Kapitel 8

Die Hauptaufgaben bei der Active Directory-Administration

In diesem Kapitel:

Bei den Hauptaufgaben der Active Directory-Verwaltung handelt es sich im Wesentlichen um Routinearbeiten wie zum Beispiel das Erstellen von Computerkonten oder das Hinzufügen von Computern zu einer Domäne. In diesem Kapitel erhalten Sie Informationen über die Tools zur Verwaltung von Active Directory sowie über spezielle Techniken zur Verwaltung von Computern, Domänencontrollern und Organisationseinheiten.

Tools für die Verwaltung von Active Directory

Für die Verwaltung von Active Directory stehen die folgenden Gruppen von Tools zur Verfügung: grafische Verwaltungsprogramme, Befehlszeilenprogramme, Supporttools und Windows PowerShell-Cmdlets.

Active Directory-Verwaltungstools

Die Active Directory-Verwaltungstools werden als Snap-Ins für die Microsoft Management Console (MMC) bereitgestellt. Zur Verwaltung von Active Directory werden hauptsächlich eingesetzt:

- **Active Directory-Verwaltungscenter** Ermöglicht eine Verwaltung, die sich an den häufig ausgeführten Aufgaben orientiert.
- **Active Directory-Domänen und -Vertrauensstellungen** Dient zum Arbeiten mit Domänen, Domänenstrukturen und Domänengesamtstrukturen.
- **Active Directory-Modul für Windows PowerShell** Ermöglicht das Verwalten von Active Directory mit Windows PowerShell.
- **Active Directory-Standorte und -Dienste** Dient zur Verwaltung von Standorten und Subnetzen.
- **Active Directory-Benutzer und -Computer** Dient zur Verwaltung von Benutzern, Gruppen, Computern und Organisationseinheiten.
- **Gruppenrichtlinienverwaltung** Dient zur Verwaltung von Gruppenrichtlinien in der Organisation. Bietet Zugriff auf den Richtlinienergebnissatz für Zwecke der Modellierung und Protokollierung.

SICHERHEIT Die Windows-Firewall kann sich auf die Remoteverwaltung mit bestimmten MMC-Snap-Ins auswirken. Wenn die Windows-Firewall auf dem Remotecomputer aktiviert ist und Sie eine Fehlermeldung erhalten, die besagt, dass Sie nicht über die erforderlichen Rechte verfügen, der Netzwerkpfad nicht zu finden ist oder der Zugriff verweigert wird, müssen Sie auf dem Remotecomputer vielleicht eine Ausnahme für eingehende Übertragungen auf dem TCP-Port 445 konfigurieren. Sie können dieses Problem lösen, indem Sie die Richtlinieneinstellung *Windows Firewall: Remoteverwaltungsausnahme zulassen* unter *Computerkonfiguration\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen\Windows-Firewall\Domänenprofil* aktivieren. Oder Sie geben auf dem Remotecomputer in einer Eingabeaufforderung Folgendes ein: **netsh firewall set portopening tcp 445 smb enable**. Weitere Details finden Sie im Microsoft Knowledge Base-Artikel 840634 (*support.microsoft.com/default.aspx?scid=kb;en-us; 840634*).

Active Directory-Befehlszeilenprogramme

Es gibt mehrere Programme, mit denen Sie Active Directory über die Befehlszeile verwalten können. Dies sind unter anderem:

- **Adprep** Bereitet eine Windows-Gesamtstruktur oder -Domäne auf die Installation von Windows-Domänencontrollern vor. Verwenden Sie zur Vorbereitung einer Gesamtstruktur **adprep /forestprep** und zur Vorbereitung einer Domäne **adprep /domainprep**.

SICHERHEIT Unter Windows Server 2003 SP1 oder neuer werden die Gruppenrichtlinien einer Domäne nicht automatisch aktualisiert. Sie müssen zur Vorbereitung der Gruppenrichtlinien für die Domäne **adprep /domainprep /gpprep** verwenden. Dadurch werden die Einträge für die Zugriffssteuerung für alle Gruppenrichtlinienobjektordner im Verzeichnis *Sysvol* so geändert, dass ein Zugriff auf alle Domänencontroller des Unternehmens möglich ist. Das ist erforderlich, damit der Richtlinienergebnissatz der Standortrichtlinien bestimmt werden kann. Da diese Umstellung den Dateireplikationsdienst dazu veranlasst, erneut alle Gruppenrichtlinienobjekte an alle Domänencontroller zu senden, sollten Sie **adprep /domainprep /gpprep** nur nach sorgfältiger Planung anwenden.

- **Dsadd** Dient zum Hinzufügen von Computern, Kontakten, Gruppen, Organisationseinheiten und Benutzern zu Active Directory. Geben Sie auf der Befehlszeile **dsadd <*Objektname*> /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen, zum Beispiel: **dsadd computer /?**.
- **Dsget** Zeigt Eigenschaften von Computern, Kontakten, Gruppen, Organisationseinheiten, Benutzern, Standorten, Subnetzen und Servern an, die in Active Directory registriert sind. Geben Sie auf der Befehlszeile **dsget <*Objektname*> /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen. Beispiel: **dsget subnet /?**.
- **Dsmod** Ändert Eigenschaften von Computern, Kontakten, Gruppen, Organisationseinheiten, Benutzern und Servern, die bereits in Active Directory vorhanden sind. Geben Sie auf der Befehlszeile **dsmod <*Objektname*> /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen. Beispiel: **dsmod server /?**.
- **Dsmove** Verschiebt ein einzelnes Objekt innerhalb einer einzelnen Domäne an eine neue Position oder benennt das Objekt um, ohne es zu verschieben. Geben Sie auf der Befehlszeile **dsmove /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen.
- **Dsquery** Sucht mithilfe von Suchkriterien Computer, Kontakte, Gruppen, Organisationseinheiten, Benutzer, Standorte, Subnetze und Server in Active Directory. Geben Sie auf der Befehlszeile **dsquery /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen.
- **Dsrm** Entfernt Objekte aus Active Directory. Geben Sie auf der Befehlszeile **dsrm /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen.
- **Ntdsutil** Dient zum Anzeigen von Standort-, Domänen- und Serverinformationen, Verwalten von Betriebsmastern und Durchführen der Active Directory-Datenbankpflege. Geben Sie auf der Befehlszeile **ntdsutil /?** ein, um Hilfeinformationen zum Verwenden des Befehls anzuzeigen.

Active Directory-Supporttools

In Windows Server 2008 R2 sind viele Active Directory-Tools enthalten. Tabelle 8.1 listet einige der nützlichsten Supporttools für die Konfiguration, Verwaltung und Problembehebung von Active Directory auf.

Active Directory-Verwaltungscenter und Windows PowerShell

Das Active Directory-Verwaltungscenter (Abbildung 8.1) stellt eine Benutzeroberfläche zum Verwalten von Active Directory bereit, die sich an den häufig ausgeführten Aufgaben orientiert. Sie starten dieses Tool, indem Sie im Startmenü auf *Verwaltung* und dann auf *Active Directory-Verwaltungscenter* klicken. In diesem Tool können Sie folgende Aufgaben erledigen:

- Herstellen der Verbindung zu einer oder mehreren Domänen
- Anlegen und Verwalten von Benutzerkonten

- Anlegen und Verwalten von Gruppen
- Anlegen und Verwalten von Organisationseinheiten
- Durchführen einer globalen Suche in Active Directory

Tabelle 8.1 Kurzübersicht über die Active Directory-Supporttools

Supporttool	Ausführbare Datei	Beschreibung
Active Directory-Dienstschnittstelleneditor	Adsiedit.msc	Greift auf die Active Directory-Dienstschnittstellen für Domänen, Schemas und Konfigurationscontainer zu und bearbeitet sie.
Active Directory-Verwaltungsprogramm	Ldp.exe	Wendet LDAP-Vorgänge (Lightweight Directory Access Protocol) auf Active Directory an.
Dienstprogramm für die Verwaltung von Zugriffssteuerungslisten für Verzeichnisdienste	Dsacls.exe	Verwaltet Zugriffssteuerungslisten (Access Control List, ACL) für Objekte in Active Directory.
Dienstprogramm für das verteilte Dateisystem (DFS)	Dfsutil.exe	Verwaltet das verteilte Dateisystem (Distributed File System, DFS) und zeigt DFS-Informationen an.
Problembehebungstool für DNS-Server	Dnscmd.exe	Verwaltet die Eigenschaften von DNS-Servern, Zonen und Ressourceneinträgen.
Replikationsdiagnosetool	Repadmin.exe	Verwaltet und überwacht die Replikation über die Befehlszeile.
Windows-Domänen-Manager	Netdom.exe	Ermöglicht die Verwaltung von Domänen und Vertrauensstellungen über die Befehlszeile.

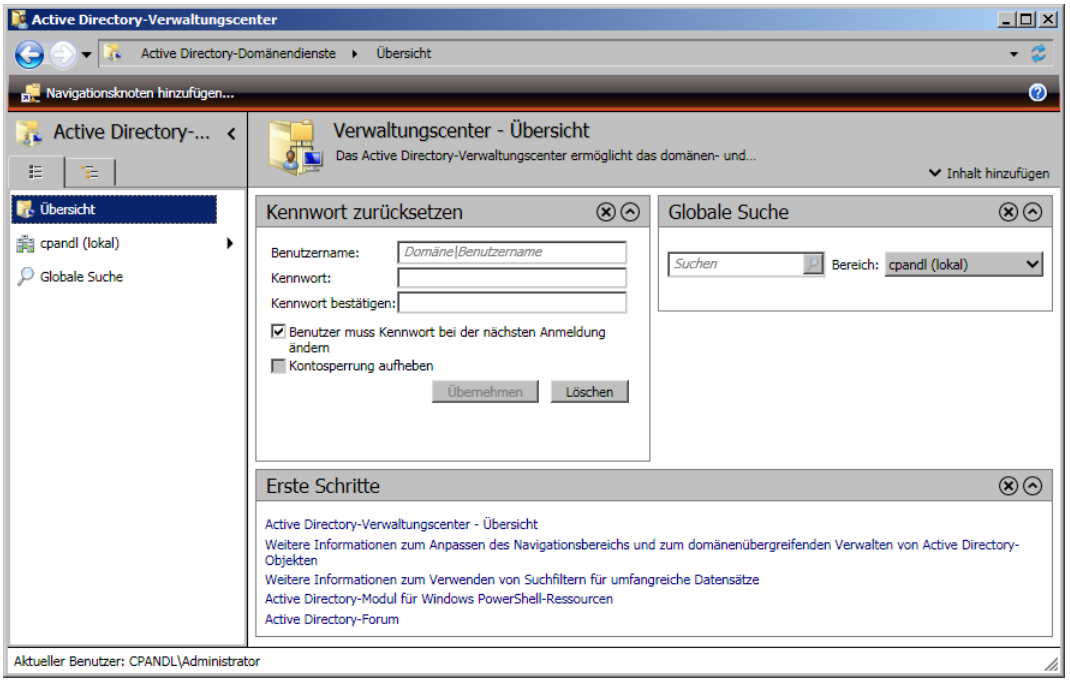

Abbildung 8.1 Durchführen von Verwaltungsaufgaben in Active Directory

Das Active Directory-Verwaltungscenter wird in Windows Server 2008 R2 standardmäßig installiert. In Windows 7 steht es zur Verfügung, wenn Sie die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) installieren. Dieses Tool greift auf Windows PowerShell zurück, um Verwaltungsaufgaben auszuführen, und setzt .NET Framework 3.5.1 voraus. Beide Features müssen installiert und richtig konfiguriert sein, damit Sie das Active Directory-Verwaltungscenter benutzen können.

Außerdem greift das Active Directory-Verwaltungscenter auf Webdienste zu, die von den Active Directory-Webdiensten (Active Directory Web Services, ADWS) zur Verfügung gestellt werden. Auf mindestens einem Domänencontroller in jeder Active Directory-Domäne, die Sie verwalten wollen, muss ADWS installiert sein, und die zugehörigen Dienste müssen laufen. Verbindungen werden in der Standardeinstellung über TCP-Port 9389 hergestellt, daher müssen Firewallrichtlinien für ADWS eine Ausnahme für diesen Port aktivieren.

Sie können Active Directory auch mit dem Active Directory-Modul für Windows PowerShell bearbeiten. Das Modul wird automatisch importiert, wenn Sie den entsprechenden Eintrag im Menü *Verwaltung* wählen. Andernfalls wird das Modul nicht standardmäßig in Windows PowerShell importiert, sodass Sie dies nachholen müssen, bevor Sie mit Active Directory-Cmdlets arbeiten können.

In der Windows PowerShell-Eingabeaufforderung importieren Sie das Active Directory-Modul, indem Sie **Import-Module ActiveDirectory** eingeben. Sobald das Modul einmal importiert ist, können Sie es in der momentan laufenden Instanz von Windows PowerShell einsetzen. Wenn Sie Windows PowerShell das nächste Mal neu starten, müssen Sie das Modul erneut importieren, wenn Sie seine Features brauchen. Stattdessen können Sie auch im Menü *Verwaltung* den Eintrag *Active Directory-Modul für Windows PowerShell* wählen, dann wird das Modul direkt beim Start von Windows PowerShell geladen.

In der Windows PowerShell-Eingabeaufforderung erhalten Sie eine Liste aller verfügbaren Cmdlets, wenn Sie den Befehl **get-command** eingeben. Mit *Get-Help* bekommen Sie weitere Informationen darüber, wie Cmdlets benutzt werden. Wenn Sie **get-help** *-* eingeben, erhalten Sie eine Liste aller Cmdlets, jeweils mit einer kurzen Beschreibung. Die Dokumentation zu einem bestimmten Cmdlet zeigen Sie an, indem Sie **get-help** gefolgt vom Namen des Cmdlets eingeben. Es gibt mehrere Dutzend Active Directory-Cmdlets, eine Liste derer, die Sie am häufigsten brauchen, wird angezeigt, wenn Sie in der Windows PowerShell-Eingabeaufforderung den Befehl **get-help *-ad*** ausführen.

HINWEIS Das Active Directory-Modul für Windows PowerShell wird in Windows Server 2008 R2 standardmäßig installiert. In Windows 7 steht es zur Verfügung, wenn Sie die Remoteserver-Verwaltungstools installieren und die entsprechenden Optionen auswählen. Windows PowerShell benötigt .NET Framework 3.5.1 und Windows-Remoteverwaltung (WinRM), um administrative Aufgaben auszuführen.

Arbeiten mit der Konsole *Active Directory-Benutzer und -Computer*

Active Directory-Benutzer und -Computer ist das Hauptverwaltungstool für Active Directory. Sie führen damit alle benutzer-, gruppen- und computerbezogenen Aufgaben durch und verwalten Organisationseinheiten.

Sie können *Active Directory-Benutzer und -Computer* durch Auswählen der entsprechenden Option im Menü *Verwaltung* starten. Es lässt sich jedoch auch als Snap-In zu jeder aktualisierbaren Konsole hinzufügen.

Erste Schritte mit *Active Directory-Benutzer und -Computer*

Standardmäßig arbeitet *Active Directory-Benutzer und -Computer* mit der Domäne, mit der Ihr Computer gerade verbunden ist. Sie können, wie in Abbildung 8.2 dargestellt, über die Konsolenstruktur auf Computer- und Benutzerobjekte zugreifen. Falls Sie jedoch keinen Domänencontroller finden oder die gewünschte Domäne nicht angezeigt wird, müssen Sie gegebenenfalls eine Verbindung zu einem Domänencontroller in der aktuellen oder in einer anderen Domäne herstellen. Andere Arbeiten, die sich ebenfalls mit *Active Directory-Benutzer und -Computer* durchführen lassen, sind die Anzeige erweiterter Optionen oder die Suche nach Objekten.

