zugewiesen und niemals verändert, auch dann nicht, wenn das Objekt innerhalb seiner Domäne in andere Container verschoben wird.

Exchange Server 2007 und Active Directory

Exchange Server 2007 ist stark in den Active Directory-Dienst von Windows Server 2003 integriert. Diese Lösung bietet mehrere Vorteile:

- **Zentrale Objektverwaltung** Die Verwaltung von Exchange Server 2007 und Windows Server 2003 ist nun vereinheitlicht. Die Verzeichnisobjekte lassen sich von einem Team an einem Ort und mit nur einem Werkzeug verwalten.
- **Vereinfachte Sicherheitsverwaltung** Exchange Server 2007 verwendet die Sicherheitsfunktionen von Windows Server 2003, beispielsweise die diskrete Zugriffssteuerungsliste (Discretionary Access Control List, DACL). Änderungen an den Sicherheitsprinzipalen (wie Benutzer- oder Gruppenkonten) gelten gleichzeitig für alle Daten, die in Freigaben von Exchange Server 2007 und Windows Server 2003 gespeichert sind.
- **Vereinfachte Erstellung von Verteilerlisten** Exchange Server 2007 verwendet automatisch die Sicherheitsgruppen von Windows Server 2003 als Verteilerlisten. Auf diese Weise müssen Sie nicht mehr für jede Abteilung eine Sicherheitsgruppe und eine entsprechende Verteilergruppe anlegen. Verteilergruppen können in den Fällen erstellt werden, in denen als einzige Funktion die E-Mail-Verteilung benötigt wird.
- **Leichterer Zugriff auf Verzeichnisinformationen** LDAP ist das standardmäßige Protokoll für den Zugriff auf Verzeichnisinformationen.

Exchange Server 2007 und die Active Directory-Standorttopologie

Exchange 2000 Server und Exchange Server 2003 erforderten die Einrichtung von Routinggruppen, um die Verteilung von Nachrichten und anderem Exchange-bezogenen Datenverkehr innerhalb der Organisation zu regeln. Exchange Server 2007 nutzt Routinggruppen nicht länger, sondern greift auf die Topologie des Active Directory-Standorts zurück.

Alle Computer an einem Active Directory-Standort sollten mit einem verlässlichen Hochgeschwindigkeitsnetzwerk verbunden sein. Per Voreinstellung wird bei der ersten Bereitstellung von Active Directory im Netzwerk ein einzelner Standort namens **Standardname-des-ersten-Standorts** erstellt. Alle Server- und Clientcomputer in der Struktur werden zu Mitgliedern dieses ersten Standorts. Wenn Sie mehr als einen Standort definieren möchten, müssen Sie die Subnetze bestimmen, die sich derzeit im Netzwerk befinden, und jeweils mit Active Directory-Standorten verbinden.

In Active Directory definieren *IP-Standortverknüpfungen* die Beziehung zwischen Standorten und verbinden zwei oder mehr Active Directory-Standorte. Jede Standortverknüpfung ist mit Kosten verbunden, die Active Directory diktieren, wie diese Verknüpfung im Vergleich mit den Kosten anderer verfügbarer Verbindungen zu verwenden ist. Sie (oder der Active Directory-Administrator) legen die Kosten einer Verbindung anhand der relativen Netzwerkgeschwindigkeit und der verfügbaren Bandbreite im Vergleich zu anderen verfügbaren Verbindungen fest.

Exchange Server 2007 verwendet die Kostenbestimmung für eine Standortverknüpfung um bei mehreren vorhandenen Verbindungsmöglichkeiten die günstigste Verbindungsroute herauszufinden. Die Kosten einer Route werden durch Summieren der Kosten aller Standortverknüpfungen eines Pfades ermittelt. Nehmen Sie beispielsweise an, dass ein Computer im Standort A mit einem Computer im Standort C kommunizieren muss. A ist über eine Standortverknüpfung mit Kosten von 10 mit dem Standort B und B über eine Standortverknüpfung mit Kosten von 5 mit C verbunden. Die Kosten für die Route A zu C betragen also 15.

Active Directory-Clients ermitteln die Standortzugehörigkeit, indem sie ihre zugewiesene IP-Adresse mit dem zugehörigen Subnetz des jeweiligen Standorts vergleichen.

