PEARSON Education


# Exchange Server 2007 und Outlook

Messaging, Mails und mehr – für Profis

THOMAS JOOS

Markt+Technik

KOMPENDIUM

Einführung | Arbeitsbuch | Nachschlagewerk

CD

Tools und Bonusbuch „Microsoft Netzwerke" als PDF

# 3 Serverrollen, Verzeichnisse und Dienste

In diesem Kapitel gehe ich ausführlicher auf die einzelnen Serverrollen von Exchange Server 2007 ein. Ich zeige Ihnen in diesem Kapitel auch die Systemdienste und Verzeichnisse, die ein Exchange-Server benötigt. Administratoren, die eine Exchange-Infrastruktur verwalten, sollten nicht nur über die grafische Oberfläche oder die Exchange-Verwaltungsshell Bescheid wissen, sondern auch die Hintergründe verstehen, da bei Problemen mit dem Server oft hier die Lösung liegt.

Die Serverrollen und die Standorte im Active Directory interagieren miteinander. Exchange-Administratoren, die Exchange-Server über mehrere Standorte verteilt einsetzen, sollten sich daher auch mit der Thematik der Active Directory-Standorte auseinandersetzen. Auch diesem Bereich habe ich in diesem Kapitel einen eigenen Abschnitt gewidmet.

## 3.1 Allgemeine Informationen zu Serverrollen

Die verschiedenen Serverrollen in Exchange Server 2007 sind eine der maßgeblichsten Änderungen. Durch diese neuen Möglichkeiten können Unternehmen einzelne Exchange-Server speziell nach deren gewünschter Funktion einsetzen. Nicht benötigte Funktionen werden nicht mit installiert. Dadurch steigt die Sicherheit, und die Belastung der Hardware durch unnötige Dienste wird verringert.

Bevor Sie sich an die Planung und Umsetzung eines Exchange-Projektes machen, sollten Sie sich daher mit dem Rollenmodell in Exchange Server 2007 vertraut machen. Vor allem beim Einsatz mehrerer Exchange-Server auch in verschiedenen physikalischen Niederlassungen ist das Verständnis für die Serverrollen wichtig für die Planung, Installation, Verwaltung und Optimierung.

Insgesamt können Sie bei der Installation von Exchange Server 2007 einem Server eine oder mehrere der fünf Rollen zuweisen. Im nächsten Abschnitt gehe ich näher auf die einzelnen Rollen und deren Funktionen ein:

- Edge-Transport – Diese Exchange-Server sind für das Routing vom und ins Internet in der DMZ, auch für das Viren- und Spam-Scannen verantwortlich. Dieser Server muss kein Bestandteil einer Domäne sein. Diese Rolle wird standardmäßig nicht mit installiert, sondern muss explizit getrennt installiert werden, da diese nicht zusammen mit den anderen Rollen auf einem Server betrieben werden kann. Diese Art von Server ist der erste Berührungspunkt von E-Mails aus dem Internet und der letzte vom internen Netzwerk ins Internet (siehe Kapitel 5 und 15).
- Hub-Transport – Diese Server nehmen die Aufgaben der bisherigen Bridgehead-Server zwischen verschiedenen Routinggruppen ein. In Exchange Server 2007 gibt es keine Routinggruppen mehr, da Exchange jetzt die Active Directory-

Standorte unterstützt. Außerdem ist dieser Servertyp für das Durchsetzen der verschiedenen Richtlinien zuständig. Diese Rolle kann auch auf einem einzelnen Exchange-Server zusammen mit der Mailbox-, Client-Access- und Unified Messaging-Rolle installiert werden. In jedem Active Directory-Standort in der Gesamtstruktur, in der auch Exchange-Server positioniert werden, muss mindestens ein Server die Rolle eines Hub- Transport-Servers einnehmen. Alle E-Mails eines Active Directory-Standorts laufen immer durch einen Hub-Transport-Server. Die Kommunikation zwischen Hub-Transport-Servern der verschiedenen Active Directory-Standorte findet zertifikatsbasierend und verschlüsselt statt. Exchange Server 2007 stellt dazu bereits eingebaute Zertifikate zur Verfügung, sodass Administratoren nicht zwingend eine eigene Zertifikats-Infrastruktur (Certificate Authority, CA) aufbauen und verwalten müssen. Admins, die sich mit diesem Thema auskennen, können aber auch selbsterstellte Zertifikate verwenden (siehe Kapitel 5).

- Mailbox – Diese Server entsprechen der bisherigen Rolle eines Back-End-Servers, dienen also nur dem Speichern von Postfächern und öffentlichen Ordnern. Diese Rolle kann auch auf einem einzelnen Exchange-Server zusammen mit der Hub-Transport-, Client-Access- und Unified Messaging-Rolle installiert werden. Diese Rolle ist als einzige clusterfähig (siehe Kapitel 14), alle anderen Rollen müssen durch Loadbalancing oder anderen Absicherungsmethoden vor Ausfall geschützt werden (siehe Kapitel 6).
- Client-Access – Diese Server entsprechen den bisherigen Front-End-Servern mit dem Unterschied, dass auch interne Outlook-Clients über Client-Access-Server Verbindung zu Mailbox-Servern aufbauen können. Auch der Zugriff von Smartphones (Exchange ActiveSync), Outlook Anywhere (RPC über HTTP) oder Outlook Web Access erfolgt über diese Art von Servern. Diese Rolle kann auch auf einem einzelnen Exchange-Server zusammen mit der Hub-Transport-, Mailbox- und Unified Messaging-Rolle installiert werden (siehe Kapitel 9).
- Unified Messaging – Diese Server dienen dem Empfangen (Senden geht nicht) von Faxen und der Anbindung direkt an Telefonanlagen für Voice Mail und Outlook Voice Access. Diese Rolle kann auch auf einem einzelnen Exchange-Server zusammen mit der Hub-Transport-, Client-Access- und Mailbox-Rolle installiert werden. Für die Konfiguration dieser Rolle ist etwas Wissen für die Konfiguration und Steuerung von Telefonanlagen notwendig (siehe Kapitel 10).