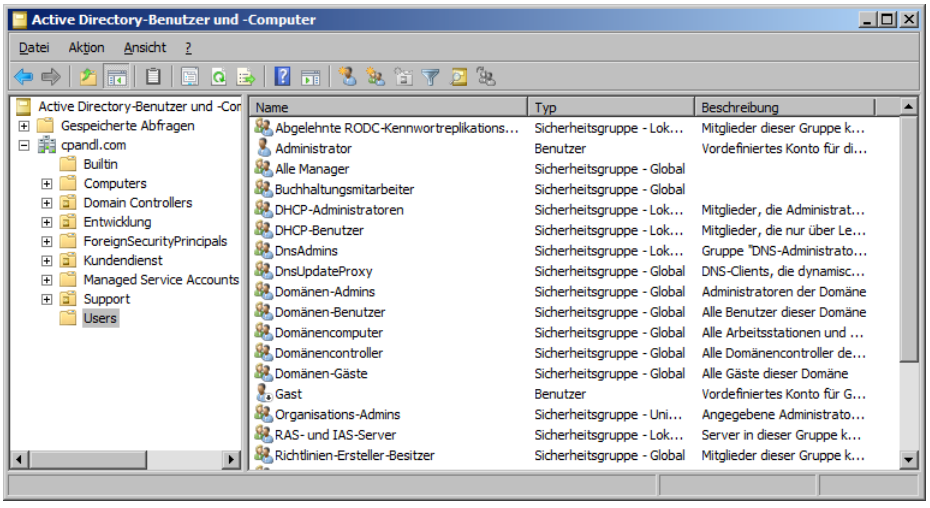

Abbildung 8.2 Beim Arbeiten mit *Active Directory-Benutzer und -Computer* können Sie über die Konsolenstruktur auf Computer- und Benutzerobjekte zugreifen

Wenn Sie in *Active Directory-Benutzer und -Computer* auf eine Domäne zugreifen, werden Sie feststellen, dass eine Reihe von Standardordnern verfügbar ist. Dazu zählen folgende Ordner:

- **Builtin** Die Liste vordefinierter Benutzer- und Gruppenkonten.
- **Computers** Der Standardcontainer für Computerkonten.
- **Domain Controllers** Der Standardcontainer für Domänencontroller.
- **ForeignSecurityPrincipals** Enthält Informationen zu Objekten in einer vertrauenswürdigen externen Domäne. Diese Objekte werden normalerweise erstellt, wenn ein Objekt aus einer externen Domäne zu einer Gruppe in der aktuellen Domäne hinzugefügt wird.
- **Managed Service Accounts** Der Standardcontainer für verwaltete Dienstkonten.
- **Microsoft Exchange Security Groups** Der Standardcontainer für Gruppen, die von Microsoft Exchange Server benutzt werden. Dieser Ordner wird nur aufgelistet, wenn Exchange Server in der Umgebung läuft.
- **Gespeicherte Abfragen** Enthält gespeicherte Suchkriterien, damit Sie zuvor durchgeführte Active Directory-Suchen schnell nochmals ausführen können.
- **Users** Der Standardcontainer für Benutzer.

Active Directory-Benutzer und -Computer bietet erweiterte Optionen, die standardmäßig nicht angezeigt werden. Um diese Optionen anzuzeigen, klicken Sie auf *Ansicht* und wählen *Erweiterte Funktionen*. Nun werden die folgenden Ordner angezeigt:

- **LostAndFound** Enthält verwaiste Objekte. Diese können Sie löschen oder wiederherstellen.
- **NTDS Quotas** Enthält Kontingentdaten für den Verzeichnisdienst.
- **Program Data** Enthält gespeicherte Active Directory-Daten für Microsoft-Anwendungen.
- **System** Enthält vordefinierte Systemeinstellungen.

Sie können auch Ordner für Organisationseinheiten hinzufügen. In Abbildung 8.2 wurden vom Administrator mehrere Organisationseinheiten in der Domäne *cpandl.com* erstellt.

Herstellen einer Verbindung zu einem Domänencontroller

Die Verbindungsherstellung zu einem Domänencontroller dient mehreren Zwecken. Wenn nach dem Starten von *Active Directory-Benutzer und -Computer* keine Objekte verfügbar sind, können Sie eine Verbindung zu einem Domänencontroller herstellen, um auf Benutzer-, Gruppen- und Computerobjekte aus der aktuellen Domäne zuzugreifen. Sie können eine Verbindung zu einem Domänencontroller auch dann herstellen, wenn Sie befürchten, dass die Replikation nicht ordnungsgemäß funktioniert und Sie die Objekte auf einem bestimmten Controller untersuchen möchten. Nach dem Aufbau der Verbindung suchen Sie nach Unstimmigkeiten in den zuletzt aktualisierten Objekten.

Um eine Verbindung zu einem Domänencontroller herzustellen, gehen Sie wie folgt vor:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Active Directory-Benutzer und -Computer*. Wählen Sie danach *Domänencontroller ändern* aus.

   Im Dialogfeld *Verzeichnisserver ändern* werden die aktuelle Domäne und der Domänencontroller angezeigt, mit dem Sie arbeiten.
2. Im Feld *Wechseln zu* werden die in der Domäne verfügbaren Controller aufgeführt. Standardmäßig ist *Beliebiger schreibbarer Domänencontroller* ausgewählt. Wenn Sie diese Option auswählen, wird eine Verbindung zu dem Domänencontroller hergestellt, der als erster auf Ihre Anforderung antwortet. Andernfalls wählen Sie einen bestimmten Domänencontroller, mit dem eine Verbindung hergestellt werden soll. Klicken Sie auf *OK*.
3. Falls Sie stets diesen Domänencontroller verwenden wollen, wenn Sie mit *Active Directory-Benutzer und -Computer* arbeiten, können Sie das Kontrollkästchen *Diese Einstellung für die aktuelle Konsole speichern* aktivieren und auf *OK* klicken. Klicken Sie andernfalls einfach auf *OK*.

HINWEIS Das Dialogfeld *Verzeichnisserver ändern* zeigt jetzt den Standort an, der mit den Domänencontrollern verknüpft ist, und zusätzlich Typ, Version und Status eines Domänencontrollers. Falls der Typ des Domänencontrollers als »GC« aufgeführt ist, hostet dieser Domänencontroller auch einen globalen Katalog.

Herstellen einer Verbindung zu einer Domäne

In *Active Directory-Benutzer und -Computer* können Sie mit jeder beliebigen Domäne der Gesamtstruktur arbeiten, vorausgesetzt, Sie besitzen die erforderlichen Zugriffsrechte. Um eine Verbindung zu einer Domäne herzustellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf *Active Directory-Benutzer und -Computer*. Wählen Sie danach *Domäne ändern* aus.

2. Im Dialogfeld *Domäne ändern* wird die aktuelle (oder standardmäßige) Domäne angezeigt. Geben Sie einen neuen Domänennamen ein, oder klicken Sie auf *Durchsuchen*, wählen Sie anschließend im Dialogfeld *Domäne suchen* eine Domäne aus und klicken Sie auf *OK*.
3. Falls Sie stets diese Domäne verwenden wollen, wenn Sie mit *Active Directory-Benutzer und -Computer* arbeiten, können Sie das Kontrollkästchen *Diese Domäneneinstellung für die aktuelle Konsole speichern* aktivieren und auf *OK* klicken. Klicken Sie andernfalls einfach auf *OK*.

Suchen nach Konten und freigegebenen Ressourcen

Active Directory-Benutzer und -Computer enthält eine vordefinierte Funktion für die Suche nach Konten, freigegebenen Ressourcen und anderen Verzeichnisobjekten. Auf einfache Weise lassen sich die aktuelle Domäne, eine bestimmte Domäne oder das gesamte Verzeichnis durchsuchen.

Um nach Verzeichnisobjekten zu suchen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf die aktuelle Domäne oder auf einen bestimmten Container, der durchsucht werden soll. Wählen Sie anschließend *Suchen* aus. Ein Suchdialogfeld wie in Abbildung 8.3 wird geöffnet.

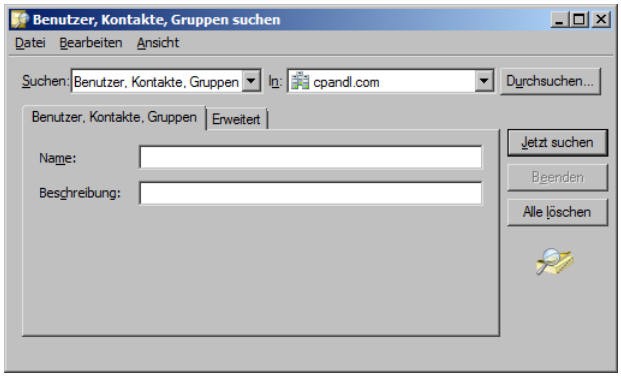

Abbildung 8.3 Im Dialogfeld *Suchen* können Sie nach Ressourcen in Active Directory suchen

2. Wählen Sie in der Auswahlliste *Suchen* die Art der Suche aus. Es sind folgende Optionen verfügbar:
   - **Benutzer, Kontakte und Gruppen** Suche nach Benutzer- und Gruppenkonten sowie nach im Verzeichnisdienst aufgelisteten Kontakten
   - **Computer** Suche nach Computerkonten über Typ, Name und Besitzer
   - **Drucker** Suche nach Druckern über Name, Modell und Eigenschaften
   - **Freigegebene Ordner** Suche nach freigegebenen Ordnern über Name oder Schlüsselwort
   - **Organisationseinheiten** Suche nach Organisationseinheiten über Name
   - **Benutzerdefinierte Suche** Durchführen einer erweiterten Suche oder LDAP-Abfrage
   - **Allgemeine Abfragen** Ermöglicht eine Schnellsuche nach Kontonamen, Kontobeschreibungen, deaktivierten Konten, nicht ablaufenden Kennwörtern und Tagen seit der letzten Anmeldung.
3. Wählen Sie in der Dropdownliste *In* den zu durchsuchenden Ort. Wenn Sie mit der rechten Maustaste auf einen Container, zum Beispiel *Computer*, geklickt haben, ist dieser standardmäßig ausgewählt. Um alle Objekte im Verzeichnis zu durchsuchen, wählen Sie *Gesamtes Verzeichnis* aus.

4. Klicken Sie nach Eingabe der Suchparameter auf *Jetzt suchen*. Wie in Abbildung 8.4 dargestellt, werden alle Treffer in der Ansicht *Suchergebnisse* angezeigt. Doppelklicken Sie auf ein Objekt, um seine Eigenschaften anzuzeigen oder sie zu ändern. Klicken Sie mit der rechten Maustaste auf das Objekt, um ein Kontextmenü für seine Verwaltung anzuzeigen.

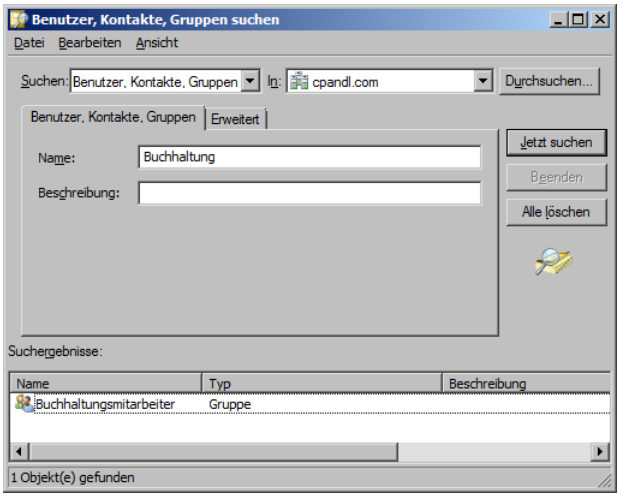

Abbildung 8.4 In der Ansicht *Suchergebnisse* werden übereinstimmende Objekte angezeigt, die Sie durch Klicken mit der rechten Maustaste auf den entsprechenden Eintrag verwalten können

HINWEIS Die Art der Suche bestimmt, welche Felder und Registerkarten im Dialogfeld *Suchen* verfügbar sind. In den meisten Fällen werden Sie einfach den Namen des zu suchenden Objekts in das Feld *Name* eingeben. Es gibt jedoch auch andere Suchoptionen. Beispielsweise können Sie bei Druckern nach einem Farbdrucker suchen, nach einem Drucker, der beidseitig drucken kann, nach einem, der klammern kann, und so weiter.

Verwalten von Computerkonten

Computerkonten werden in Active Directory als Objekte gespeichert. Mit ihrer Hilfe steuern Sie den Zugriff auf das Netzwerk und dessen Ressourcen. Computerkonten können Sie zu jedem in *Active Directory-Benutzer und -Computer* angezeigten Container hinzufügen. Am besten verwenden Sie dazu die Ordner *Computers*, *Domain Controllers* und beliebige von Ihnen erstellte Organisationseinheiten.

Erstellen von Computerkonten auf Arbeitsstationen und Servern

Am einfachsten erstellen Sie ein Computerkonto, indem Sie sich an dem zu konfigurierenden Computer anmelden und einer Domäne beitreten, wie im Abschnitt »Hinzufügen eines Computers zu einer Domäne« auf Seite 263 beschrieben. Dabei wird das erforderliche Computerkonto automatisch erstellt und im Ordner *Computers* beziehungsweise *Domain Controllers* abgelegt. In *Active Directory-Benutzer und -Computer* können Sie Computerkonten auch erstellen, bevor Sie versuchen, den Computer zu installieren.

Erstellen von Computerkonten in *Active Directory-Benutzer und -Computer*

Sie können zwei Arten von Computerkonten erstellen: Standardcomputerkonten und verwaltete Computerkonten. Mit *Active Directory-Benutzer und -Computer* lassen sich Standardcomputerkonten wie folgt erstellen:

1. Klicken Sie in der Konsolenstruktur von *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf den Container, in dem das Computerkonto angelegt werden soll. Wählen Sie zunächst *Neu* und klicken Sie dann auf *Computer*. Das in Abbildung 8.5 dargestellte Dialogfeld *Neues Objekt – Computer* wird angezeigt.
2. Geben Sie den Namen des Computers ein.

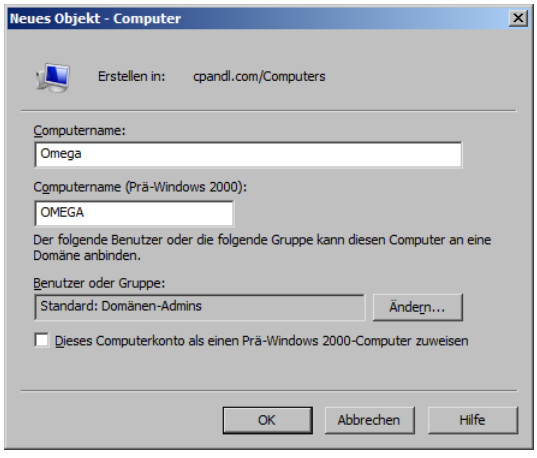

Abbildung 8.5 Erstellen Sie im Dialogfeld *Neues Objekt – Computer* neue Computerkonten

3. Standardmäßig dürfen nur Mitglieder der Gruppe *Domänen-Admins* Computer zur Domäne hinzufügen. Um einem anderen Benutzer oder einer anderen Gruppe die Erlaubnis dazu zu erteilen, klicken Sie auf *Ändern*. Wählen Sie danach im Dialogfeld *Benutzer oder Gruppe wählen* ein Benutzer- oder Gruppenkonto aus.