Da Exchange Server 2007 nun eine standortbezogene Anwendung ist, kann es seine eigene Mitgliedschaft in einem Active Directory-Standort und die Standortmitgliedschaft anderer Servercomputer bestimmen. Alle Exchange Server 2007-Serverfunktionen verwenden die Standortmitgliedschaft, um festzustellen, welche Domänencontroller und globalen Katalogserver für Active Directory-Anfragen zu verwenden sind. Außerdem versucht Exchange Server 2007 Empfängerinformationen von Verzeichnisservern abzurufen, die sich im selben Standort wie der Exchange Server 2007-Computer befinden.

Die Funktionen von Exchange Server 2007 verwenden die Informationen der Active Directory-Standortmitgliedschaft wie folgt:

- Die Funktion des Postfachservers stellt fest, welche Hub-Transport-Server sich im gleichen Active Directory-Standort befinden. Der Postfachserver schlägt Nachrichten für die Weiterleitung zu einem Hub-Transport-Server im gleichen Active Directory-Standort vor. Der Hub-Transport-Server führt eine Empfängerauflösung durch und fordert bei Active Directory an, eine E-Mail-Adresse für ein Empfängerkonto zu erstellen. Anschließend liefert der Hub-Transport-Server die Nachricht an den Postfachserver im gleichen Active Directory-Standort aus oder übermittelt sie zu einem anderen Hub-Transport-Server, der sie dann zu einem Postfachserver außerhalb des Active Directory-Standorts weiterleitet. Wenn sich keine Hub-Transport-Server im Active Directory-Standort des Postfachservers befinden, können zu Letzterem keine Nachrichten übermittelt werden.
- Die Mitgliedschaft im Active Directory-Standort und die Informationen über die Standortverknüpfung werden verwendet, um Prioritäten in einer Serverliste zu setzen, die für Verweise öffentlicher Ordner genutzt wird. Benutzer werden beim Zugriff auf ihre Postfachdatenbank zuerst zur standardmäßigen Datenbank für öffentliche Ordner verwiesen. Wenn sich in der standardmäßigen Öffentlichen Ordner-Datenbank kein Replikat des angeforderten öffentlichen Ordners befindet, stellt der Postfachspeicher (der die standardmäßige Öffentliche Ordner-Datenbank enthält) eine priorisierte Verweisliste der Postfachserver bereit, die ein Replikat für den Client enthalten. Datenbanken für öffentliche Ordner, die sich im gleichen Active Directory-Standort wie die standardmäßige Öffentliche Ordner-Datenbank befinden, werden zuerst aufgelistet. Zusätzliche Verweise auf Positionen werden nach der Lage ihrer Active Directory-Standorte aufgeführt.
- Die Funktion des Unified Messaging-Servers verwendet die Mitgliedschaftsinformationen des Active Directory-Standorts, um festzustellen, welche Hub-Transport-Server sich im gleichen Active Directory-Standort befinden. Der Unified Messaging-Server schlägt Nachrichten für die Weiterleitung zu einem Hub-Transport-Server im selben Active Directory-Standort vor. Der Hub-

Transport-Server liefert die Nachricht an den Postfachserver im gleichen Active Directory-Standort aus oder übermittelt sie zu einem anderen Hub-Transport-Servercomputer, der sie dann zu einem Postfachserver außerhalb des Active Directory-Standorts weiterleitet.

- Wenn der Clientzugriffsserver eine Anforderung für eine Benutzerverbindung erhält, fragt er bei Active Directory an, welcher Postfachserver das Benutzerpostfach verwaltet. Dem Clientzugriffsserver wird daraufhin die Active Directory-Standortmitgliedschaft des Postfachservers mitgeteilt. Befindet sich der Postfachserver nicht im gleichen Standort wie der Clientzugriffsserver, wird die Verbindung zu einem Clientzugriffsserver im Standort des Postfachservers umadressiert.
- Exchange Server 2007 Hub-Transport-Server fragen Informationen von Active Directory ab, um festzulegen, wie Nachrichten innerhalb der Organisation geleitet werden sollen. Befindet sich das Postfach eines Empfängers auf einem Postfachserver im selben Active Directory-Standort wie der Hub-Transport-Server, wird die Nachricht direkt an das Postfach übermittelt. Liegt das Postfach jedoch auf einem Postfachserver in einem anderen Active Directory-Standort, wird die Nachricht zunächst an einen Hub-Transport-Server in diesem Standort weitergeleitet und danach erst zum Postfachserver.