Unternehmen, die nur einen Exchange-Server einsetzen, installieren diesen natürlich mit allen Serverrollen, die auf einem einzelnen Exchange-Server installiert werden können, also Client-Access, Mailbox, Hub-Transport und bei Bedarf auch Unified Messaging.


*Ist ein Edge-Transport-Server in der DMZ geplant, muss diese Rolle zwingend auf einer eigenständigen Maschine installiert werden, eine Kombination mit den anderen vier Rollen ist nicht möglich.*

**Anzeigen der verschiedenen Serverrollen in der Exchange-Verwaltungskonsole**

Klicken Sie in der Exchange-Verwaltungskonsole auf den Menüpunkt *Serverkonfiguration*, werden Ihnen im Ergebnis-Bereich alle Exchange-Server der Organisation mit den verschiedenen Rollen angezeigt *(siehe Abbildung 3.1)*.

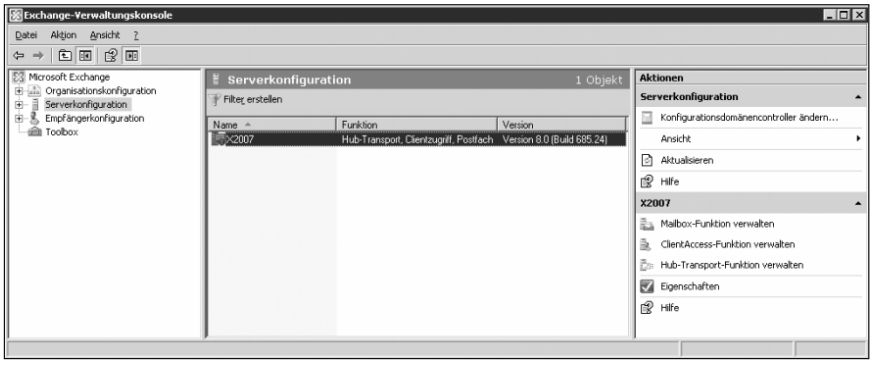



**Abbildung 3.1:** Anzeigen der Serverrollen in der Exchange-Verwaltungskonsole



Unterhalb des Menüpunktes *Serverkonfiguration* finden Sie die vier Serverrollen, die in einem internen Netzwerk installiert werden können. Klicken Sie auf einen dieser Menüpunkte, werden Ihnen die Server angezeigt, auf denen die entsprechende Rolle installiert ist.

**Serverrollen während der Migration zu Exchange Server 2007**

Migrieren Sie zu Exchange Server 2007 und setzen Sie dedizierte Server für die verschiedenen Rollen ein, sollten Sie die Migration in folgender Reihenfolge vornehmen:

1. Client-Access-Server (unter Exchange 2000/2003 Front-End-Server)
2. Hub-Transport-Server
3. Mailbox-Server (untere Exchange 2000/2003 Back-End-Server)
4. Unified Messaging-Server

Bei der Installation eines Edge-Transport-Servers während der Migration müssen Sie keine besondere Reihenfolge beachten, Sie können diese Server vor, während oder nach der Migration zu Exchange Server 2007 installieren.


*Migrieren Sie Exchange Server 2003-Front-End-Server zu Exchange Server 2007-Client-Access-Servern, können Anwender, deren Postfächer noch auf Exchange Server 2003-Back-End-Servern liegen, wie gewohnt auf deren Postfächer mit Outlook Web Access zugreifen.*

### 3.1.1 Edge-Transport-Server und ADAM (Active Directory Application Mode)

ADAM ist eine Low End-Variante von Active Directory. Es basiert auf der gleichen Technologie und unterstützt ebenfalls Replikation. Im Gegensatz zum Active Directory wird aber beispielsweise kein Kerberos für die Authentifizierung unterstützt. Mit ADAM können LDAP-Verzeichnisse für Anwendungen erstellt werden, die wiederum mit dem Active Directory synchronisiert werden können und dieses auch für die Authentifizierung nutzen können. Es können mehrere ADAM-Instanzen parallel auf einem Server betrieben werden.

ADAM ist eine Alternative zu den *Application Directory Partitions* im Active Directory. ADAM wurde für Organisationen, die eine flexible Unterstützung verzeichnis-

fähiger Anwendungen benötigen, entwickelt. ADAM ist ein LDAP-Verzeichnisdienst (Lightweight Directory Access-Protokoll), der als Benutzerdienst und nicht als Systemdienst ausgeführt wird. Mit den ADAM-Services können Unternehmen zum Beispiel andere LDAP-Verzeichnisse in Testumgebungen oder der DMZ installieren, ohne auf Software eines Drittanbieters zurückgreifen zu müssen.

Sie können ADAM im Internet auf der Seite `http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4` herunterladen. Alternativ können Sie auch nach ADAM auf der Microsoft Homepage suchen.

Setzen Sie Windows Server 2003 R2 ein, ist ADAM bereits im Lieferumfang des Servers enthalten. Sie können ADAM über *Systemsteuerung/Software/Windows-Komponenten hinzufügen/Active Directory-Dienste/Details/ Active Directory-Anwendungsmodus* installieren. Die Verwaltung von ADAM findet über die Programmgruppe *Start/Programme/ADAM* statt.