HINWEIS Sie können ein beliebiges vorhandenes Benutzer- beziehungsweise Gruppenkonto auswählen. Damit wird die Berechtigung delegiert, diesen Computer zur Domäne hinzuzufügen.

4. Wenn Windows NT-Systeme dieses Konto verwenden, aktivieren Sie *Dieses Computerkonto als einen Prä-Windows 2000-Computer zuweisen*.
5. Sofern die Windows-Bereitstellungsdienste nicht installiert sind, müssen Sie auf *OK* klicken, um das Computerkonto anzulegen. Klicken Sie andernfalls zweimal auf *Weiter* und dann auf *Fertig stellen*.

Wenn Sie mit Remoteinstallationsservern und Windows-Bereitstellungsdiensten arbeiten, werden verwaltete Computerkonten benutzt, um Computerkonten vorzubereiten, sodass ein Computer automatisch installiert werden kann. In *Active Directory-Benutzer und -Computer* können Sie ein verwaltetes Computerkonto folgendermaßen erstellen:

1. Führen Sie die Schritte 1 bis 4 aus der vorhergehenden Anleitung durch. Klicken Sie auf *Weiter*, um die Seite *Verwaltet* anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen *Verwalteter Computer* und geben Sie die GUID/UUID (Globally Unique Identifier/Universally Unique Identifier) des Computers ein. Sie finden die GUID/UUID im System-BIOS oder auf dem Computergehäuse. Klicken Sie auf *Weiter*.
3. Auf der Seite *Hostserver* können Sie angeben, welcher Hostserver verwendet werden soll. Sie können auch festlegen, dass für die Remoteinstallation ein beliebiger verfügbarer Hostserver verwendet wird. Wählen Sie *Folgender Remoteinstallationsserver*, wenn Sie einen Hostserver angeben wollen. Klicken Sie im Dialogfeld *Suchen* auf *Jetzt suchen*, um eine Liste aller Remoteinstallationsserver in der Organisation anzuzeigen. Klicken Sie auf den gewünschten Hostserver und dann auf *OK*, um das Dialogfeld *Suchen* zu schließen.
4. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Anzeigen und Bearbeiten von Computerkontoeigenschaften

Zum Anzeigen und Bearbeiten von Computerkontoeigenschaften gehen Sie wie folgt vor:

1. Öffnen Sie *Active Directory-Benutzer und -Computer*. Erweitern Sie in der Konsolenstruktur den Domänenknoten.
2. Wählen Sie den Container oder die Organisationseinheit, in der sich das Computerkonto befindet.
3. Klicken Sie mit der rechten Maustaste auf das gewünschte Konto und wählen Sie *Eigenschaften* aus. Ein Eigenschaftendialogfeld wird angezeigt, in dem Sie die Einstellungen anzeigen und bearbeiten können.

Löschen, Deaktivieren und Aktivieren von Computerkonten

Wenn ein Computerkonto nicht mehr benötigt wird, können Sie es endgültig aus Active Directory löschen. Sie können es auch vorübergehend deaktivieren und später gegebenenfalls wieder aktivieren.

Zum Löschen, Deaktivieren oder Aktivieren von Computerkonten gehen Sie wie folgt vor:

1. Öffnen Sie *Active Directory-Benutzer und -Computer*. Klicken Sie in der Konsolenstruktur auf den Container, in dem sich das Computerkonto befindet. Klicken Sie anschließend mit der rechten Maustaste auf den Computer. Sie haben nun folgende Befehle zur Auswahl:
   - Wählen Sie *Löschen* aus, um das Konto endgültig zu löschen, und bestätigen Sie den Vorgang, indem Sie auf *Ja* klicken.
   - Wählen Sie *Konto deaktivieren* aus, um das Konto vorübergehend zu deaktivieren, und bestätigen Sie den Vorgang, indem Sie auf *Ja* klicken. Ein roter Kreis mit einem X zeigt an, dass das Konto deaktiviert ist.
   - Wählen Sie *Konto aktivieren* aus, um das Konto für die Wiederverwendung zu aktivieren.

TIPP Wenn das Konto gerade verwendet wird, können Sie es möglicherweise nicht deaktivieren. Fahren Sie den Computer herunter oder trennen Sie die Verbindung der Computersitzung im Ordner *Sitzungen* in *Computerverwaltung*.

Zurücksetzen gesperrter Computerkonten

Wie Benutzerkonten haben Computerkonten Kennwörter. Doch im Gegensatz zu Benutzerkonten werden die Kennwörter von Computerkonten automatisch verwaltet und gepflegt. Um diese automatische Verwaltung durchzuführen, speichern Computer in der Domäne ein Kennwort für ein Computerkonto, das standardmäßig alle 30 Tage gesperrt wird, und ein Kennwort für einen sicheren Kanal zum Einrichten sicherer Kommunikationsverbindungen mit Domänencontrollern. Das Kennwort für den sicheren Kanal wird ebenfalls standardmäßig alle 30 Tage aktualisiert. Beide Kennwörter müssen synchronisiert sein. Wenn das Kennwort für den sicheren Kanal und das Kennwort für das Computerkonto nicht mehr synchronisiert sind, kann sich der Computer nicht bei der Domäne anmelden. Außerdem wird ein Domänenauthentifizierungsfehler für den Anmeldedienst mit der Ereigniskennung 3210 oder 5722 protokolliert.

Falls dies geschieht, müssen Sie das Kennwort für das Computerkonto zurücksetzen. Eine Möglichkeit wäre, das Computerkonto in *Active Directory-Benutzer und -Computer* mit der rechten Maustaste anzuklicken und *Konto zurücksetzen* zu wählen. Anschließend müssen Sie den Computer aus der Domäne entfernen (indem Sie den Computer zum Mitglied einer Arbeitsgruppe oder einer anderen Domäne machen) und ihn dann wieder in die Domäne aufnehmen. Dafür können Sie das Befehlszeilenprogramm Netdom verwenden, um das Kennwort eines Computers zurückzusetzen. Einzelheiten finden Sie im Microsoft Knowledge Base-Artikel 325850 (*support.microsoft.com/default.aspx?scid=kb;en-us;325850*).

Für einen Mitgliedserver können Sie das Kennwort des Computerkontos folgendermaßen zurücksetzen:

1. Melden Sie sich lokal auf dem Computer an. Geben Sie in einer Eingabeaufforderung **netdom resetpwd /s:<*ServerName*> /ud:<*Domäne\Benutzername*> /pd:*** ein. Darin ist <*ServerName*> der Name des Domänencontrollers, mit dem das Kennwort festgelegt werden soll, und <*Domäne\Benutzername*> gibt ein Administratorkonto an, das über die Berechtigung zum Ändern des Kennworts verfügt. Das Sternchen (*) weist Netdom an, Sie zur Eingabe des Kennworts für das Konto aufzufordern.
2. Geben Sie Ihr Kennwort ein, wenn Sie dazu aufgefordert werden. Netdom ändert dann das Kennwort des Computerkontos lokal und auf dem Domänencontroller. Anschließend leitet der Domänencontroller die Kennwortänderung an die anderen Domänencontroller der Domäne weiter.
3. Starten Sie den Computer neu.

Für Domänencontroller sind noch weitere Schritte erforderlich. Nachdem Sie sich lokal angemeldet haben, müssen Sie den Dienst *Kerberos-Schlüsselverteilungscenter* beenden und seinen Starttyp auf Manuell stellen. Nachdem Sie den Computer neu gestartet und sich überzeugt haben, dass das Kennwort erfolgreich zurückgesetzt wurde, können Sie den Dienst *Kerberos-Schlüsselverteilungscenter* neu starten und seinen Starttyp auf Automatisch zurücksetzen.

Verschieben von Computerkonten

Computerkonten werden normalerweise in den Containern *Computers*, *Domain Controllers* oder in Containern benutzerdefinierter Organisationseinheiten abgelegt. Sie können ein Konto in einen anderen Container verschieben, indem Sie in *Active Directory-Benutzer und -Computer* das Computerkonto auswählen und das Konto mit der Maus an den neuen Speicherort ziehen.

Die folgenden Schritte beschreiben eine andere Methode zum Verschieben von Computerkonten:

1. Öffnen Sie *Active Directory-Benutzer und -Computer*.
2. Klicken Sie in der Konsolenstruktur auf den Container, in dem sich das Computerkonto befindet.

3. Klicken Sie mit der rechten Maustaste auf das zu verschiebende Konto und wählen Sie anschließend die Option *Verschieben* aus. Das in Abbildung 8.6 dargestellte Dialogfeld *Verschieben* wird angezeigt.

Abbildung 8.6 Mithilfe des Dialogfelds *Verschieben* können Sie Computerkonten in andere Container verschieben

4. Erweitern Sie in diesem Dialogfeld den Domänenknoten und klicken Sie anschließend auf den Container, in den der Computer verschoben werden soll. Klicken Sie auf *OK*.

Verwalten von Computern

Wie der Name sagt, verwalten Sie Computer mithilfe der Computerverwaltung. Wenn Sie mit *Active Directory-Benutzer und -Computer* arbeiten, klicken Sie im Ansichtsfenster mit der rechten Maustaste auf den Eintrag eines Computers und wählen *Verwalten* aus, um die Computerverwaltung zu öffnen und direkt eine Verbindung zu einem bestimmten Computer herzustellen.

Hinzufügen eines Computers zu einer Domäne oder Arbeitsgruppe

Nach dem Hinzufügen eines Computers zu einer Domäne oder Arbeitsgruppe können sich Windows NT-, Windows 2000-, Windows XP-, Windows Server 2003-, Windows Vista-, Windows 7-, Windows Server 2008- und Windows Server 2008 R2-Computer an einem Netzwerk anmelden und auf dieses zugreifen. Windows 95- und Windows 98-Computer benötigen keine Computerkonten und treten dem Netzwerk nicht auf diese Weise bei. Bei Windows 95 und Windows 98 müssen Sie den Computer als Active Directory-Client konfigurieren.

Bevor Sie beginnen, stellen Sie sicher, dass die Netzwerkkomponenten ordnungsgemäß auf dem Computer installiert sind. Dies sollte während des Einrichtens des Betriebssystems geschehen sein. Genaue Informationen über das Konfigurieren von TCP/IP-Verbindungen finden Sie in Kapitel 17, »Verwalten von TCP/IP-Netzwerken«. Die TCP/IP-Einstellungen müssen richtig sein und die Kommunikation zwischen dem Computer, den Sie konfigurieren, und einem Controller in der Domäne erlauben. Wenn DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Naming Service) und DNS ordnungsgemäß im Netzwerk installiert sind, müssen Arbeitsstationen keine statischen IP-Adressen zugewiesen bekommen oder diese nicht speziell konfiguriert werden. Die einzigen Voraussetzungen sind ein Computer- und ein Domänenname, die Sie angeben, wenn Sie den Computer zur Domäne hinzufügen.

PRAXISTIPP Windows Server 2008 R2 erteilt der impliziten Benutzergruppe *Authentifizierte Benutzer* automatisch das Benutzerrecht *Hinzufügen von Arbeitsstationen zur Domäne*. Dies bedeutet, dass ein Benutzer, der sich bei der Domäne als Benutzer anmeldet und authentifiziert ist, ohne Administratorrechte Arbeitsstationen zur Domäne hinzufügen kann. Als Sicherheitsmaßnahme darf ein solcher Benutzer jedoch höchstens 10 Arbeitsstationen zur Domäne hinzufügen. Falls ein authentifizierter Benutzer diesen Grenzwert überschreitet, wird eine Fehlermeldung angezeigt. Bei Windows NT-Arbeitsstationen lautet die Meldung »Das Computer-Konto für diesen Computer existiert nicht, oder es kann nicht darauf zugegriffen werden«. Bei Windows 2000- und Windows XP-Arbeitsstationen lautet die Meldung »Der Computer konnte der Domäne nicht beitreten. Die maximale Anzahl der Computerkonten, die in dieser Domäne erstellt werden können, wurde überschritten.« Obgleich Sie mithilfe des Programms *Ldp.exe* aus den Windows Server 2008 R2-Supporttools den Standardgrenzwert der Anzahl der Computer ändern können, die ein authentifizierter Benutzer zu einer Domäne hinzufügen kann (mit dem Attribut ms-DS-MachineAccountQuota), ist dies aus Sicherheitsgründen nicht ratsam. Eine bessere Methode ist bei Sicherheitsbedenken die Voraberstellung des benötigten Computerkontos in einer bestimmten Organisationseinheit oder das Erteilen der erweiterten Sicherheitsberechtigung zum Erstellen von Computerobjekten in einer bestimmten Organisationseinheit an den Benutzer.

Während der Betriebssysteminstallation wurde wahrscheinlich eine Netzwerkverbindung für den Computer konfiguriert. Möglicherweise haben Sie den Computer auch bereits zu einer Domäne oder einer Arbeitsgruppe hinzugefügt. In diesem Fall können Sie den Computer zu einer neuen Domäne oder Arbeitsgruppe hinzufügen. Im Abschnitt »Die Registerkarte Computername« auf Seite 93 ist beschrieben, wie Sie einen Windows Vista-, Windows 7-, Windows Server 2008- oder Windows Server 2008 R2-Computer zu einer Domäne hinzufügen. Für Windows 2000 Professional-, Windows 2000 Server-, Windows XP Professional- und Windows Server 2003-Computer ist der Ablauf praktisch derselbe. Der einzige wesentliche Unterschied ist, dass Sie in der Systemsteuerung auf *System und Sicherheit* und dann *System* klicken können, um das Dialogfeld *Systemeigenschaften* direkt zu öffnen.

Falls die Namensänderung nicht erfolgreich war, erhalten Sie entweder eine Meldung über das Fehlschlagen der Änderung, oder es wird eine Meldung angezeigt, die Sie darüber informiert, dass die Anmeldeinformationen bereits existieren. Dieses Problem kann auftreten, wenn Sie den Namen eines Computers ändern, der bereits mit einer Domäne verbunden ist, und wenn auf dem Computer Sitzungen in dieser Domäne aktiv sind. Schließen Sie die Anwendungen, die mit der Domäne verbunden sind, zum Beispiel Windows-Explorer, falls diese Anwendung über das Netzwerk auf einen freigegebenen Ordner zugreift. Wiederholen Sie danach den Vorgang.

Wenn Sie andere Probleme beim Beitritt zu einer Domäne haben, stellen Sie sicher, dass der zu konfigurierende Computer über die entsprechende Netzwerkkonfiguration verfügt. Auf dem Computer müssen die Netzwerkdienste installiert sein, und die TCP/IP-Einstellungen müssen über die korrekten DNS-Servereinstellungen verfügen, wie in Kapitel 17 beschrieben.