Verwaltungsshell

Sie können das Commandlet **Set-AdSiteLink** in der Exchange-Verwaltungsshell zur Konfiguration Exchange-spezifischer Kosten einer IP-Standortverknüpfung in Active Directory verwenden. Diese Kosten stellen ein eigenes Attribut dar, das anstelle der Active Directory-Kosten verwendet wird, um einen Exchange-Routenplan festzulegen. Eine solche Konfiguration ist nützlich, wenn die IP-Standortverknüpfungskosten nicht zu einem optimalen Ergebnis der Topologie für das Nachrichtenrouting führt.

Exchange Server 2007-Daten in Active Directory speichern

Wir haben bereits erwähnt, dass Active Directory in drei Namenspartitionen eingeteilt ist: Konfiguration, Schema und Domäne. In diesem Abschnitt geht es nun darum, wie Exchange Server 2007 jede dieser Partitionen verwendet und welche Arten von Daten darin gespeichert werden.

Domänennamenspartition

In der Domänennamenspartition werden alle Domänenobjekte für Exchange Server 2007 gespeichert und von dort aus auf alle Domänencontroller in der Domäne repliziert. Die Empfängerobjekte, also Benutzer, Kontakte und Gruppen, sind in dieser Partition gespeichert. Exchange Server 2007 nutzt Active Directory, um den Benutzer-, Gruppen- und Kontaktobjekten für die Nachrichtenübermittlung Attribute zuzuweisen.

Einen Gruppenimplementierungsstrategie entwerfen

Exchange Server 2007 verwendet Verteilergruppen, um eine Nachricht an viele Empfänger zu senden. Alle Benutzerkonten, die zu einer Verteilergruppe gehören, empfangen die Nachrichten, die an die Gruppe gesendet werden. Wenn Windows Server 2003 im einheitlichen Modus ausgeführt wird, können Gruppen innerhalb anderer Gruppen verschachtelt werden, wobei Verteilerlisten mit mehreren Ebenen entstehen. Für die Verbreitung von Nachrichten an eine große Anzahl von Empfängern werden meist entweder globale oder universelle Gruppen verwendet.

Der größte Nachteil der universellen Gruppen besteht darin, dass ihre Mitgliedschaft vollständig an jeden globalen Katalogserver repliziert wird. Das bedeutet, dass bei jeder Änderung einer Mitgliedschaft das Netzwerk mit dem Datenverkehr belastet wird, der bei der Replikation entsteht. Aus diesem Grund empfiehlt es sich, in universelle Gruppen möglichst nur globale Gruppen aufzunehmen. In diesem Fall ändert sich die Mitgliedschaft nur in den globalen Gruppen und nicht in der universellen Gruppe selbst, sodass keine Daten repliziert werden müssen.

Wenn Sie sich gegen die Verwendung universeller Gruppen entscheiden, können Sie auch globale Gruppen E-Mail-aktivieren, um Nachrichten an mehrere Empfänger zu verteilen. Da die Daten über die Mitgliedschaft in einer globalen Gruppe nicht an den globalen Katalog weitergegeben werden, müssen Sie sich über die folgenden Dinge Gedanken machen, wenn Ihre Exchange-Umgebung mehrere Domänen umfasst:

Wenn eine Nachricht an eine globale Gruppe in einer Remotedomäne gesendet wird, muss der Server für die Aufgliederung der Verteilerlisten eine Verbindung zu einem Domänencontroller in der Basisdomäne der Gruppe herstellen und die Mitgliederliste abrufen. Darüber hinaus muss er eine IP-Verbindung zu einem Domänencontroller in der Basisdomäne der Gruppe haben. Das Abrufen der Mitgliederliste aus einer Remotedomäne kann lange dauern, wenn die Verbindung zwischen zwei Domänen langsam oder unzuverlässig ist, sodass die Zustellung von Nachrichten verzögert wird, was wiederum die Gesamtleistung des Systems schmälert. Am besten ist es, wenn sich in der Remotedomäne ein Exchange Server 2007-Computer befindet, den Sie dann als Server für die Aufgliederung der Verteilerlisten einsetzen können, anstatt die Mitgliederliste über das Netzwerk abzurufen und die Gruppenmitgliedschaft lokal aufzugliedern.