## 3.2 Active Directory–Standorte und Exchange Server 2007

Exchange Server 2007 kennt keine administrativen Gruppen und Routinggruppen mehr, sondern verwendet die Active Directory-Standorte der Gesamtstruktur. Aus diesem Grund gehört die Planung von Active Directory und Exchange zukünftig enger zusammengelegt als noch bei den Vorgänger-Versionen von Exchange Server 2007. Durch die Integration von Exchange Server 2007 in die Active Directory-Standorte verringert sich die Verwaltung von Exchange 2007-Servern. Exchange-Administratoren müssen daher zukünftig auch im Bereich der Active Directory-Replikation und -Standorte entsprechendes Wissen mitbringen. Im folgenden Abschnitt gehe ich auf die Erstellung und Verwaltung von Active Directory-Standorten ein. Die Fehlerbehebung zu diesem Bereich zeige ich Ihnen im Kapitel 16.

Das Active Directory bietet die Möglichkeit, eine Gesamtstruktur in mehrere Standorte zu unterteilen, die durch verschiedene IP-Subnetze voneinander getrennt sind (siehe *Abbildung 3.2*).

Durch diese physische Trennung der Standorte ist es nicht mehr notwendig, für jede Niederlassung eine eigene Domäne zu erstellen. An jedem Standort müssen zwar weiterhin Domänencontroller installiert werden, allerdings kann die Domäne von einem zentralen Standort aus verwaltet werden, von dem die Änderungen auf die einzelnen Standorte repliziert werden können.

### 3.2.1 Konfiguration der Routingtopologie im Active Directory

Die Replikation zwischen verschiedenen Standorten im Active Directory läuft weitgehend automatisiert ab. Damit die Replikation aber stattfinden kann, müssen Sie zunächst die notwendige Routingtopologie erstellen. Installieren Sie später Exchange, werden automatisch Connectoren, basierend auf den verschiedenen Standorten, erstellt.

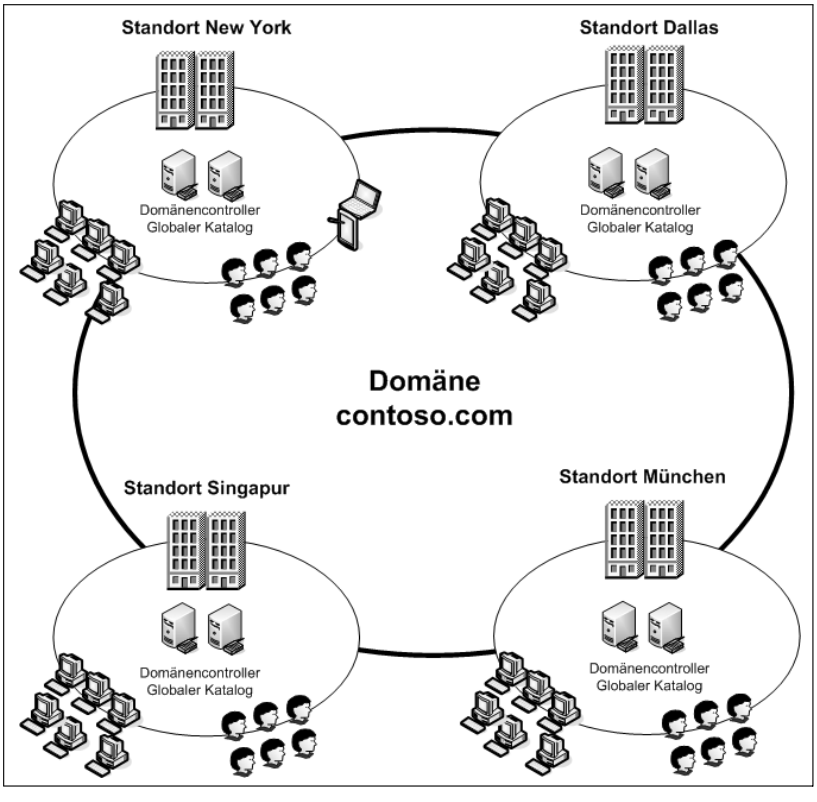



**Abbildung 3.2:** Standorte im Active Directory



Bei der Erstellung der Routingtopologie fallen hauptsächlich folgende Aufgaben an, die auf den nächsten Seiten ausführlicher behandelt werden:

- Erstellen von *Standorten* in der Active Directory-Standortverwaltung.
- Erstellen von IP-Subnetzen und zuweisen an die Standorte.
- Erstellen von *Standortverknüpfungen* für die Replikation des Active Directorys.
- Konfiguration von Zeitplänen und Kosten für die optimale Standort-Replikation.

Damit Sie die standortübergreifende Replikation von Active Directory verwenden können, müssen Sie in jedem Standort, an dem später ein Domänencontroller angeschlossen wird, ein unabhängiges IP-Subnetz verwenden. Dieses IP-Subnetz wird in der Active Directory-Verwaltung hinterlegt und dient fortan zur Unterscheidung der Standorte im Active Directory. Das wichtigste Verwaltungswerkzeug, um Standorte im Active Directory zu verwalten, ist das Snap-In *Active Directory-Standorte und -Dienste* (siehe *Abbildung 3.3*).

### Voraussetzungen für eine Routingtopologie

Die Standorte müssen mit WAN-Leitungen angebunden werden. Dazu ist es nicht unbedingt notwendig, dass jeder Standort mit der Zentrale durch eine Sterntopologie angebunden ist. Die Replikation im Active Directory ermöglicht auch die Anbindung von Standorten, die zwar mit anderen Standorten verbunden sind, aber nicht mit der Zentrale.