Verwenden des Offlinebeitritts zur Domäne

Computer, die unter Windows 7 Professional, Enterprise oder Ultimate Edition oder irgendeiner Edition von Windows Server 2008 R2 laufen, unterstützen den Offlinebeitritt zur Domäne. Das zugehörige Dienstprogramm, *Djoin.exe*, ist in diesen Windows-Versionen enthalten. Alle Mitglieder der Gruppe *Domänen-Admins* können Offlinebeitritte zur Domäne durchführen (wie auch alle anderen Konten, denen die entsprechenden Benutzerrechte zugewiesen wurden).

Sie gehen im Prinzip folgendermaßen vor, um einen Offlinebeitritt zur Domäne durchzuführen:

1. Sie legen das Computerkonto in Active Directory an und erzwingen die Replikation des gemeinsamen geheimen Schlüssels des Computers, der der Domäne beitreten soll.

2. Sie schreiben die benötigten Zustandsinformationen, die der Computer braucht, um der Domäne beizutreten, in eine Textdatei und machen Sie auf dem Computer verfügbar.
3. Sobald der Computer startet, liest Windows die Bereitstellungsdaten und fügt den Computer zur Domäne hinzu.

Sie führen *Djoin.exe* in einer Administratoreingabeaufforderung aus, um die Metadaten für das Computerkonto bereitzustellen. Die Metadaten des Computerkontos werden in eine *.txt*-Datei geschrieben. Nach der Bereitstellung des Computers können Sie *Djoin.exe* erneut ausführen, um die Metadaten des Computerkontos abzurufen und in das Windows-Verzeichnis des Zielcomputers einzufügen. Stattdessen können Sie die Metadaten des Computerkontos in einer *Unattend.xml*-Datei speichern und dann während einer unbeaufsichtigten Betriebssysteminstallation diese *Unattend.xml*-Datei verwenden.

Gehen Sie folgendermaßen vor, wenn Sie eine *.txt*-Datei für die Bereitstellung verwenden:

1. Melden Sie sich unter einem Konto, das die Berechtigung hat, Computer zur Domäne hinzuzufügen, an einem Computer an, der Mitglied dieser Domäne ist.
2. Erstellen Sie mit *Djoin.exe* eine Textdatei, die die Metadaten des Computerkontos enthält. Geben Sie dazu in einer Administratoreingabeaufforderung **djoin /provision /domain <*Domänenname*> /machine <*Computername*> /savefile <*Dateiname*>**, wobei <*Domänenname*> der Name der Domäne ist, zu der Sie den Computer hinzufügen, <*Computername*> der Name des Computers und <*Dateiname*> der Name der *.txt*-Datei, in der die Metadaten gespeichert werden sollen. Hier ein Beispiel:

   ```
   djoin /provision /domain cpandl /machine HrComputer15 /savefile Hrcomputer15.txt
   ```

TIPP In der Standardeinstellung werden Computerkonten im Container *Computers* erstellt. Falls Sie einen anderen Container verwenden wollen, können Sie das Argument */Machineou* hinzufügen und den gewünschten Container angeben. Wurde das Computerkontoobjekt bereits erstellt, können Sie die benötigten Metadaten generieren, indem Sie das Argument */reuse* anhängen. Wenn Ihr Domänencontroller noch nicht unter Windows Server 2008 R2 läuft, müssen Sie das Argument */downlevel* angeben.

3. Importieren Sie die *.txt*-Datei auf dem neuen Computer mit *Djoin.exe*. Geben Sie dazu in einer Administratoreingabeaufforderung den Befehl **djoin /requestODJ /loadfile <*Dateiname*> /windowspath %SystemRoot% /localosCaution** ein, wobei <*Dateiname*> der Name der Metadatendatei ist. Ein Beispiel:

   ```
   djoin /requestODJ /loadfile HrComputer15.txt /windowspath %SystemRoot% /localos
   ```

4. Stellen Sie sicher, dass der neue Computer mit dem Netzwerk verbunden ist, und starten Sie ihn neu. Beim Neustart wird der Computer nun zur Domäne hinzugefügt.

Sie können eine *Unattend.xml*-Datei für die Bereitstellung verwenden. Dazu legen Sie einen Abschnitt in der *Unattend.xml*-Datei an, in dessen *AccountData*-Element Sie den Inhalt der *.txt*-Datei mit den Metadaten einfügen. Hier ein Beispiel:

```
<Component name=Microsoft-Windows-UnattendedJoin>
   <Identification>
      <Provisioning>
         <AccountData> Hier Metadaten einfügen! </AccountData>
      </Provisioning>
   </Identification>
</Component>
```

Sobald Sie die *Unattend.xml*-Datei erstellt haben, starten Sie den neuen Computer im abgesicherten Modus oder unter Windows PE (Windows Preinstallation Environment) und führen Setup mit einer Antwortdatei aus, wie im folgenden Beispiel:

```
setup /unattend: <VollständigerPfadZurAntwortdatei>
```

Dabei ist <*VollständigerPfadZurAntwortdatei*> der vollständige Dateipfad zur *Unattend.xml*-Datei.

Verwalten von Domänencontrollern, Rollen und Katalogen

Domänencontroller führen zahlreiche wichtige Aufgaben in Active Directory-Domänen aus. Viele davon wurden bereits in Kapitel 7, »Arbeiten mit Active Directory«, behandelt.

Installieren und Herabstufen von Domänencontrollern

Sie installieren einen Domänencontroller, indem Sie auf einem Server die Active Directory-Domänendienste konfigurieren. Wenn Sie später möchten, dass der Server keine Controlleraufgaben übernimmt, können Sie ihn wieder herabstufen. Danach fungiert er wieder als Mitgliedserver. Auf ähnliche Weise erfolgt die Installation oder die Herabstufung von Servern, doch sollten Sie vorher die Auswirkungen auf das Netzwerk bedenken und den Abschnitt »Grundlagen der Verzeichnisstruktur« auf Seite 242 lesen.

Wie dort erläutert, müssen Sie Betriebsmasterrollen übertragen und die globale Katalogstruktur neu konfigurieren, wenn Sie einen Domänencontroller installieren. Außerdem muss vor der Installation von Active Directory DNS im Netzwerk funktionsfähig sein. Entsprechend sollten Sie vor dem Herabstufen eines Domänencontrollers alle zentralen Verantwortlichkeiten auf andere Domänencontroller verlagern. Dies umfasst gegebenenfalls die Verschiebung des globalen Katalogs vom Server und die Übertragung aller Betriebsmasterrollen. Außerdem müssen Sie alle Anwendungsverzeichnispartitionen entfernen, die sich auf dem Server befinden.

PRAXISTIPP Wichtig ist zu wissen, dass Sie in Windows Server 2003, Windows Server 2008 und Windows Server 2008 R2 einen Domänencontroller nicht mehr herabstufen müssen, um ihn umzubenennen. Sie können einen Domänencontroller jederzeit umbenennen. Das einzige Problem dabei ist, dass der Server während des Umbenennungsvorgangs den Benutzern nicht zur Verfügung steht und dass Sie gegebenenfalls eine Verzeichnisaktualisierung erzwingen müssen, um die ordnungsgemäße Kommunikation mit dem Server wiederherzustellen. Sie können einen Domänencontroller jedoch nicht einfach in eine andere Domäne verschieben. Sie müssen den Domänencontroller herabstufen, die Domäneneinstellungen für den Server und dessen Computerkonto aktualisieren und anschließend den Server heraufstufen, damit er wieder als Domänencontroller fungieren kann.

Um einen Domänencontroller zu installieren oder herabzustufen, gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, der neu konfiguriert werden soll. Wählen Sie im Server-Manager im linken Fensterabschnitt Knoten *Rollen* aus und klicken Sie auf *Rollen hinzufügen*. Daraufhin wird der *Assistent "Rollen hinzufügen"* gestartet. Falls der Assistent die Seite *Vorbemerkungen* anzeigt, sollten Sie den Text auf der Seite lesen. Klicken Sie anschließend auf *Weiter*.
2. Wählen Sie auf der Seite *Serverrollen auswählen* den Eintrag *Active Directory-Domänendienste* aus und klicken Sie zweimal auf *Weiter*. Klicken Sie auf *Installieren*.

3. Geben Sie im Suchfeld des Startmenüs den Befehl **dcpromo** ein und drücken Sie die EINGABETASTE. Daraufhin wird der *Assistent zum Installieren von Active Directory-Domänendiensten* gestartet.
4. Wenn der Computer gegenwärtig ein Mitgliedserver ist, führt Sie der Assistent durch die Installation des Active-Directory-Verzeichnisdienstes. Sie müssen angeben, ob es sich um einen Domänencontroller für eine neue Domäne oder um einen zusätzlichen Domänencontroller für eine vorhandene Domäne handelt. Sie sollten folgendermaßen vorgehen, um zu überprüfen, ob ein Domänencontroller richtig installiert ist: Suchen Sie im Verzeichnisdienst-Ereignisprotokoll nach Fehlern, stellen Sie sicher, dass Clients auf den *Sysvol*-Ordner zugreifen können, überprüfen Sie, dass die Namensauflösung mit DNS arbeitet, und prüfen Sie, ob die Replikation von Änderungen in Active Directory funktioniert.

Gehen Sie folgendermaßen vor, um einen Domänencontroller herabzustufen:

1. Melden Sie sich bei dem Server an, der neu konfiguriert werden soll. Geben Sie im Suchfeld des Startmenüs den Befehl **dcpromo** ein und drücken Sie die EINGABETASTE. Daraufhin wird der *Assistent zum Installieren von Active Directory-Domänendiensten* gestartet.
2. Falls der Computer gegenwärtig ein Domänencontroller ist, führt Sie der Assistent durch den Vorgang der Herabstufung des Domänencontrollers. Nach der Herabstufung arbeitet der Computer als Mitgliedserver.
3. Wählen Sie im Server-Manager im linken Fensterabschnitt Knoten *Rollen* aus und klicken Sie auf *Rollen entfernen*. Daraufhin wird der *Assistent "Rollen entfernen"* gestartet. Falls der Assistent die Seite *Vorbemerkungen* anzeigt, sollten Sie den Text auf der Seite lesen. Klicken Sie anschließend auf *Weiter*.
4. Deaktivieren Sie auf der Seite *Serverrollen entfernen* das Kontrollkästchen *Active Directory-Domänendienste* und klicken Sie zweimal auf *Weiter*. Klicken Sie auf *Fertig stellen*.

ACHTUNG Bei der Herabstufung des Servers mit Dcpromo werden seine Rollen auf andere Domänencontroller übertragen. Der Microsoft Knowledge Base-Artikel 332199 (*support.microsoft.com/kb/332199*) beschreibt, wie man eine Herabstufung mit **dcpromo /forceremoval** erzwingen kann. Allerdings bleiben die Betriebsmasterrollen des herabgestuften Servers bei Verwendung von **dcpromo /forceremoval** in einem ungültigen Zustand, bis sie vom Administrator neu zugewiesen werden. Wenn die erzwungene Herabstufung eines Domänencontrollers fehlschlägt oder wenn Sie nicht in der Lage sind, einen Server herabzustufen, bleiben die Domänendaten vielleicht in einem ungültigen Zustand. Angaben zur Lösung dieses Problems finden Sie im Microsoft Knowledge Base-Artikel 216498 (*support.microsoft.com/kb/216498/en-us*).

PRAXISTIPP Eine Alternative für die Installation von Domänencontrollern ist die Installation von einem Sicherungsmedium aus. Diese Option wurde in Windows Server 2003 eingeführt. Um einen Domänencontroller von Sicherungsmedien zu installieren, erstellen Sie eine Sicherung der Systemstatusdaten eines Domänencontrollers und stellen diese auf einem anderen Server wieder her, auf dem Windows Server 2003, Windows Server 2008 oder Windows Server 2008 R2 ausgeführt wird. Wenn Sie einen Domänencontroller von Sicherungsmedien erstellen, muss nicht die gesamte Verzeichnisdatenbank über das Netzwerk auf den neuen Domänencontroller repliziert werden. Dadurch können Sie sich sehr viel Mühe ersparen, wenn die Bandbreite begrenzt ist oder die Verzeichnisdatenbank Tausende von Einträgen hat.

Anzeigen und Übertragen domänenweiter Rollen

Mit *Active Directory-Benutzer und -Computer* können Sie die Orte domänenweiter Betriebsmasterrollen anzeigen und ändern. Auf der Domänenebene können Sie mit Rollen für RID-Master (Relative ID), PDC-Emulationsmaster (Primärer Domänencontroller) und Infrastrukturmaster arbeiten.

HINWEIS Betriebsmasterrollen werden im Abschnitt »Grundlagen von Betriebsmasterrollen« auf Seite 246 behandelt. Mit *Active Directory-Domänen und -Vertrauensstellungen* legen Sie die Domänennamen-Masterfunktion fest, mit *Active Directory-Schema* ändern Sie die Schemamasterrolle. Am schnellsten findet man den aktuellen Betriebsmaster für alle Rollen heraus, indem man in einer Eingabeaufforderung **netdom query fsmo** eingibt.

Zur Anzeige der aktuellen Betriebsmasterrollen gehen Sie wie folgt vor:

1. Klicken Sie in der Konsolenstruktur von *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf den Knoten *Active Directory-Benutzer und -Computer*. Wählen Sie im Kontextmenü *Alle Aufgaben* und anschließend *Betriebsmaster* aus. Das in Abbildung 8.7 dargestellte Dialogfeld *Betriebsmaster* wird geöffnet.

Abbildung 8.7 Mithilfe des Dialogfelds *Betriebsmaster* übertragen Sie Betriebsmasterrollen an andere Computer oder zeigen an, welcher Computer aktuell die betreffende Rolle hat

2. Das Dialogfeld *Betriebsmaster* hat drei Registerkarten. Die Registerkarte *RID* zeigt den aktuellen RID-Master an. Die Registerkarte *PDC* zeigt den aktuellen PDC-Emulationsmaster an. Und auf der Registerkarte *Infrastruktur* wird der aktuelle Infrastrukturmaster angezeigt.

Zur Übertragung der aktuellen Betriebsmasterrollen gehen Sie wie folgt vor:

1. Starten Sie *Active Directory-Benutzer und -Computer*. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Active Directory-Benutzer und -Computer* und wählen Sie *Domänencontroller ändern*.

2. Klicken Sie im Dialogfeld *Verzeichnisserver ändern* auf *Domänencontroller oder AD LDS-Instanz* und wählen Sie den Domänencontroller aus, auf den Sie eine Betriebsmasterrolle übertragen wollen. Klicken Sie auf *OK*.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Active Directory-Benutzer und -Computer* und wählen Sie im Kontextmenü den Befehl *Alle Aufgaben* und dann *Betriebsmaster*.
4. Wählen Sie im Dialogfeld *Betriebsmaster* eine der Registerkarten *RID*, *PDC* oder *Infrastruktur*, je nach der zu übertragenden Rolle.
5. Klicken Sie auf *Ändern*, um die Rolle an den zuvor ausgewählten Domänencontroller zu übertragen. Klicken Sie auf *OK*.

Anzeigen und Übertragen der Domänennamen-Masterrolle

Mit *Active Directory-Domänen und -Vertrauensstellungen* können Sie die Position des DNS-Masters in der Gesamtstruktur anzeigen und ändern. *Active Directory-Domänen und -Vertrauensstellungen* zeigt die Stammebene der Steuerungsstruktur für die ausgewählte Domäne an.