Wenn Sie sich für einen Gruppentyp entscheiden, müssen Sie die folgenden Gesichtspunkte bedenken:

- **Besteht Ihre Umgebung nur aus einer oder aus mehreren Domänen?** Wenn Sie nur eine Domäne haben, brauchen Sie keine universellen Gruppen, da es in der Domäne nur lokale Objekte gibt. Falls Sie dagegen über mehrere Domänen verfügen, sollten Sie universelle Gruppen verwenden, wenn es nur selten Änderungen in der Mitgliedschaft gibt (wenn die Mitglieder also globale Gruppen und nicht einzelne Benutzer sind). Denken Sie daran, dass die einzelnen Benutzer bei der Verwendung von universellen Gruppen möglicherweise nicht auf alle Attribute von Objekten aus anderen Domänen zugreifen können.
- **Können Sie zwischen allen Domänen direkte IP-Verbindungen herstellen?** Wenn Sie IP-Verbindungen haben, sollten Sie globale Gruppen verwenden, sofern sich die Mitgliedschaft häufig ändert bzw. sofern in jeder Domäne Exchange Server-Computer vorhanden sind, die als Server für die Aufgliederung der Verteilerlisten fungieren können. Andernfalls sollten Sie universelle Gruppen verwenden, weil der lokale Server für die Aufgliederung der Verteilerlisten verwendet werden kann, wenn sich die Mitgliedschaft nicht häufig ändert.
- **Ändert sich die Mitgliedschaft häufig?** Ist dies der Fall, verwenden Sie globale Gruppen. Wenn nicht, dann sind universelle Gruppen zu empfehlen.

Outlook-Benutzer können die Mitglieder einer in einer Remotedomäne erstellten Gruppe nicht einsehen, sondern nur die Mitglieder von globalen und lokalen Domänengruppen, die in ihrer eigenen Basisdomäne angelegt wurden.

Der bereits erwähnte Server für die Aufgliederung der Verteilerlisten erfordert Erklärung. Wenn eine Nachricht an eine E-Mail-aktivierte Gruppe gesendet wird, muss sie aufgegliedert und an jedes einzelne Mitglied der Gruppe adressiert werden. Standardmäßig wird diese Aufgliederung von dem lokalen Servercomputer übernommen. Er nimmt über LDAP Kontakt mit dem globalen Katalogserver auf, damit die Nachricht an jedes einzelne Mitglied der Gruppe übermittelt werden kann. Wenn die Nachricht für eine lokale Gruppe innerhalb der Domäne bestimmt ist, wird der lokale Server mit

dem globalen Katalog angesprochen. Falls der lokale Server nicht für die Aufgliederung der Verteilerlisten zur Verfügung steht, wird dafür ein anderer Server im Standort verwendet.

Sie können einen bestimmten Server in einer Organisation für die Aufgliederung bestimmen. Der Vorteil besteht hierbei in der Auslagerung des teilweise arbeitsaufwändigen Prozesses der Aufgliederung großer Verteilergruppen auf einen dedizierten Server und somit der Entlastung des Postfachservers. Als Nachteil ergibt sich, dass bei Nichterreichbarkeit dieses Servers keine Nachrichten an die Verteilergruppe weitergeleitet werden und Exchange auch keinen anderen Server dafür ausprobiert. Aus diesem Grund sollten Sie, wenn Sie einen Server für die Aufgliederung bestimmen, auf eine hohe Verfügbarkeit dieses Computers achten.

Konfigurationsnamenspartition

In der Konfigurationsnamenspartition von Active Directory werden Informationen über den Aufbau Ihres Exchange Server 2007-Systems gespeichert. Da diese Informationen an alle Domänencontroller in der Gesamtstruktur repliziert werden, gilt dies auch für die Exchange Server 2007-Konfiguration. Die Konfigurationsinformationen enthalten die Exchange Server 2007-Topologie, -Connectors, -Protokolle und -Diensteinstellungen.

Schemanamenspartition

In der Schemapartition sind alle Objekttypen, die in Active Directory erstellt werden können, und ihre Attribute gespeichert. Diese Informationen werden an alle Domänencontroller in der Gesamtstruktur repliziert. Bei der ersten Installation von Exchange Server 2007 in der Gesamtstruktur wird das Active Directory-Schema erweitert, sodass es zusätzlich neue Exchange Server 2007-spezifische Objektklassen und -attribute umfasst. Diese neuen Klassen beginnen mit »msExch« oder »ms-Exch« und werden aus den LDIF-Dateien (LDAP Data Interchange Format) in den Exchange Server 2007-Installationsdateien abgeleitet.