In jedem Standort sollten darüber hinaus ein oder mehrere unabhängige IP-Subnetze verwendet werden. Das Active Directory unterscheidet auf Basis dieser IP-Subnetze, ob Domänencontroller zum gleichen oder zu unterschiedlichen Standorten gehören. Auf dieser Basis werden in Exchange Server 2007 auch E-Mails geroutet, die entsprechenden Connectoren werden automatisch angelegt.

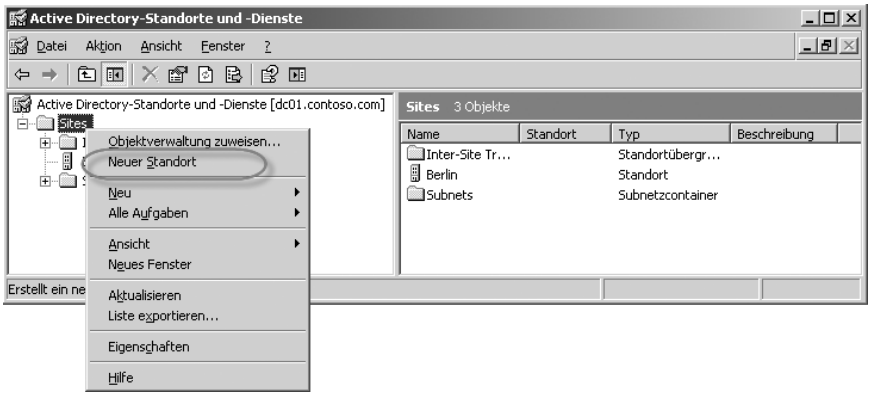
### Erstellen von neuen Standorten im Snap-In Active Directory-Standorte und -Dienste

Sobald die Voraussetzungen für die Routingtopologie vorhanden sind, sollten Sie die einzelnen physischen Standorte im Snap-In *Active Directory-Standorte und -Dienste* erstellen.

Öffnen Sie das Snap-In, wird unterhalb des Menüpunktes *Sites* der erste Standort als *Standardname-des-ersten-Standortes* bezeichnet. Im ersten Schritt sollten Sie für diesen Standardnamen einen richtigen Namen eingeben, indem Sie ihn mit der rechten Maustaste anklicken und *Umbenennen* wählen. Sie müssen die Domänencontroller im Anschluss nicht neu starten, der Name wird sofort aktiv.

Als Nächstes können Sie alle notwendigen Standorte erstellen, an denen Sie Domänencontroller installieren wollen. Klicken Sie dazu mit der rechten Maustaste im Snap-In auf den Menüpunkt *Sites* und wählen aus dem Menü die Option *Neuer Standort* aus (siehe *Abbildung 3.3*).

**Abbildung 3.3:** Erstellen eines neuen Standortes




Es öffnet sich ein neues Fenster, in dem Sie den Namen des Standortes sowie die Standortverknüpfung, die diesem Standort zugewiesen werden soll, auswählen können.

Standardmäßig gibt es bereits die Verknüpfung *DEFAULTIPSITELINK*. Verwenden Sie bei der Erstellung eines neuen Standortes zunächst diese Standortverknüpfung (siehe *Abbildung 3.4*).

Später werden in diesem Abschnitt noch neue Standortverknüpfungen erstellt und den einzelnen Standorten zugewiesen.

Bestätigen Sie die Erstellung mit *OK*, erhalten Sie eine Meldung, welche Aufgaben nach der Erstellung noch notwendig sind (siehe *Abbildung 3.5*). Bestätigen Sie diese Meldung, damit der Standort erstellt wird.