TIPP Wenn Sie eine Verbindung zu einer anderen Domäne herstellen müssen, gehen Sie genauso vor wie beim Herstellen einer Verbindung zu einem Domänencontroller, wie weiter oben im Abschnitt »Herstellen einer Verbindung zu einem Domänencontroller« auf Seite 257 beschrieben. Der einzige Unterschied besteht darin, dass Sie in der Konsolenstruktur mit der rechten Maustaste auf *Active Directory-Domänen und -Vertrauensstellungen* klicken.

Zum Übertragen der Domänennamen-Masterrolle gehen Sie wie folgt vor:

1. Starten Sie *Active Directory-Domänen und -Vertrauensstellungen*. Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf *Active Directory-Domänen und -Vertrauensstellungen* und wählen Sie anschließend *Domänencontroller ändern* aus.
2. Klicken Sie im Dialogfeld *Verzeichnisserver ändern* auf *Domänencontroller oder AD LDS-Instanz* und wählen Sie den Domänencontroller aus, auf den Sie die Rolle des Domänennamensmasters übertragen wollen. Klicken Sie auf *OK*.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Active Directory-Domänen und -Vertrauensstellungen*. Wählen Sie anschließend *Betriebsmaster* aus. Das Dialogfeld *Betriebsmaster* wird geöffnet.
4. Im Feld *Domänennamen-Betriebsmaster* wird der aktuelle Domänennamensmaster angezeigt. Klicken Sie auf *Ändern*, um diese Rolle an den zuvor gewählten Domänencontroller zu übertragen.
5. Klicken Sie auf *Schließen*.

Anzeigen und Übertragen der Schemamasterrolle

Mithilfe von *Active Directory-Schema* können Sie die Position des Schemamasters anzeigen oder ändern. Geben Sie an einer Eingabeaufforderung **regsvr32 schmmgmt.dll** ein, um Active Directory-Schema zu registrieren. Zum Übertragen der Schemamasterrolle gehen Sie wie folgt vor:

1. Fügen Sie das Snap-In *Active Directory-Schema* zu einer MMC hinzu.
2. Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf *Active Directory-Schema*. Wählen Sie danach *Active Directory-Domänencontroller ändern* aus.
3. Klicken Sie im Dialogfeld *Verzeichnisserver ändern* auf *Beliebiger schreibbarer Domänencontroller*, um den neuen Schemamaster von Active Directory auswählen zu lassen. Oder Sie wählen *Domänencon-*

troller oder AD LDS-Instanz und geben Sie den Namen des neuen Schemamasters ein, zum Beispiel *zeta.seattle.cpandl.com*.

4. Klicken Sie auf *OK*. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Active Directory-Schema* und wählen Sie den Befehl *Betriebsmaster*.
5. Klicken Sie im Dialogfeld *Schemamaster ändern* auf *Ändern*. Klicken Sie auf *OK* und dann auf *Schließen*.

Übertragen von Rollen mithilfe der Befehlszeile

Eine weitere Möglichkeit zum Übertragen von Rollen besteht darin, sich mit Netdom einen Überblick über die aktuellen Betriebsmaster zu verschaffen und die Rollen dann mit *Ntdsutil.exe* zu übertragen. Ntdsutil ist ein Befehlszeilenprogramm für die Verwaltung von Active Directory. Gehen Sie wie folgt vor, um Rollen über die Befehlszeile zu übertragen:

1. Erstellen Sie sich eine Liste der aktuellen Betriebsmaster, indem Sie in einer Eingabeaufforderung **netdom query fsmo** eingeben.
2. Es wird empfohlen, sich an der Konsole des Servers anzumelden, den Sie als neuen Betriebsmaster zuweisen möchten (das ist allerdings nicht unbedingt nötig). Sie können sich lokal an der Konsole anmelden oder eine Remotedesktopverbindung verwenden.
3. Geben Sie im Suchfeld des Startmenüs den Befehl **cmd** ein und drücken Sie die EINGABETASTE.
4. Geben Sie an der Eingabeaufforderung **ntdsutil** ein. Das Dienstprogramm für die Verzeichnisdienstverwaltung wird gestartet.
5. Geben Sie an der Ntdsutil-Eingabeaufforderung **roles** ein. Das Dienstprogramm wechselt in den Modus zur Betriebsmasterwartung.
6. Geben Sie an der »Fsmo maintenance«-Eingabeaufforderung **connections** ein und an der »server connections«-Eingabeaufforderung **connect to server**, gefolgt vom vollqualifizierten Domänennamen des Domänencontrollers, der die betreffende Betriebsmasterrolle übernehmen soll. Beispiel:

   ```
   connect to server engdc01.technology.adatum.com
   ```

7. Geben Sie nach einem erfolgreichen Verbindungsaufbau **quit** ein, um die Eingabeaufforderung für Serververbindungen zu beenden. Geben Sie an der »Fsmo maintenance«-Eingabeaufforderung **transfer** und anschließend die Kennung der zu übertragenden Rolle ein. Die Kennungen heißen wie folgt:
   - **pdc** Für die PDC-Emulationsrolle
   - **rid master** Für die RID-Masterrolle
   - **infrastructure master** Für die Infrastrukturmasterrolle
   - **schema master** Für die Schemamasterrolle
   - **domain naming master** Für die Domänennamensmasterrolle
8. Geben Sie erst an der »Fsmo maintenance«-Eingabeaufforderung und anschließend an der »Ntdsutil«-Eingabeaufforderung jeweils **quit** ein.

Übernehmen von Rollen mithilfe der Befehlszeile

Gelegentlich kommt es vor, dass Sie Serverfunktionen nicht fehlerlos übertragen können. Beispielsweise kann auf einem als RID-Master fungierenden Server ein Laufwerk ausfallen, wodurch der gesamte Server ausfällt. Wenn Sie den Server nicht wieder online bringen können, müssen Sie gegebenenfalls die RID-Masterrolle übernehmen und einem anderen Domänencontroller zuweisen.

HINWEIS Übernehmen Sie eine Serverfunktion nur dann, wenn der für die aktuelle Rolle zuständige Domänencontroller außer Betrieb geht. Sobald der ursprüngliche Servermaster wieder online gebracht wird, erkennt er die Änderung und richtet sich danach.

Übernehmen Sie eine Rolle nur, wenn Sie vorher festgestellt haben, dass der Domänencontroller, der die Rolle übernehmen soll, auf demselben Stand ist wie der vorherige Besitzer der Rolle. Active Directory verfolgt Replikationsänderungen über USNs (Update Sequence Number). Weil die Replikation einige Zeit dauert, sind nicht unbedingt alle Domänencontroller auf dem neuesten Stand. Wenn Sie die USN eines Domänencontrollers mit der eines anderen Servers in der Domäne vergleichen, können Sie feststellen, ob der Domänencontroller auf demselben Stand ist wie der vorherige Besitzer der Rolle. Falls der Domänencontroller auf dem aktuellen Stand ist, können Sie die Rolle problemlos übertragen. Falls der Domänencontroller nicht auf dem neuesten Stand ist, können Sie warten, bis die Replikation durchgeführt wurde, und die Rolle dann auf den Domänencontroller übertragen.

Windows Server 2008 R2 stellt für die Arbeit mit der Active Directory-Replikation das Dienstprogramm Repadmin zur Verfügung. Sie können die höchste Sequenznummer für einen angegebenen Namenskontext auf allen Replikationspartnern eines Domänencontrollers anzeigen, indem Sie den folgenden Befehl an einer Eingabeaufforderung ausführen:

```
repadmin /showutdvec Domänencontrollername Namenskontext
```

Dabei sind *Domänencontrollername* der vollqualifizierte Domänenname des Domänencontrollers und *Namenskontext* der definierte Name der Domäne, in der dieser Server liegt. Ein Beispiel:

```
repadmin /showutdvec server252.cpandl.com dc=cpandl,dc=com
```

Die Ausgabe zeigt die höchste USN auf den Replikationspartner für die Domänenpartition:

```
Default-First-Site-Name\SERVER252 @ USN   45164 @ Zeit 30.03.2008 14:25:36
Default-First-Site-Name\SERVER147 @ USN   45414 @ Zeit 30.03.2008 14:25:36
```

Falls *Server252* der vorherige Besitzer der Rolle war und der Domänencontroller, den Sie untersuchen, dieselbe oder eine größere USN als *Server252* hat, ist der Domänencontroller auf dem neuesten Stand. Falls allerdings *Server252* der vorherige Besitzer der Rolle ist und der Domänencontroller, den Sie untersuchen, eine kleinere USN als *Server252* hat, ist der Domänencontroller nicht auf dem neuesten Stand. Dann sollten Sie warten, bis die Replikation durchgeführt wurde, bevor Sie die Rolle übernehmen. Mit dem Befehl *repadmin /syncall* können Sie auch den Domänencontroller, der die aktuelle Version vom vorherigen Besitzer der Rolle bezogen hat, dazu zwingen, die Replikation mit allen seinen allen Replikationspartnern auszuführen.

Gehen Sie folgendermaßen vor, um eine Serverrolle zu übernehmen:

1. Beschaffen Sie sich eine Liste der aktuellen Betriebsmaster, indem Sie in einer Eingabeaufforderung **netdom query fsmo** eingeben.
2. Vergewissern Sie sich, dass der aktuelle Domänencontroller mit der Rolle, die Sie übernehmen möchten, dauerhaft offline ist. Falls der Server wieder online gebracht werden kann, führen Sie diesen Vorgang nicht durch, es sei denn, Sie möchten den Server vollständig neu installieren.

3. Es wird empfohlen, sich auf der Konsole des Servers anzumelden, den Sie als neuen Betriebsmaster zuweisen möchten. Sie können sich lokal an der Konsole anmelden oder eine Remotedesktopverbindung verwenden.
4. Öffnen Sie eine Eingabeaufforderung.
5. Geben Sie in der Eingabeaufforderung **ntdsutil** ein. Das Dienstprogramm für die Verzeichnisdienstverwaltung wird gestartet.
6. Geben Sie an der Ntdsutil-Eingabeaufforderung **roles** ein. Das Dienstprogramm wechselt in den Modus zur Betriebsmasterwartung.
7. Geben Sie an der »Fsmo maintenance«-Eingabeaufforderung **connections** und an der »server connections«-Eingabeaufforderung **connect to server** sowie den vollqualifizierten Namen des Domänencontrollers ein, der die betreffende Betriebsmasterrolle übernehmen soll. Beispiel:

   ```
   connect to server engdc01.technology.adatum.com
   ```

8. Nach dem erfolgreichen Aufbau einer Verbindung geben Sie **quit** ein, um die Eingabeaufforderung für Serververbindungen zu verlassen. Geben Sie an der »Fsmo maintenance«-Eingabeaufforderung **seize** und anschließend die Kennung der zu übertragenden Rolle ein. Die Kennungen heißen wie folgt:
   - **pdc** Für die PDC-Emulationsrolle
   - **rid master** Für die RID-Masterrolle
   - **infrastructure master** Für die Infrastrukturmasterrolle
   - **schema master** Für die Schemamasterrolle
   - **domain naming master** Für die Domänennamensmasterrolle
9. Geben Sie erst an der »Fsmo maintenance«-Eingabeaufforderung und anschließend an der »Ntdsutil«-Eingabeaufforderung jeweils **quit** ein.

Konfigurieren globaler Kataloge

Globale Kataloge spielen im Netzwerk eine wichtige Rolle. Diese Rolle wird im Abschnitt »Grundlagen der Verzeichnisstruktur« auf Seite 242 erörtert. Zusätzliche globale Kataloge lassen sich konfigurieren, indem Sie Domänencontroller als Host für den globalen Katalog aktivieren. Sie können einen Domänencontroller auch als Host des globalen Katalogs deaktivieren, wenn an einem Standort zwei oder mehr globale Kataloge existieren. Dazu deaktivieren Sie den globalen Katalog auf dem Domänencontroller.

Zum Aktivieren beziehungsweise Deaktivieren eines globalen Katalogs gehen Sie wie folgt vor:

1. Erweitern Sie in der Konsolenstruktur von *Active Directory-Standorte und -Dienste* den Standort, mit dem Sie arbeiten wollen.
2. Erweitern Sie den Ordner *Servers* des Standorts und klicken Sie danach auf den Server, der als Host für den globalen Katalog fungieren soll.
3. Klicken Sie in der Detailansicht mit der rechten Maustaste auf *NTDS Settings* und wählen Sie den Befehl *Eigenschaften*.
4. Um den Server in die Lage zu versetzen, den globalen Katalog aufzunehmen, aktivieren Sie das Kontrollkästchen *Globaler Katalog* auf der Registerkarte *Allgemein*.
5. Um den globalen Katalog zu deaktivieren, deaktivieren Sie *Globaler Katalog* auf der Registerkarte *Allgemein*.

ACHTUNG Aktivieren oder deaktivieren Sie keine globalen Kataloge ohne sorgfältige vorherige Planung und Analyse der Folgen für das Netzwerk. In großen Unternehmensnetzwerken kann die Zuweisung eines globalen Katalogs an einen Domänencontroller dazu führen, dass die Daten von Tausenden von Active Directory-Objekten über das Netzwerk repliziert werden.

Konfigurieren der Zwischenspeicherung der universellen Gruppenmitgliedschaft

Durch das Zwischenspeichern der universellen Gruppenmitgliedschaft besteht bei Anmeldungen keine Abhängigkeit mehr von der Verfügbarkeit eines globalen Katalogservers. Wenn diese Rolle in einer Domäne der Funktionsebene »Windows Server 2003« oder höher aktiviert ist, kann jeder Domänencontroller Anmeldeanforderungen lokal auflösen, ohne dass der globale Katalogserver abgefragt werden muss. Wie im Abschnitt »Zwischenspeichern der universellen Gruppenmitgliedschaft« auf Seite 244 erläutert, hat dies Vor- und Nachteile.

Sie können die Zwischenspeicherung der universellen Gruppenmitgliedschaft wie folgt aktivieren oder deaktivieren:

1. Erweitern Sie in *Active Directory-Standorte und -Dienste* den Standort, mit dem Sie arbeiten wollen, und wählen Sie ihn dann aus.
2. Klicken Sie in der Detailansicht mit der rechten Maustaste auf *NTDS Site Settings* und wählen Sie den Befehl *Eigenschaften*.
3. Zur Aktivierung der Zwischenspeicherung der universellen Gruppenmitgliedschaft wählen Sie auf der Registerkarte *Standorteinstellungen* das Kontrollkästchen *Zwischenspeichern der universellen Gruppenmitgliedschaft aktivieren*. Anschließend wählen Sie mithilfe der Liste *Cache aktualisieren von* einen Standort aus, von dem die universellen Gruppenmitgliedschaften zwischengespeichert werden sollen. Der ausgewählte Standort muss über einen funktionierenden Server verfügen, auf dem der globale Katalog gespeichert ist.
4. Um die Zwischenspeicherung der universellen Gruppenmitgliedschaft zu deaktivieren, müssen Sie das Kontrollkästchen *Zwischenspeichern der universellen Gruppenmitgliedschaft aktivieren* auf der Registerkarte *Standorteinstellungen* deaktivieren.
5. Klicken Sie auf *OK*.

Verwalten von Organisationseinheiten

Wie in Kapitel 7 erläutert, helfen Ihnen Organisationseinheiten unter anderem beim Strukturieren von Objekten und beim Festlegen einer Gruppenrichtlinie mit begrenztem Geltungsbereich. In diesem Abschnitt erfahren Sie, wie Organisationseinheiten erstellt und verwaltet werden.