Da durch diese Erweiterung mehr als 1000 Änderungen am Schema vorgenommen und diese Änderungen an alle Domänencontroller in Ihrer Gesamtstruktur repliziert werden, sollten Sie die Installation von Exchange Server 2007 an einem Zeitpunkt beginnen, zu dem das Netzwerk erwartungsgemäß nur wenig belastet ist, beispielsweise am Freitagabend. Durch eine solche Zeitplanung bleibt den Domänencontrollern genügend Zeit, um alle Schemaänderungen in ihre Datenbanken zu replizieren.

HINWEIS

Wenn Sie Exchange Server 2007 mit der Option **/prepare AD** installieren, werden zwar die neuen Objektklassen und -attribute in das Schema geschrieben, Exchange selbst aber nicht installiert. Für diesen Vorgang müssen Sie je nach Geschwindigkeit und Kapazität der Hardware in Ihrem System zwischen 30 und 90 Minuten einplanen. Je früher Sie bei einer Active Directory-Bereitstellung das Schema erweitern, umso besser, da die Domänencontroller das erweiterte Schema erben, wenn sie zu einer Gesamtstruktur hinzugefügt werden, was den Replikationsverkehr bei der Ausführung von **/prepare AD** verringert. Weitere Informationen zur Installation von Exchange Server 2007 finden Sie im Kapitel 6.

Auswirkungen der Grenzen von Gesamtstrukturen auf Exchange Server 2007

Da ein großer Teil der Informationen von Exchange Server 2007 in der Konfigurationsnamenspartition gespeichert wird, lässt sich eine Exchange Server 2007-Organisation nicht über die Grenzen der

Gesamtstruktur hinaus erweitern. In dieser Hinsicht wird die Exchange-Topologie direkt von der Struktur von Active Directory beeinflusst. Wenn Sie in einem Unternehmen mehrere Gesamtstrukturen haben, müssen Sie die folgenden Einschränkungen akzeptieren:

- Sie müssen getrennte Exchange-Organisationen verwalten.
- Sie haben getrennte globale Adresslisten, zwischen denen keine automatische Verzeichnisreplikation stattfindet.
- Die Funktionen des E-Mail-Systems sind nicht gesamtstrukturübergreifend verfügbar.

Eine gesamtstrukturübergreifende Authentifizierung ist jedoch möglich. Mehr darüber erfahren Sie in [Kapitel 21](#), »Exchange Server 2007-Nachrichten schützen«.

Obwohl die Verwendung einer einzelnen Gesamtstruktur der empfohlene Weg für die Erstellung einer Exchange-Organisation ist, können Sie Verzeichnisinformationen mehrerer Gesamtstrukturen synchronisieren und dabei eines der folgenden Szenarien verwenden:

- **Ressourcengesamtstruktur** Hierbei wird eine Gesamtstruktur zur Ausführung von Exchange Server 2007 bestimmt, die dann die Postfächer verwaltet. Zugehörige Benutzerkonten dieser Postfächer sind in separaten Gesamtstrukturen enthalten. Nachteilig hierbei sind die höheren Kosten für die Konfiguration der zusätzlichen Gesamtstrukturen, Domänencontroller und Exchange Server-Computer. Außerdem müssen Sie sicherstellen, dass in einer Gesamtstruktur erstellte Objekte entsprechende Platzhalterobjekte in der anderen erhalten.
- **Gesamtstrukturübergreifend** Exchange Server 2007 wird in mehreren Gesamtstrukturen ausgeführt, wobei eine E-Mail-Funktionalität zwischen diesen Gesamtstrukturen eingerichtet ist. Hauptsächlich liegt der Nachteil dieses Szenarios in der eingeschränkten E-Mail-Funktionalität zwischen den Gesamtstrukturen.

Konfigurationspartition und Verzeichnisdaten

Von allen Diensten in Active Directory nimmt ein Exchange Server-Computer am häufigsten den globalen Katalogserver zur Suche nach Adressen und die Konfigurationsnamenspartition zum Auffinden von Routinginformationen in Anspruch. Je nach Art der Anfrage, die der Exchange Server-Computer startet, können dabei auch zwei verschiedene Domänencontroller angesprochen werden.

Wenn ein Exchange Server-Computer startet, stellt er eine Reihe von LDAP-Verbindungen zu Domänencontrollern und globalen Katalogservern her. Falls er zum Weiterleiten einer Nachricht Routinginformationen benötigt, kann er diese Angaben von jedem beliebigen Domänencontroller abrufen, weil alle über eine vollständige Kopie der Konfigurationsnamenspartition verfügen. Braucht der Exchange Server-Computer dagegen die globale Adressliste, nimmt er Kontakt mit dem nächsten globalen Katalogserver auf. Die empfohlene Vorgehensweise besteht darin, einen globalen Katalogserver in der Nähe der Exchange Server-Computer aufzustellen und dafür zu sorgen, dass sie sich alle in demselben Standort und in derselben Domäne befinden.