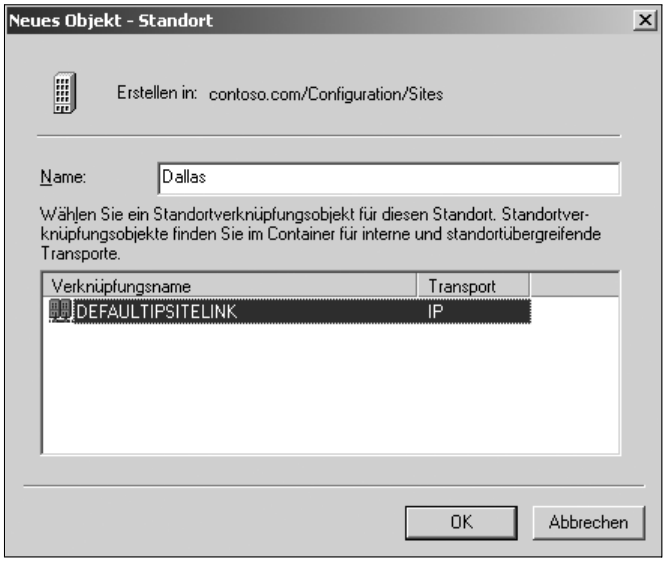



**Abbildung 3.4:** Erstellen eines neuen Standortes und Festlegen der Standortverknüpfung

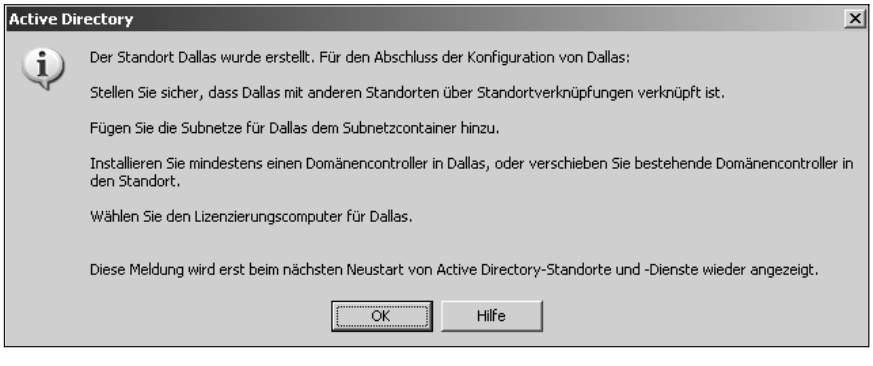



**Abbildung 3.5:** Meldung bei der Erstellung eines neuen Standortes

Sobald diese Meldung bestätigt wird, erscheint der neue Standort im Snap-In. Legen Sie auf die gleiche Weise alle Standorte in Ihrer Gesamtstruktur an.


*Nur Mitglieder der Gruppe* Organisations-Admins *dürfen neue Standorte im Active Directory erstellen.*

## Erstellen und Zuweisen von IP-Subnetzen

Haben Sie die Standorte erstellt, an denen Domänencontroller installiert werden sollen, müssen Sie IP-Subnetze anlegen und diese dem jeweiligen Standort zuweisen.

Um ein neues Subnetz zu erstellen, klicken Sie mit der rechten Maustaste im Snap-In *Active Directory-Standorte und -Dienste* auf den Menüpunkt *Subnets* und wählen aus dem Menü *Neues Subnetz* aus (siehe *Abbildung 3.6*).

Es öffnet sich ein neues Fenster, in dem Sie das IP-Subnetz definieren und dem jeweiligen Standort zuweisen können (siehe *Abbildung 3.7*).

Haben Sie das Subnetz erstellt und die Erstellung mit *OK* bestätigt, wird es unterhalb des Menüs *Subnets* angezeigt.

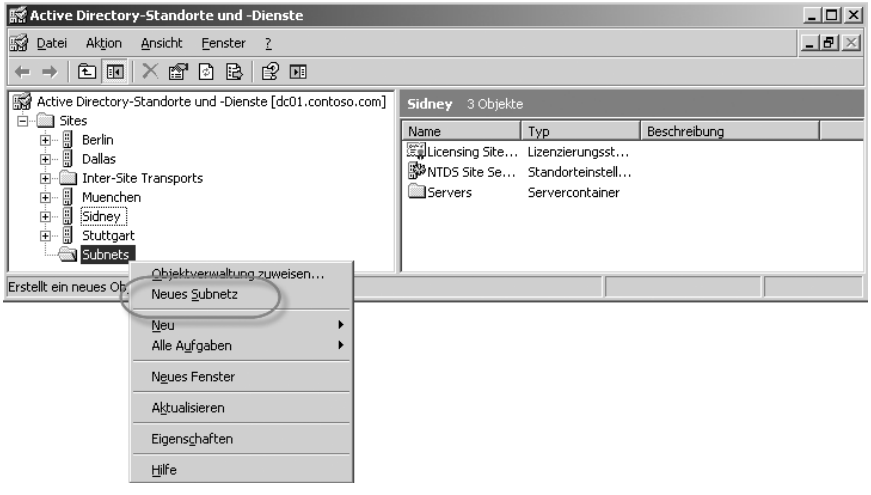



**Abbildung 3.6:** Erstellen eines neuen IP-Subnetzes in der Active Directory-Verwaltung

Wiederholen Sie diesen Vorgang für jedes Subnetz in Ihrem Unternehmen. Auch IP-Subnetze, in denen keine Domänencontroller installiert sind, in denen aber unter Umständen Mitgliedsrechner liegen, die sich bei dem Domänencontroller anmelden, sollten Sie an dieser Stelle anlegen und dem entsprechenden Standort zuweisen.

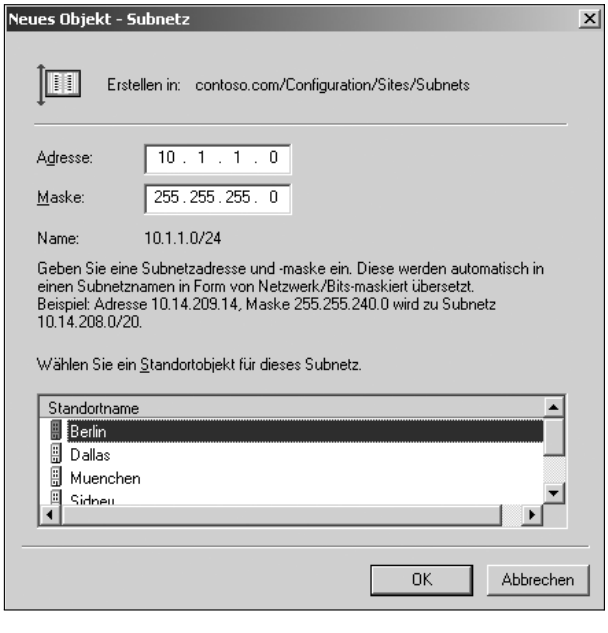



**Abbildung 3.7:** Anlegen neuer Subnetze

Klicken Sie den Menüpunkt *Subnets* an, werden Ihnen auf der rechten Seite alle IP-Subnetze und die ihnen zugewiesenen Standorte angezeigt (siehe *Abbildung 3.8*).