Erstellen von Organisationseinheiten

Organisationseinheiten erstellen Sie für gewöhnlich, um die geschäftliche oder funktionale Struktur Ihrer Organisation abzubilden. Sie können Organisationseinheiten als Untergruppen einer Domäne oder als untergeordnete Einheiten innerhalb einer vorhandenen Organisationseinheit erstellen.

Zum Erstellen einer Organisationseinheit gehen Sie so vor:

1. Klicken Sie in *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf den Domänenknoten oder den Ordner einer vorhandenen Organisationseinheit, zu dem die Organisationseinheit hinzugefügt werden soll. Wählen Sie im Kontextmenü *Neu* aus und klicken Sie auf *Organisationseinheit*.
2. Geben Sie den Namen der Organisationseinheit ein. Klicken Sie auf *OK*.
3. Nun können Sie Konten und freigegebene Ressourcen in die Organisationseinheit verschieben. Ein Beispiel hierzu finden Sie im Abschnitt »Verschieben von Computerkonten« auf Seite 262.

Anzeigen und Bearbeiten der Eigenschaften einer Organisationseinheit

Zum Anzeigen und Bearbeiten der Eigenschaften einer Organisationseinheit gehen Sie wie folgt vor:

1. Öffnen Sie *Active Directory-Benutzer und -Computer*.
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Organisationseinheit und wählen Sie anschließend *Eigenschaften* aus. Es wird ein Eigenschaftendialogfeld angezeigt, in dem Sie die Einstellungen anzeigen und bearbeiten können.

Umbenennen und Löschen von Organisationseinheiten

Zum Umbenennen und Löschen einer Organisationseinheit gehen Sie wie folgt vor:

1. Klicken Sie in *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf den Ordner der betreffenden Organisationseinheit.
2. Um die Organisationseinheit zu löschen, wählen Sie *Löschen* aus. Bestätigen Sie anschließend den Vorgang, indem Sie auf *Ja* klicken.
3. Um die Organisationseinheit umzubenennen, wählen Sie *Umbenennen* aus. Geben Sie einen neuen Namen für die Organisationseinheit ein und drücken Sie die EINGABETASTE.

Verschieben von Organisationseinheiten

Sie können Organisationseinheiten an eine andere Position innerhalb einer Domäne verschieben, indem Sie die Organisationseinheit in *Active Directory-Benutzer und -Computer* auswählen und an die neue Position ziehen.

Die folgenden Schritte beschreiben eine andere Methode zum Verschieben von Organisationseinheiten:

1. Klicken Sie in *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf den Ordner der Organisationseinheit, die Sie verschieben möchten. Wählen Sie anschließend die Option *Verschieben* aus.
2. Klicken Sie im Dialogfeld *Verschieben* auf den Domänenknoten und anschließend auf den Container, in den die Organisationseinheit verschoben werden soll. Klicken Sie auf *OK*.

Verwalten von Standorten

Der Assistent zum Installieren von Active Directory erstellt einen Standardstandort und eine Standardstandortverknüpfung, wenn Sie Active Directory-Domänendienste auf dem ersten Domänencontroller in einem Standort installieren. Der Standardstandort trägt den Namen *Default-First-Site-Name*, und die Standardstandortverknüpfung heißt *DEFAULTIPSITELINK*. Sie können den Standardstandort und die Standardstandortverknüpfung bei Bedarf umbenennen. Alle weiteren Standorte und Standortverknüpfungen müssen Sie von Hand anlegen.

Das Konfigurieren eines Standorts ist ein mehrstufiger Vorgang, der folgende Schritte umfasst:

1. Erstellen des Standorts.
2. Erstellen eines oder mehrerer Subnetze und Zuordnen dieser Subnetze zum Standort.
3. Zuordnen eines Domänencontrollers zum Standort.
4. Verknüpfen des Standorts mit anderen Standorten mithilfe von Standortverknüpfungen. Außerdem (bei Bedarf) Erstellen von Standortverknüpfungsbrücken.

Die folgenden Abschnitte beschreiben diese Aufgaben.

Erstellen von Standorten

Jeder Administrator, der Mitglied der Gruppen *Domänen-Admins* oder *Organisations-Admins* ist, kann Standorte erstellen. Gehen Sie folgendermaßen vor, um einen neuen Standort zu erstellen:

1. Klicken Sie im Konsolenstamm von *Active Directory-Standorte und -Dienste* mit der rechten Maustaste auf den Container *Sites* und wählen Sie den Befehl *Neuer Standort*.
2. Geben Sie im Dialogfeld *Neues Objekt – Standort* (Abbildung 8.8) einen Namen für den Standort ein, zum Beispiel »ChicagoSite«. Standortnamen dürfen keine Leerzeichen oder Sonderzeichen außer einem Bindestrich enthalten.

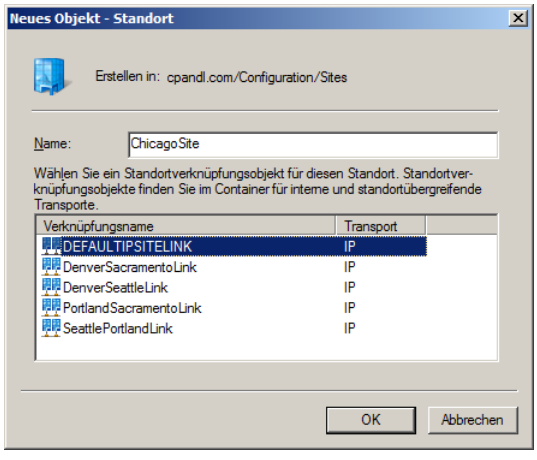

Abbildung 8.8 Erstellen eines Standorts durch Eingeben von Standortname und der zugehörigen Standortverknüpfung

3. Klicken Sie auf die Standortverknüpfung, die Sie benutzen wollen, um diesen Standort mit anderen Standorten zu verknüpfen. Falls es die Standortverknüpfung, die Sie verwenden wollen, noch nicht

gibt, können Sie die Standardstandortverknüpfung nehmen und die Einstellungen für die Standortverknüpfung später ändern.

4. Klicken Sie auf *OK*. Es wird ein Dialogfeld angezeigt, in dem beschrieben ist, welche Schritte Sie durchführen müssen, um die Standortkonfiguration abzuschließen. Klicken Sie erneut auf *OK*.
5. Um die Standortkonfiguration abzuschließen, müssen Sie die übrigen Konfigurationsaufgaben vollständig durchführen.

TIPP Sie können einen Standort jederzeit umbenennen. Klicken Sie in *Active Directory-Standorte und -Dienste* mit der rechten Maustaste auf den Standort und wählen Sie den Befehl *Umbenennen*. Geben Sie den gewünschten Namen für den Standort ein und drücken Sie die EINGABETASTE.

Erstellen von Subnetzen

Jeder Standort, den Sie definieren, muss ein zugeordnetes Subnetz haben, das festlegt, welche Netzwerksegmente zum Standort gehören. Jeder Computer mit einer IP-Adresse in einem Netzwerksegment, das einem Standort zugeordnet ist, »liegt« in diesem Standort. Ein einzelner Standort kann zwar mehrere Subnetze zugeordnet haben, aber ein Subnetz kann immer nur einem einzigen Standort zugeordnet sein.

Gehen Sie folgendermaßen vor, um ein Subnetz zu erstellen und es einem Standort zuzuordnen:

1. Klicken Sie in der Konsolenstruktur von *Active Directory-Standorte und -Dienste* mit der rechten Maustaste auf den Container *Subnets* und wählen Sie den Befehl *Neues Subnetz*. Daraufhin öffnet sich das Dialogfeld *Neues Objekt – Subnetz* (Abbildung 8.9).

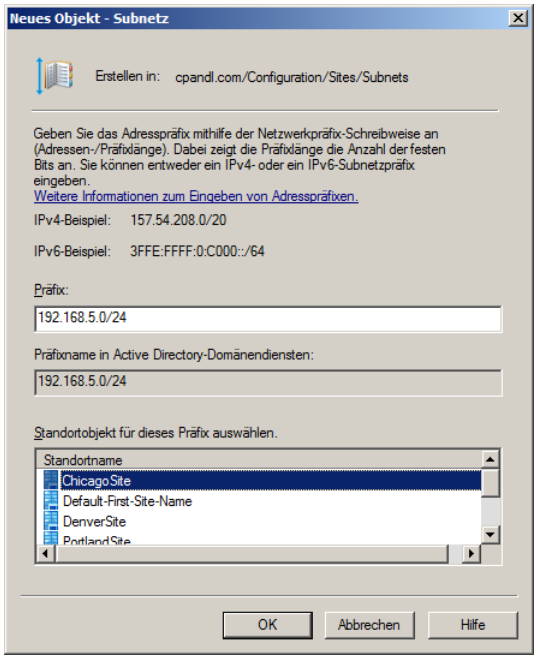

Abbildung 8.9 Zum Erstellen eines Subnetzes geben Sie das Netzwerkpräfix ein und wählen den zugeordneten Standort aus

2. Geben Sie im Feld *Präfix* das IPv4- oder IPv6-Netzwerkadressenpräfix ein. Verwenden Sie dabei die Netzwerkpräfixnotation, die sich aus einer Netzwerk-ID, einem Schrägstrich und den für die Netzwerk-ID verwendeten Bits zusammensetzt. Falls zum Beispiel die Netzwerk-ID 192.168.5.0 lautet und die ersten 24 Bits die Netzwerk-ID bilden, geben Sie »192.168.5.0/24« als Netzwerkpräfixnotation ein.
3. Wählen Sie den Standort aus, dem das Subnetz zugeordnet werden soll, und klicken Sie auf *OK*.

TIPP Sie können die Standortzuordnung für ein Subnetz jederzeit ändern. Klicken Sie dazu in *Active Directory-Standorte und -Dienste* doppelt auf das Subnetz im Ordner *Subnets* und ändern Sie dann auf der Registerkarte *Allgemein* die Standortzuordnung in der Liste *Standortobjekt für dieses Präfix auswählen*.

Verknüpfen von Domänencontrollern mit Standorten

Jeder Standort sollte mindestens einen Domänencontroller zugeordnet haben. Indem Sie einen zweiten Domänencontroller zu einem Standort hinzufügen, sorgen Sie für Fehlertoleranz und Redundanz. Falls mindestens ein Domänencontroller im Standort auch ein globaler Katalogserver ist, können Sie sicherstellen, dass Verzeichnissuchoperationen und Authentifizierungsverkehr auf den Standort begrenzt bleiben.

Sie können Domänencontroller automatisch oder von Hand zu Standorten hinzufügen. Wenn Sie Subnetze mit einem Standort verknüpfen, werden alle neu installierten Domänencontroller automatisch zum Standort hinzugefügt, falls die IP-Adresse des Domänencontrollers innerhalb des gültigen Bereichs der IP-Adressen für das Subnetz liegt. Vorhandene Domänencontroller werden aber nicht automatisch mit Standorten verknüpft. Sie müssen alle vorhandenen Domänencontroller von Hand mit einem neuen Standort verknüpfen, indem Sie das Domänencontrollerobjekt in den Standort verschieben.

Bevor Sie einen Domänencontroller von einem Standort in einen anderen verschieben können, müssen Sie feststellen, in welchem Standort der Domänencontroller momentan liegt. Das können Sie sehr schnell herausfinden, indem Sie den folgenden Befehl an einer Eingabeaufforderung eingeben:

```
dsquery server -s Domänencontrollername | dsget server -site
```

Dabei ist *Domänencontrollername* der vollqualifizierte Domänenname des Domänencontrollers, zum Beispiel:

```
dsquery server -s server241.cpandl.com | dsget server -site
```

Die Ausgabe dieses Befehls ist der Name des Standorts, in dem der angegebene Domänencontroller liegt.

Gehen Sie folgendermaßen vor, um einen Domänencontroller von einem Standort in einen anderen zu verschieben:

1. In *Active Directory-Standorte und -Dienste* sind alle Domänencontroller, die einem Standort zugeordnet sind, im *Servers*-Knoten dieses Standorts aufgelistet. Wählen Sie den Standort aus, dem der Domänencontroller momentan zugeordnet ist.
2. Klicken Sie mit der rechten Maustaste auf den Domänencontroller und wählen Sie den Befehl *Verschieben*. Klicken Sie im Dialogfeld *Server verschieben* auf den Standort, in den Sie den Server verlegen wollen, und klicken Sie auf *OK*.

HINWEIS Verschieben Sie einen Domänencontroller nicht in einen Standort, falls er sich nicht in einem Subnetz befindet, das diesem Standort zugeordnet ist. Falls Sie die Subnetz- und Standortzuordnungen ändern, müssen Sie Domänencontroller aus den betreffenden Subnetzen in die Container der betreffenden Standorte verschieben.

Konfigurieren von Standortverknüpfungen

Standorte sind Gruppen von IP-Subnetzen, die über zuverlässige Hochgeschwindigkeitsverbindungen miteinander kommunizieren. Üblicherweise sind alle Subnetze im selben lokalen Netzwerk Teil desselben Standorts. Netzwerke mit mehreren Standorten sind über Standortverknüpfungen (engl. site link) verbunden. Standortverknüpfungen sind logische, transitive Verbindungen zwischen zwei oder mehr Standorten. Jede Standortverknüpfung hat einen Replikationszeitplan, ein Replikationsintervall, Verbindungskosten und einen Replikationstransport.

Weil Standortverknüpfungen über WAN-Verbindungen (Wide Area Network) laufen, sind Bandbreitenverfügbarkeit und -verbrauch wichtige Faktoren, wenn Sie Standortverknüpfungen konfigurieren. In der Standardeinstellung sind Standortverknüpfungen so konfiguriert, dass sie Daten 24 Stunden am Tag, 7 Tage die Woche mit einem Intervall von mindestens 180 Minuten replizieren. Falls Sie wissen, dass eine Verbindung nur über eingeschränkte Bandbreite verfügt, sollten Sie den Zeitplan ändern, damit Benutzerverkehr während der Phasen stärkster Nutzung Priorität bekommt.

Wenn Sie mehrere Verknüpfungen zwischen Standorten haben, müssen Sie die relative Priorität jeder Verknüpfung planen. Sie weisen die Priorität anhand von Verfügbarkeit und Zuverlässigkeit der Verknüpfung zu. Der Standardwert für Verknüpfungskosten beträgt 100. Falls es mehrere mögliche Routen zu einem Standort gibt, wird die Route mit den geringsten Standortverknüpfungskosten zuerst benutzt. Daher sollten die zuverlässigsten Pfade mit der meisten Bandbreite zwischen Standorten üblicherweise so konfiguriert werden, dass sie die geringsten Standortverknüpfungskosten haben.

Sie können Standortverknüpfungen so konfigurieren, dass sie entweder RPC über IP oder SMTP (Simple Mail Transfer Protocol) als Transportprotokoll einsetzen. Wird IP als Transport verwendet, stellen Domänencontroller jeweils genau eine RPC-über-IP-Verbindung mit einem einzelnen Replikationspartner her und replizieren Active Directory-Änderungen synchron. Weil RPC über IP synchron arbeitet, müssen beide Replikationspartner verfügbar sein, wenn die Verbindung aufgebaut wird. Sie sollten RPC über IP verwenden, wenn Sie eine zuverlässige, dedizierte Verbindung zwischen den Standorten haben.