DNS-Konfiguration

Im Internet (und auch in allen anderen TCP/IP-Netzwerken) wird jedes Gerät durch eine IP-Adresse in der vierteiligen, durch Punkte getrennten Dezimalschreibweise repräsentiert, beispielsweise 192.168.0.1. Ein Gerät mit TCP/IP-Adresse wird als *Host* bezeichnet und erhält einen Hostnamen, der aus Buchstaben besteht und für Menschen leichter zu erkennen und zu behalten ist als die numeri-

sche IP-Adresse. Das Format des Hostnamens lautet *hostname.domäne.com*. Wenn eine Ressource in einem TCP/IP-Netzwerk durch einen Hostnamen bezeichnet wird, müssen die Computer ihn in eine IP-Adresse umwandeln, da sie ausschließlich über IP-Adressen miteinander kommunizieren. Diese Umwandlung wird als *Namensauflösung* bezeichnet.

In TCP/IP-Netzwerken können die Hostnamen auf zwei verschiedene Weisen zu IP-Adressen aufgelöst werden. Bei der ersten Methode benötigt man eine so genannte Hosts-Datei. Dies ist eine einzelne, lineare Datei, in der lediglich die Hosts in einem Netzwerk zusammen mit ihren IP-Adressen aufgelistet sind. Wenn Sie SMTP mit einer Hosts-Datei verwenden wollen, müssen Sie den Domännennamen und die IP-Adresse der Hosts, an die IMS Nachrichten übermittelt, in die Datei eintragen. Dieser Vorgang kann ziemlich langwierig sein.

Die zweite Methode der Namensauflösung ist effizienter. Bei ihr wird das so genannte Domain Name System (DNS) herangezogen, eine hierarchisch strukturierte, verteilte Datenbank mit Hostnamen und IP-Adressen. Damit Sie Exchange Server 2007 ausführen können, müssen Sie zuvor Windows Server 2003 Active Directory und DNS-Dienste in Ihrem Netzwerk installiert haben. Aufgrund der Dynamik der neuen DNS-Implementierung werden Sie kaum noch Hosts-Dateien verwenden wollen, obwohl sie in Windows Server 2003 weiterhin zur Verfügung stehen.

Wahrscheinlich wünschen Sie, dass SMTP-Hosts außerhalb Ihres Netzwerks Nachrichten an Ihren SMTP-Dienst übertragen können. Zu diesem Zweck müssen Sie in der DNS-Datenbank zwei Einträge erstellen, damit die Hosts von außerhalb die IP-Adresse Ihres Servers auflösen können. Der erste Eintrag ist ein Adresseintrag für den Exchange Server-Computer. Er kann in Windows Server 2003 dynamisch bei DNS registriert werden. Der zweite Eintrag ist ein MX-Eintrag (Mail Exchanger), ein standardmäßiger DNS-Eintrag, in dem ein oder mehrere Hosts angegeben werden, die die E-Mail für eine Organisation bzw. einen Standort verarbeiten. Diesen Eintrag müssen Sie manuell in die DNS-Tabellen eingeben.

Weitere Informationen

Dieses Kapitel enthält nur grundlegende Informationen über die Konfiguration von TCP/IP und DNS, doch gibt es zu diesen Themen beinahe unerschöpfliches Material. Wenn Sie weitere Einzelheiten darüber benötigen, wie Sie TCP/IP und DNS in der Windows Server 2003-Umgebung verwenden können, lesen Sie beispielsweise *Microsoft Windows Server 2003 Administrator's Companion* von Charlie Russel, Sharon Crawford und Jason Gerend (Microsoft Press, 2006).

Zusammenfassung

In diesem Kapitel wurde beschrieben, wie Exchange Server 2007 in Windows Server 2003 integriert ist. Es gab einen Überblick über die Struktur von Active Directory und seine Zusammenarbeit mit Exchange Server 2007. Außerdem wurden die Internetinformationsprotokolle, die mit Windows Server 2003 installiert werden, und die in Exchange Server 2007 verfügbaren Dienste behandelt (wie beispielsweise Outlook Web Access). In Kapitel 3, »Architektur von Exchange Server 2007«, erfahren Sie mehr über die Exchange Server 2007-Architektur.