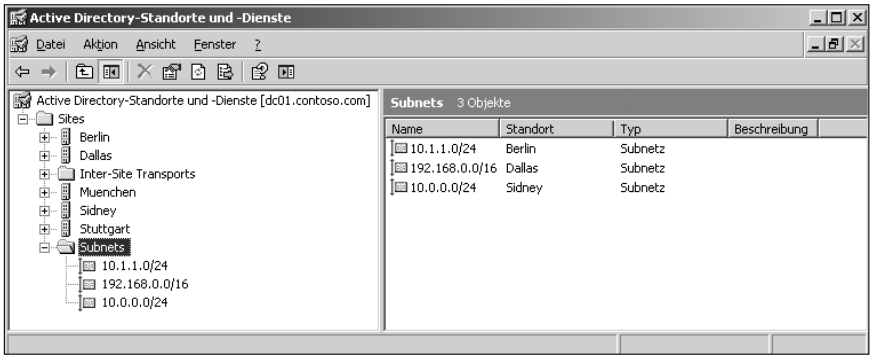



**Abbildung 3.8:** Anzeigen der angelegten IP-Subnetze in der Active Directory-Verwaltung



Die Zuweisung des Subnetzes zu einem bestimmten Standort kann jederzeit über dessen Eigenschaften geändert werden. Sie können auch nachträglich Standorte erstellen und neue Subnetze vorhandenen Standorten zuweisen.

### Erstellen von Standortverknüpfungen

Haben Sie Standorte und IP-Subnetze erstellt, können Sie neue *Standortverknüpfungen* anlegen.

Bei der Installation von Active Directory wird bereits automatisch die Standortverknüpfung *DEFAULTIPSITELINK* angelegt. Für viele Unternehmen reicht diese Verknüpfung bereits aus. Setzen Sie in Ihrem Unternehmen verschiedene Bandbreiten der WAN-Leitungen ein, macht es Sinn, auch verschiedene Standortverknüpfungen zu erstellen. Sie können auf Basis jeder Standortverknüpfung einen Zeitplan festlegen, wann die Replikation möglich ist.

Standortverknüpfungen können auf Basis von IP oder SMTP erstellt werden. SMTP hat starke Einschränkungen bei der Replikation und wird nur selten verwendet. Sie sollten daher auf das IP-Protokoll setzen, über das von Active Directory alle Daten repliziert werden können.

Um eine neue Standortverknüpfung zu erstellen, klicken Sie mit der rechten Maustaste auf den Menüpunkt *IP* unterhalb des Menüs *Inter-Site Transports* (siehe *Abbildung 3.9*).

Wählen Sie aus dem Menü die Option *Neue Standortverknüpfung* aus. Den Menüpunkt *Neue Standortverknüpfungsbrücke* benötigen Sie an dieser Stelle nicht.

*Standortverknüpfungsbrücken* werden verwendet, wenn zwischen zwei Standorten keine physische Verbindung besteht, aber beide über einen dritten Standort angebunden sind. Standortverknüpfungsbrücken werden automatisch erstellt. Sie müssen diese nur dann manuell erstellen, wenn Sie den Automatismus deaktivieren. Diese automatische Erstellung können Sie deaktivieren, wenn Sie die Eigenschaften des Menüpunktes *IP* unterhalb des Menüs *Inter-Site Transports* aufrufen und die Option *Brücke zwischen allen Standortverknüpfungen herstellen* deaktivieren (siehe *Abbildung 3.10*).

*Sie sollten die automatische Erstellung von Standortverknüpfungsbrücken nicht deaktivieren.*

**Abbildung 3.9:** Erstellen einer neuen Standortverknüpfung

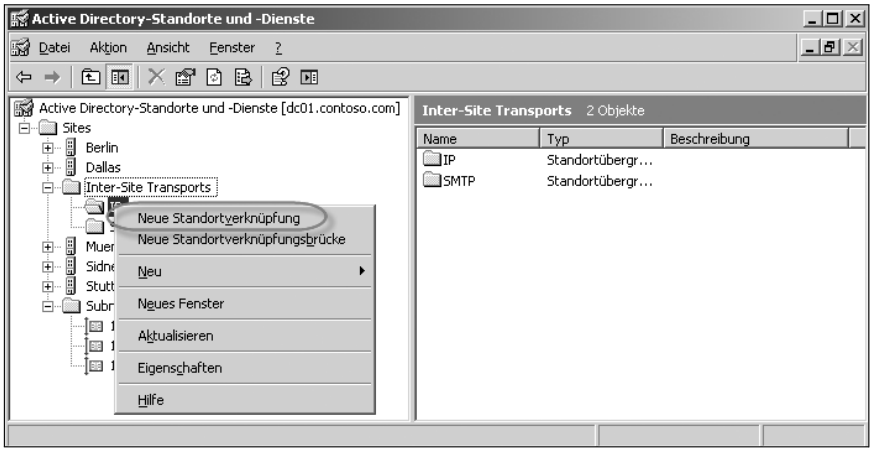
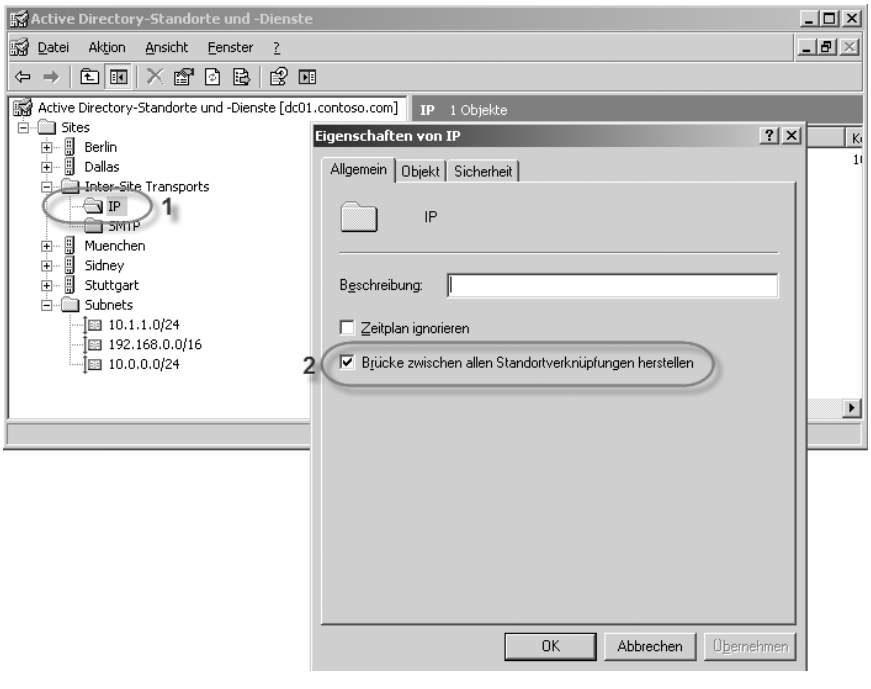