Wird SMTP als Transportmechanismus verwendet, konvertieren Domänencontroller den gesamten Replikationsverkehr in E-Mail-Nachrichten, die asynchron zwischen den Standorten ausgetauscht werden. Weil SMTP-Replikation asynchron arbeitet, brauchen nicht beide Replikationspartner verfügbar zu sein, wenn die Verbindung aufgebaut wird. Die Replikationstransaktionen können gespeichert werden, bis ein Zielserver verfügbar wird. Sie sollten SMTP verwenden, wenn die Verbindungen unzuverlässig oder nur zeitweise verfügbar sind.

HINWEIS Falls Sie SMTP verwenden wollen, müssen Sie eine Zertifizierungsstelle einrichten. Zertifikate dieser Zertifizierungsstelle werden gebraucht, um die SMTP-Nachrichten, die zwischen den Standorten ausgetauscht werden, digital zu signieren und zu verschlüsseln. Beim Transportmechanismus IP sind in der Standardeinstellung keine Zertifizierungsstellen erforderlich.

Gehen Sie folgendermaßen vor, um eine Standortverknüpfung zwischen zwei oder mehr Standorten einzurichten:

1. Erweitern Sie in *Active Directory-Standorte und -Dienste* den Container *Sites* und dann den Container *Inter-Site Transports*.
2. Klicken Sie mit der rechten Maustaste auf den Container für das Transportprotokoll, das Sie verwenden wollen (entweder *IP* oder *SMTP*), und wählen Sie den Befehl *Neue Standortverknüpfung*.

3. Geben Sie im Dialogfeld *Neues Objekt – Standortverknüpfung* (Abbildung 8.10) einen Namen für die Standortverknüpfung ein, zum Beispiel »ChicagoToSeattleLink«. Die Namen von Standortverknüpfungen dürfen keine Leerzeichen oder Sonderzeichen außer einem Bindestrich enthalten.

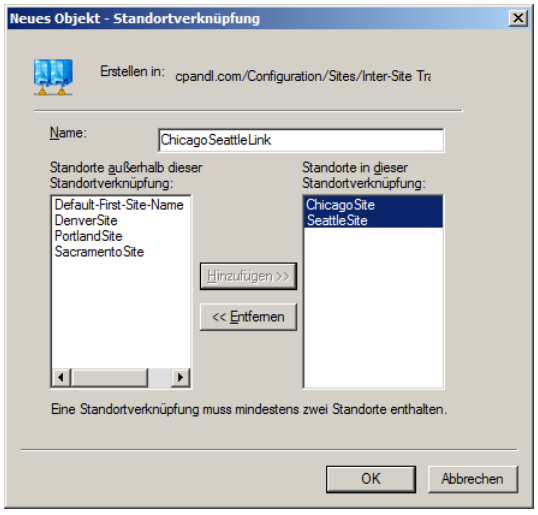

Abbildung 8.10 Sie erstellen die Standortverknüpfung, indem Sie einen Namen für die Verknüpfung eingeben und die zugehörigen Standorte auswählen

4. Klicken Sie in der Liste *Standorte außerhalb dieser Standortverknüpfung* auf den ersten Standort, der in der Verknüpfung enthalten sein soll, und klicken Sie auf *Hinzufügen*, um diesen Standort in die Liste *Standorte in dieser Standortverknüpfung* zu kopieren. Wiederholen Sie diesen Vorgang für jeden Standort, den Sie zur Verknüpfung hinzufügen wollen. Sie müssen mindestens zwei Standorte hinzufügen. Klicken Sie auf *OK*.

Wenn Sie die Standortverknüpfung erstellt haben, sollten Sie die Eigenschaften der Verknüpfung konfigurieren. Auf diese Weise können Sie die Verknüpfungskosten, den Replikationszeitplan und das Replikationsintervall festlegen. Gehen Sie folgendermaßen vor, um die Eigenschaften einer Standortverknüpfung zu konfigurieren:

1. Klicken Sie in der Detailansicht von *Active Directory-Standorte und -Dienste* mit der rechten Maustaste auf die Standortverknüpfung und wählen Sie den Befehl *Eigenschaften*.
2. Im Eigenschaftendialogfeld ist als Standardeinstellung die Registerkarte *Allgemein* ausgewählt. Tragen Sie im Feld *Kosten* die relativen Kosten der Verknüpfung ein. Der Standardwert ist 100.
3. Geben Sie im Feld *Replizieren alle* das Replikationsintervall ein. Das Standardintervall beträgt 180 Minuten.
4. Der Standardreplikationszeitplan deckt 24 Stunden pro Tag und 7 Tage pro Woche ab. Sie können einen anderen Zeitplan einstellen, indem Sie auf *Zeitplan ändern* klicken und dann den gewünschten Replikationszeitplan im Dialogfeld *Zeitplan für* einstellen. Klicken Sie auf *OK*.

Gehen Sie folgendermaßen vor, um zu ändern, welche Standorte mit einer Standortverknüpfung verbunden sind:

1. Klicken Sie in der Detailansicht von *Active Directory-Standorte und -Dienste* mit der rechten Maustaste auf die Standortverknüpfung und wählen Sie den Befehl *Eigenschaften*.

2. Im Eigenschaftendialogfeld ist als Standardeinstellung die Registerkarte *Allgemein* ausgewählt. Klicken Sie in der Liste *Standorte außerhalb dieser Standortverknüpfung* auf den ersten Standort, der zu dieser Verknüpfung hinzugefügt werden soll, und dann auf *Hinzufügen*, um den Standort in die Liste *Standorte in dieser Standortverknüpfung* zu übernehmen. Wiederholen Sie diesen Vorgang für alle Standorte, die Sie zur Verknüpfung hinzufügen wollen.
3. Klicken Sie in der Liste *Standorte in dieser Standortverknüpfung* auf den ersten Standort, der nicht mehr in dieser Verknüpfung enthalten sein soll, und dann auf *Entfernen*, um den Standort in die Liste *Standorte außerhalb dieser Standortverknüpfung* zu verschieben. Wiederholen Sie diesen Vorgang für alle Standorte, die Sie aus der Verknüpfung entfernen wollen. Klicken Sie auf *OK*.

Konfigurieren von Standortverknüpfungsbrücken

Alle Standortverknüpfungen sind standardmäßig transitiv. Das bedeutet, wenn mehr als zwei Standorte für Replikationszwecke verknüpft sind und denselben Transportmechanismus verwenden, werden Standortverknüpfungen automatisch durch Brücken verbunden, sodass Verknüpfungen zwischen Standorten transitiv sein können. Aufgrund dieser Transitivität kann ein beliebiges Paar aus zwei Domänencontrollern eine Verknüpfung über beliebige aufeinanderfolgende Verknüpfungsabschnitte herstellen. Zum Beispiel kann ein Domänencontroller in Standort *A* eine Verbindung zu einem Domänencontroller in Standort *C* herstellen, die über Standort *B* geleitet wird.

Welche Verknüpfungspfade Domänencontroller für Verbindungen zwischen Standorten wählen, wird in erster Linie durch die Kosten der Standortverknüpfungsbrücken bestimmt. Die Standortverknüpfungsbrückenkosten sind die Summe aller Verknüpfungen, die in der Brücke enthalten sind. Im Allgemeinen wird der Pfad mit den geringsten Gesamtkosten für die Standortverknüpfungsbrücke benutzt.

Wenn Sie die Kosten von Verknüpfungen und Verknüpfungsbrücken kennen, können Sie die Auswirkungen von Netzwerkverbindungsausfällen abschätzen und festlegen, welche Pfade benutzt werden sollen, wenn eine Verbindung ausfällt. Nehmen wir zum Beispiel an, ein Domänencontroller in Standort *A* ist mit einem Domänencontroller in Standort *C* normalerweise über Standort *B* verbunden. Falls nun die Verbindung zu Standort *B* ausfällt, wählen die beiden Domänencontroller automatisch einen Alternativpfad, sofern einer zur Verfügung steht, zum Beispiel über Standort *D* und Standort *E*.

Die Topologie für die Replikation zwischen unterschiedlichen Standorten ist standardmäßig so optimiert, dass maximal drei Abschnitte (engl. hop) verwendet werden. In großen Standortkonfigurationen kann das unerwartete Auswirkungen haben, wenn zum Beispiel derselbe Replikationsverkehr mehrmals über dieselbe Verbindung läuft. In diesem Fall sollten Sie die automatische Standortverknüpfungsüberbrückung deaktivieren und Standortverknüpfungsbrücken von Hand konfigurieren. Von solchen Fällen abgesehen ist es nur selten sinnvoll, die automatische Standortverknüpfungsüberbrückung zu deaktivieren.

Innerhalb einer Active Directory-Gesamtstruktur können Sie die Standortverknüpfungstransitivität für jedes Transportprotokoll individuell aktivieren oder deaktivieren. Das bedeutet, dass alle Standortverknüpfungen, die mit einem bestimmten Transportmechanismus arbeiten, entweder Standortverknüpfungstransitivität nutzen oder nicht. Sie können die Transitivität für ein Transportprotokoll folgendermaßen konfigurieren:

1. Erweitern Sie in *Active Directory-Standorte und -Dienste* den Container *Sites* und dann den Container *Inter-Site Transports*.
2. Klicken Sie mit der rechten Maustaste auf den Container für das Transportprotokoll, das Sie bearbeiten wollen (entweder *IP* oder *SMTP*), und wählen Sie den Befehl *Eigenschaften*.
3. Sie können die Standortverknüpfungstransitivität aktivieren, indem Sie das Kontrollkästchen *Brücke zwischen allen Standortverknüpfungen herstellen* aktivieren und auf *OK* klicken. Wenn die Standort-

verknüpfungstransitivität aktiviert ist, werden alle Standortverknüpfungsbrücken, die Sie für das jeweilige Transportprotokoll erstellt haben, ignoriert.

4. Sie können die Standortverknüpfungstransitivität deaktivieren, indem Sie das Kontrollkästchen *Brücke zwischen allen Standortverknüpfungen herstellen* deaktivieren und auf *OK* klicken. Wenn die Standortverknüpfungstransitivität deaktiviert ist, müssen Sie Standortverknüpfungsbrücken für das jeweilige Protokoll konfigurieren.

Sobald Sie transitive Verknüpfungen deaktiviert haben, können Sie von Hand eine Standortverknüpfungsbrücke zwischen zwei oder mehr Standorten erstellen. Gehen Sie dazu folgendermaßen vor:

1. Erweitern Sie in *Active Directory-Standorte und -Dienste* den Container *Sites* und dann den Container *Inter-Site Transports*.
2. Klicken Sie mit der rechten Maustaste auf den Container für das Transportprotokoll, das Sie bearbeiten wollen (entweder *IP* oder *SMTP*), und wählen Sie den Befehl *Neue Standortverknüpfungsbrücke*.
3. Geben Sie im Dialogfeld *Neues Objekt – Standortverknüpfungsbrücke* einen Namen für die Standortverknüpfungsbrücke ein. Namen von Brücken dürfen keine Leerzeichen oder Sonderzeichen außer dem Bindestrich enthalten.
4. Wählen Sie in der Liste *Standortverknüpfungen außerhalb dieser Standortverknüpfungsbrücke* eine Standortverknüpfung aus, die Sie in die Brücke aufnehmen wollen, und klicken Sie auf *Hinzufügen*, um die Standortverknüpfung in die Liste *Standortverknüpfungen in dieser Standortverknüpfungsbrücke* zu verschieben. Wiederholen Sie diesen Vorgang für jede Standortverknüpfung, die Sie zur Brücke hinzufügen wollen. Eine Brücke muss mindestens zwei Standortverknüpfungen enthalten. Klicken Sie auf *OK*.

Sie können die Standortverknüpfungen, die zu einer Standortverknüpfungsbrücke gehören, jederzeit ändern. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie in *Active Directory-Standorte und -Dienste* den Container für das Transportprotokoll aus, das Sie bearbeiten wollen. Klicken Sie in der Detailansicht mit der rechten Maustaste auf die Standortverknüpfungsbrücke und wählen Sie den Befehl *Eigenschaften*.
2. Im Eigenschaftendialogfeld ist als Standardeinstellung die Registerkarte *Allgemein* ausgewählt. Wählen Sie in der Liste *Standortverknüpfungen außerhalb dieser Standortverknüpfungsbrücke* die erste Standortverknüpfung aus, die in die Brücke aufgenommen werden soll, und klicken Sie auf *Hinzufügen*, um die Standortverknüpfung in die Liste *Standortverknüpfungen in dieser Standortverknüpfungsbrücke* zu verschieben. Wiederholen Sie diesen Vorgang für jede Standortverknüpfung, die Sie zur Brücke hinzufügen wollen.
3. Wählen Sie in der Liste *Standortverknüpfungen in dieser Standortverknüpfungsbrücke* die erste Standortverknüpfung aus, die nicht mehr in der Brücke enthalten sein soll, und klicken Sie auf *Entfernen*, um die Standortverknüpfung in die Liste *Standortverknüpfungen außerhalb dieser Standortverknüpfungsbrücke* zu verschieben. Wiederholen Sie diesen Vorgang für jede Standortverknüpfung, die Sie aus der Brücke entfernen wollen. Klicken Sie auf *OK*.

Pflegen von Active Directory

Um sicherzustellen, dass Active Directory einwandfrei arbeitet, müssen Sie regelmäßige Überwachungs- und Wartungsaufgaben durchführen. Bei Ihren Überwachungs- und Wartungsaufgaben werden Sie feststellen, dass einige Tools unverzichtbar sind. In diesem Abschnitt stelle ich diese Tools vor und beschreibe einige allgemeine Wartungsaufgaben.

Arbeiten mit *ADSI-Editor*

Wenn Sie Probleme untersuchen und eine Fehlerbehebung durchführen, ist der ADSI-Editor ein nützliches Active Directory-Administrationstool. Sie können im ADSI-Editor die Definitionen von Objektklassen sowie ihre Attribute im Schema verwalten und mit anderen Namenskontexten arbeiten, zum Beispiel dem Standardnamenskontext, dem Konfigurationsnamenskontext und dem RootDSE-Namenskontext. Wenn Sie benutzerdefinierte Attribute für Benutzer oder Gruppen erstellen wollen, sollten Sie den ADSI-Editor verwenden, den Sie über einen Eintrag im Untermenü *Verwaltung* starten können.

Gehen Sie folgendermaßen vor, um im Snap-In *ADSI-Editor* eine Verbindung zum gewünschten Namenskontext herzustellen:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *ADSI-Editor* und wählen Sie den Befehl *Verbindung herstellen*. Daraufhin öffnet sich das Dialogfeld *Verbindungseinstellungen* (Abbildung 8.11).

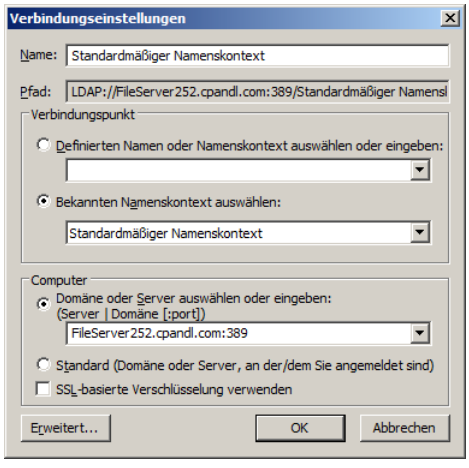

Abbildung 8.11 Herstellen der Verbindung zu einem Namenskontext im ADSI-Editor

2. Im Dialogfeld *Verbindungseinstellungen* ist als Standardeinstellung die Option *Bekannten Namenskontext auswählen* aktiviert. Wählen Sie in der zugehörigen Dropdownliste den Namenskontext aus, mit dem Sie arbeiten wollen.
3. Wenn Sie auf *OK* klicken, werden Sie mit einem beliebigen verfügbaren Domänencontroller in Ihrer Anmeldedomäne verbunden. Sie können die Verbindung zu einer anderen Domäne oder einem anderen Server herstellen, indem Sie die Option *Domäne oder Server auswählen oder eingeben* wählen und in der zugehörigen Dropdownliste den Server oder die Domäne auswählen, mit der Sie arbeiten

wollen. Dabei können Sie auch eine optionale Portnummer für die Verbindung wählen, zum Beispiel *FileServer252.cpandl.com:389*. Port 389 ist der Standardport für LDAP.