**Abbildung 3.10:** Automatische Erstellung von Standortverknüpfungsbrücken




Haben Sie die Erstellung einer neuen Standortverknüpfung gewählt, erscheint das Fenster, in dem Sie die Bezeichnung der Standortverknüpfung sowie die Standorte eingeben (siehe *Abbildung 3.11*). Wählen Sie den Namen der Standortverknüpfung so, dass bereits durch die Bezeichnung der Standortverknüpfung darauf geschlossen werden kann, welche Standorte miteinander verbunden sind, zum Beispiel *Berlin < > Stuttgart*.

In diesem Fenster können Sie auswählen, welche Standorte mit dieser Standortverknüpfung verbunden werden. Ein Standort kann Mitglied mehrerer Standortverknüpfungen sein. Die Replikation findet immer über die Standortverknüpfung statt,

deren konfigurierte Kosten am geringsten sind. Haben Sie den Namen der neuen Standortverknüpfung und deren Mitglieder festgelegt, können Sie mit *OK* die Erstellung abschließen.

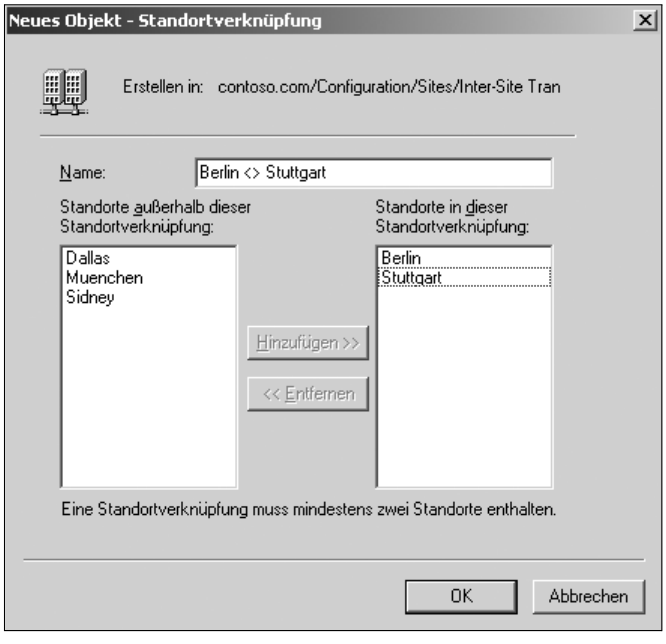



**Abbildung 3.11:** Erstellen einer neuen Standortverknüpfung



Klicken Sie das Protokoll *IP* an, werden auf der rechten Seite alle erstellten Standortverknüpfungen angezeigt (siehe *Abbildung 3.12*).

Haben Sie die Standortverknüpfung erstellt, können Sie die Eigenschaften der Verknüpfung im Snap-In *Active Directory-Standorte und -Dienste* anpassen.

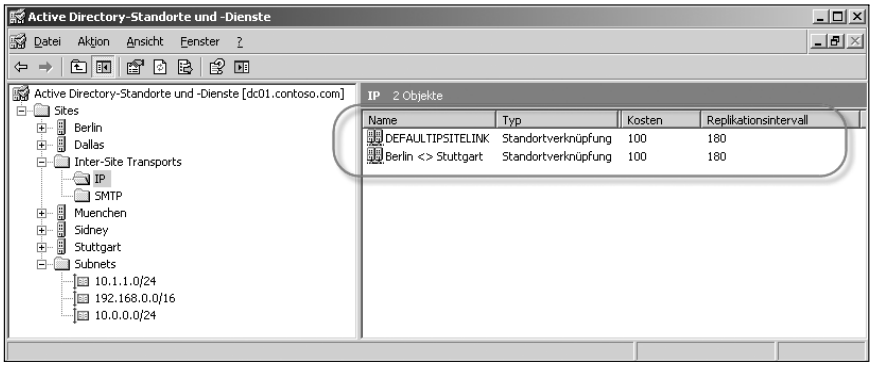



**Abbildung 3.12:** Anzeigen der Standortverknüpfungen

Rufen Sie die Eigenschaften einer Standortverknüpfung auf, können Sie einige Optionen ändern (siehe *Abbildung 3.13*).