Sobald Sie Namenskontext, Domäne und Server ausgewählt haben, werden Sie mit dem Namenskontext verbunden, sodass Sie damit arbeiten können. Wie Abbildung 8.12 zeigt, stehen unterschiedliche Knoten zum Verwalten der Kontexte zur Verfügung, wenn Sie Verbindungen mit mehreren Namenskontexten herstellen. Bei der Problembehandlung können Sie auch von unterschiedlichen Servern derselben Domäne aus eine Verbindung zum selben Namenskontext herstellen. Indem Sie die Werte der Eigenschaften auf einem Server mit denen auf einem anderen Server vergleichen, können Sie ein Replikationsproblem erkennen.

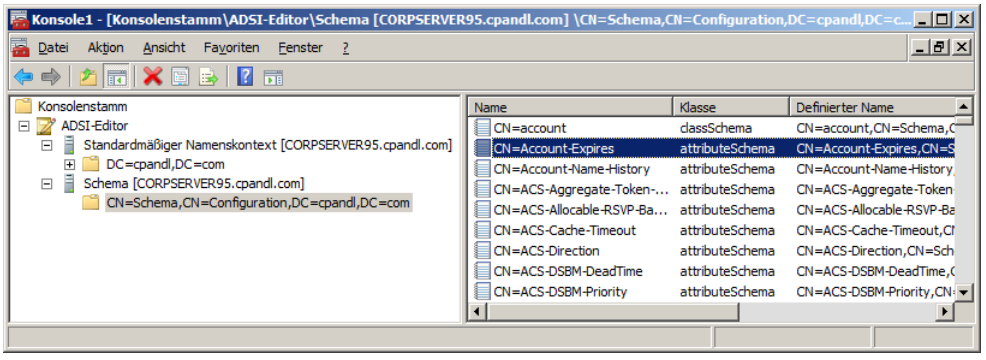

Abbildung 8.12 In den Namenskontexten können Sie die zugehörigen Container und Eigenschaften untersuchen

Untersuchen der standortübergreifenden Topologie

Der ISTG (Inter-Site Topology Generator) in einem Standort hat die Aufgabe, die standortübergreifende Replikationstopologie zu generieren. Wenn der ISTG die Replikationstopologie berechnet, kann er beachtliche Rechenlast verursachen, vor allem wenn das Netzwerk größer wird. Deswegen sollten Sie die ISTGs in jedem Standort genau beobachten und sicherstellen, dass sie nicht überlastet werden.

Gehen Sie folgendermaßen vor, um festzustellen, welcher Domänencontroller der ISTG ist:

1. Erweitern Sie in der Konsolenstruktur von *Active Directory-Standorte und -Dienste* den Container *Sites* und dann den Standortcontainer für den gesuchten ISTG.
2. Klicken Sie in der Detailansicht doppelt auf *NTDS Site Settings*. Im Dialogfeld *Eigenschaften von NTDS Site Settings* ist der aktuelle ISTG im Feld *Standortübergreifende Topologie erstellen* aufgeführt.

Die Replikation zwischen Standorten wird mithilfe von Bridgeheadservern ausgeführt. Ein Bridgeheadserver ist ein Domänencontroller, der vom ISTG dazu bestimmt wird, die standortübergreifende Replikation durchzuführen. Wenn zwei Standorte über eine Standortverknüpfung verbunden sind, wählt der ISTG in jedem Standort einen Bridgeheadserver aus und erstellt Objekte für ausschließlich eingehende Verbindungen zwischen den Servern, die für die standortübergreifende Replikation zuständig sind.

Der ISTG konfiguriert für jede Active Directory-Partition, die repliziert werden muss, einen Bridgeheadserver. Und er verwaltet eine eigene Replikationstopologie für jeden Partitionstyp. Ein einzelner Bridgeheadserver kann zwar die Replikation mehrerer Verzeichnispartitionen übernehmen, aber die Replikationstopologien für die unterschiedlichen Partitionen werden getrennt voneinander verwaltet.

Domänencontroller, die als Bridgeheadserver agieren, werden zusätzlich belastet, und diese Last steigt mit der Zahl und Häufigkeit von Replikationsänderungen. Wie beim ISTG sollten Sie die Bridgeheadserver sorgfältig überwachen und sicherstellen, dass sie nicht überlastet werden. Sie können die Bridgehead-

server in einem Standort auflisten, indem Sie an einer Eingabeaufforderung den folgenden Befehl eingeben:

```
repadmin /bridgeheads site:Standortname
```

Dabei ist *Standortname* der Name des Standorts, zum Beispiel:

```
repadmin /bridgeheads site:SacramentoSite
```

Falls die aktuellen Bridgeheadserver überlastet sind oder Sie Domänencontroller haben, die Sie lieber als Bridgeheadserver einsetzen wollen, können Sie bevorzugte Bridgeheadserver bestimmen. Wenn Sie einen bevorzugten Bridgeheadserver für einen Standort bestimmten, verwendet der ISTG nur den bevorzugten Bridgeheadserver für die standortübergreifende Replikation. Falls der bevorzugte Bridgeheadserver offline geht oder aus irgendwelchen Gründen nicht für die Replikation zur Verfügung steht, wird die standortübergreifende Replikation abgebrochen, bis der Server wieder verfügbar ist oder Sie die Konfiguration für den bevorzugten Bridgeheadserver ändern.

Wenn Sie bevorzugte Bridgeheadserver bestimmten, sollten Sie immer mehrere bevorzugte Bridgeheadserver für jeden Standort konfigurieren. Der ISTG wählt dann einen der Server aus, die Sie als bevorzugte Bridgeheadserver bestimmt haben. Falls dieser Server ausfällt, schaltet der ISTG auf einen Server aus der Liste der bevorzugten Bridgeheadserver um.

Sie müssen für jede Partition, die repliziert werden muss, einen Bridgeheadserver konfigurieren. Das bedeutet, dass Sie mindestens einen Domänencontroller mit einer Kopie jeder Verzeichnispartition als Bridgeheadserver konfigurieren müssen. Falls Sie das versäumen, schlägt die Replikation der Partition fehl, und der ISTG trägt ein Ereignis in das Verzeichnisdienste-Ereignisprotokoll ein, in dem der Fehler beschrieben wird.

Gehen Sie folgendermaßen vor, um einen Domänencontroller als bevorzugten Bridgeheadserver zu konfigurieren:

1. In *Active Directory-Standorte und -Dienste* werden die Domänencontroller, die einem Standort zugeordnet sind, im *Servers*-Knoten des Standorts aufgelistet. Klicken Sie mit der rechten Maustaste auf den Server, den Sie als bevorzugten Bridgeheadserver bestimmen wollen, und wählen Sie den Befehl *Eigenschaften*.
2. Wählen Sie im Eigenschaftendialogfeld in der Liste *Transporte für die standortübergreifende Datenübermittlung* das Transportprotokoll, für das der Server ein bevorzugter Bridgeheadserver werden soll, und klicken Sie auf *Hinzufügen*. Wiederholen Sie diesen Schritt bei Bedarf, um sowohl IP als auch SMTP auszuwählen. Klicken Sie auf *OK*.

Wenn Sie bevorzugte Bridgeheadserver bestimmt haben, haben Sie unterschiedliche Möglichkeiten, Replikationsfehler zu beheben. Sie können die ausgefallenen Server als bevorzugte Bridgeheadserver entfernen und andere bevorzugte Bridgeheadserver bestimmen. Oder Sie entfernen alle Server als bevorzugte Bridgeheadserver und erlauben dem ISTG, automatisch auszuwählen, welcher Bridgeheadserver verwendet werden soll. Gehen Sie folgendermaßen vor, um einen Server von seiner Rolle als bevorzugter Bridgeheadserver für ein bestimmtes Transportprotokoll zu entbinden:

1. In *Active Directory-Standorte und -Dienste* werden die Domänencontroller, die einem Standort zugeordnet sind, im *Servers*-Knoten des Standorts aufgelistet. Klicken Sie mit der rechten Maustaste auf den Server, den Sie als bevorzugten Bridgeheadserver löschen wollen, und wählen Sie den Befehl *Eigenschaften*.
2. Wählen Sie im Eigenschaftendialogfeld in der Liste *Server ist ein bevorzugter Bridgeheadserver für folgende Transporte* den Server aus und klicken Sie auf *Entfernen*. Klicken Sie auf *OK*.

Durchführen einer Problembehandlung für Active Directory

Im Rahmen der Routinewartung müssen Sie Domänencontroller, globale Katalogserver, Bridgeheadserver und Standortverknüpfungen überwachen. Falls Sie Probleme mit Active Directory vermuten, sollten Sie Ihre Diagnose und Problembehandlung in den meisten Fällen bei der Replikation beginnen. Indem Sie die Überwachung der standortinternen und standortübergreifenden Replikation von Active Directory konfigurieren, können Sie die meisten Replikationsprobleme diagnostizieren und beseitigen. Vergessen Sie aber nicht, dass die Active Directory-Replikation von mehreren Diensten abhängt, darunter folgende: LDAP, DNS (Domain Name System), Kerberos-Version-5-Authentifizierung und Remoteprozeduraufruf (Remote Procedure Call, RPC).

Diese wichtigen Dienste müssen einwandfrei arbeiten, damit Verzeichnisaktualisierungen repliziert werden können. Während der Replikation benutzt Active Directory verschiedene TCP- und UDP-Ports, die auf dem Domänencontroller offen sein müssen. In der Standardeinstellung werden folgende Ports benutzt:

- LDAP benutzt TCP und UDP über Port 389 für Standardverkehr und TCP über Port 686 für sicheren Verkehr.
- Globale Kataloge benutzen TCP über Port 3268. Kerberos Version 5 benutzt TCP und UDP über Port 88.
- DNS benutzt TCP und UDP über Port 53.
- SMB über IP benutzt TCP und UDP über Port 445.

Für die Replikation von Dateien in den freigegebenen Ordnern des Systemvolumes (*Sysvol*) auf Domänencontrollern benutzt Active Directory außerdem entweder den Dateireplikationsdienst oder den DFS-Replikationsdienst. Der entsprechende Replikationsdienst muss laufen und richtig konfiguriert sein, damit *Sysvol* repliziert werden kann.

Active Directory verfolgt Änderungen mithilfe von USNs (Update Sequence Number). Jedes Mal, wenn eine Änderung am Verzeichnis vorgenommen wird, weist der Domänencontroller, der die Änderung verarbeitet, dieser Änderung eine USN zu. Jeder Domänencontroller verwaltet seine eigenen lokalen USNs und erhöht den Wert jedes Mal, wenn eine Änderung auftritt. Der Domänencontroller weist die lokale USN auch dem Objektattribut zu, das geändert wurde. Jedes Objekt hat ein zugehöriges Attribut mit Namen *uSNChanged*, das zusammen mit dem Objekt gespeichert wird. Es gibt die höchste USN an, die irgendeinem der Attribute des Objekts zugewiesen wurde.

Jeder Domänencontroller verfolgt seine lokale USN und die lokalen USNs der anderen Domänencontroller. Bei der Replikation vergleichen die Domänencontroller die empfangenen USN-Werte mit den Werten, die sie selbst gespeichert haben. Falls der aktuelle USN-Wert für einen bestimmten Domänencontroller höher ist als der gespeicherte Wert, müssen Änderungen von diesem Domänencontroller repliziert werden. Falls der aktuelle Wert für einen bestimmten Domänencontroller derselbe ist wie der gespeicherte Wert, brauchen keine Änderungen aus diesem Domänencontroller repliziert zu werden.

Sie können die Replikation von der Befehlszeile aus überwachen. Dazu können Sie das Programm Repadmin verwenden. Bei den meisten Befehlszeilenargumenten von Repadmin können Sie eine Liste der Domänencontroller übergeben, mit denen Sie arbeiten wollen. Diese Liste wird als DCList bezeichnet. Sie können die Werte für DCList folgendermaßen angeben:

- * Ein Platzhalterzeichen, das für alle Domänencontroller in der Organisation steht.
- ***Namensteil**** Dabei ist *Namensteil* ein teilweise angegebener Servername, gefolgt vom Platzhalterzeichen *, das für den Rest des Servernamens steht.

- ***Site:Standortname*** Dabei ist *Standortname* der Name des Standorts, dessen Domänencontroller Sie untersuchen wollen.
- ***Gc:*** Umfasst alle globalen Katalogserver in der Organisation.

Repadmin hat viele Parameter mit etlichen unterschiedlichen Bedeutungen. Aber es gibt bestimmte Aufgaben, die Sie besonders häufig ausführen werden. Tabelle 8.2 zeigt einige dieser Aufgaben.

Tabelle 8.2 Wichtige Replikationsaufgaben und -befehle

Aufgabe	Befehl
Zwingt den KCC (Knowledge Consistency Checker), die standortinterne Replikationstopologie für einen angegebenen Domänencontroller neu zu berechnen.	*repadmin /kcc DCList [/async]*
Listet die Bridgeheadserver auf, die der DClist entsprechen.	*repadmin /bridgeheads DCList [/verbose]*
Listet alle Aufrufe vom angegebenen Server an andere Server auf, die noch nicht beantwortet wurden.	*repadmin /showoutcalls DCList*
Listet die Domänen auf, denen die angegebene Domäne vertraut.	*repadmin /showtrust DCList*
Listet fehlgeschlagene Replikationsereignisse auf, die vom KCC (Knowledge Consistency Checker) erkannt wurden.	*repadmin /failcache DCList*
Listet die Verbindungsobjekte für die angegebenen Domänencontroller auf. In der Standardeinstellung wird der lokale Standort verwendet.	*repadmin /showconn DCList*
Listet die Computer auf, die Sitzungen mit dem angegebenen Domänencontroller geöffnet haben.	*repadmin /showctx DCList*
Listet den Namen des ISTGs für den angegebenen Standort auf.	*repadmin istg DCList [/verbose]*
Listet die Replikationspartner für jede Verzeichnispartition auf dem angegebenen Domänencontroller auf.	*repadmin /showrepl DCList*
Gibt eine Zusammenfassung des Replikationsstatus aus.	*repadmin /replsummary DCList*
Listet die Serverzertifikate auf, die in die angegebenen Domänencontroller geladen sind.	*repadmin /showcert DCList*
Listet die Aufgaben auf, die in der Replikationswarteschlange auf ihre Bearbeitung warten.	*repadmin /queue DCList*
Gibt die Zeit zwischen standortübergreifenden Replikationen aus, wobei der ISTG-Keep-Alive-Zeitstempel ausgewertet wird.	*repadmin /latency DCList [/verbose]*