**Abbildung 3.13:** Eigenschaften einer Standortverknüpfung


Auf der Registerkarte *Allgemein* können Sie zunächst festlegen, in welchem Intervall die Informationen zwischen den Standorten repliziert werden sollen. Standardmäßig ist die Replikation auf alle drei Stunden sowie die Kosten auf 100 eingestellt. Die Active Directory-Replikation verwendet immer die Standortverknüpfungen, deren Kosten bei der Verbindung am günstigsten sind.

Klicken Sie auf die Schaltfläche *Zeitplan ändern*, können Sie festlegen, zu welchen Zeiten die Replikation über diese Standortverknüpfung möglich ist. Sie können zum Beispiel für Niederlassungen mit schmalbandiger Verbindung die Replikation nur außerhalb der Geschäftszeiten oder am Wochenende zulassen (siehe *Abbildung 3.14*). Die Replikationsdaten des Active Directorys werden zwischen verschiedenen Standorten komprimiert.

### 3.2.2 Zuweisen der Domänencontroller zu den Standorten

Haben Sie die Routingtopologie erstellt, werden neu installierte Domänencontroller durch ihre IP-Adresse automatisch dem richtigen Standort zugewiesen.

Bereits installierte Domänencontroller müssen Sie jedoch manuell an den richtigen Standort verschieben. Klicken Sie dazu den Server im Snap-In *Active Directory-Standorte und -Dienste* mit der rechten Maustaste an und wählen Sie aus dem Kontextmenü die Option *Verschieben* aus. Dann werden Ihnen alle Standorte angezeigt und Sie können den neuen Standort des Domänencontrollers auswählen (siehe *Abbildung 3.15*).

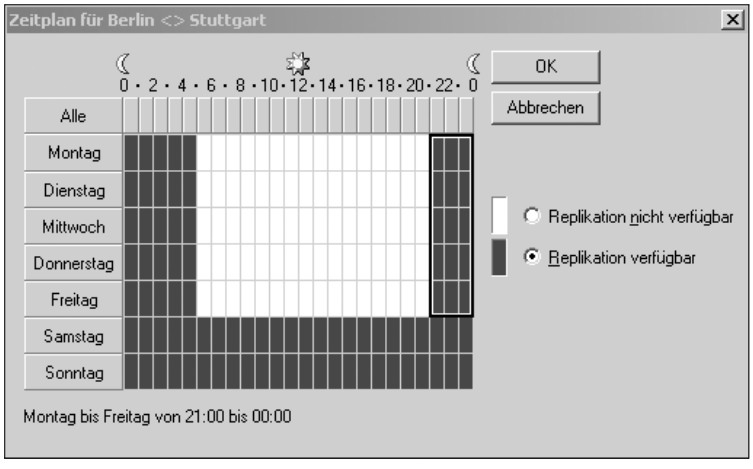



**Abbildung 3.14:** Konfiguration der Active Directory-Replikation



Haben Sie den Domänencontroller an einen anderen Standort verschoben, sollten Sie den Server neu starten. Sie können einen Domänencontroller auch mit Drag&Drop an einen anderen Standort verschieben. Achten Sie vor dem Verschieben des Domänencontrollers darauf, dass die IP-Einstellungen des Servers zu den zugewiesenen IP-Subnetzen des neuen Standortes passen.

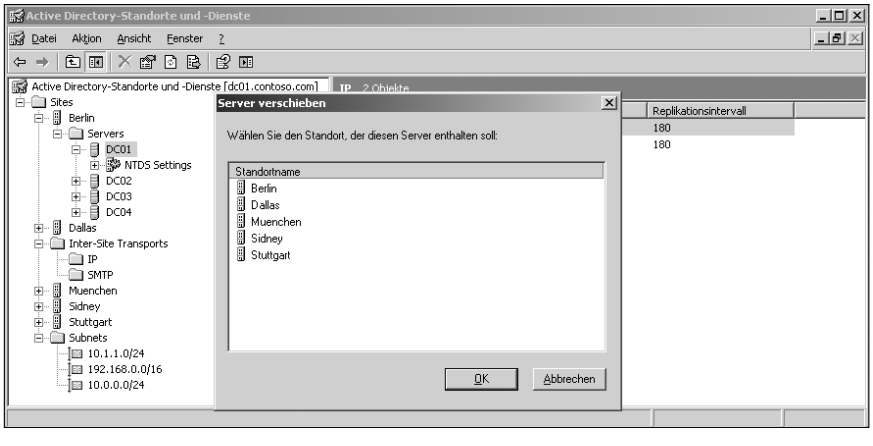



**Abbildung 3.15:** Verschieben eines Domänencontrollers an einen anderen Standort

## 3.2.3 Der Knowledge Consistency Checker (KCC)

Haben Sie die Routingtopologie wie beschrieben erstellt, kann der *KCC* die Verbindung der Domänencontroller automatisch herstellen. Der KCC konfiguriert auf Basis der konfigurierten Standorte, der Standortverknüpfungen und deren Zeitplänen und Kosten sowie den enthaltenen Domänencontrollern automatisch die Active Directory-Replikation.

Der KCC läuft vollkommen automatisch auf jedem Domänencontroller der Gesamtstruktur. Sind zwei Standorte nicht durch Standortverknüpfungen verbunden, erstellt er automatisch Standortverknüpfungsbrücken, wenn eine Verbindung über einen dritten Standort hergestellt werden kann.

Der KCC verbindet nicht jeden Domänencontroller mit jedem anderen, sondern erstellt eine intelligente Topologie. Er überprüft die vorhandenen Verbindungen alle 15 Minuten auf ihre Funktionalität und ändert bei Bedarf automatisch die Replikationstopologie.

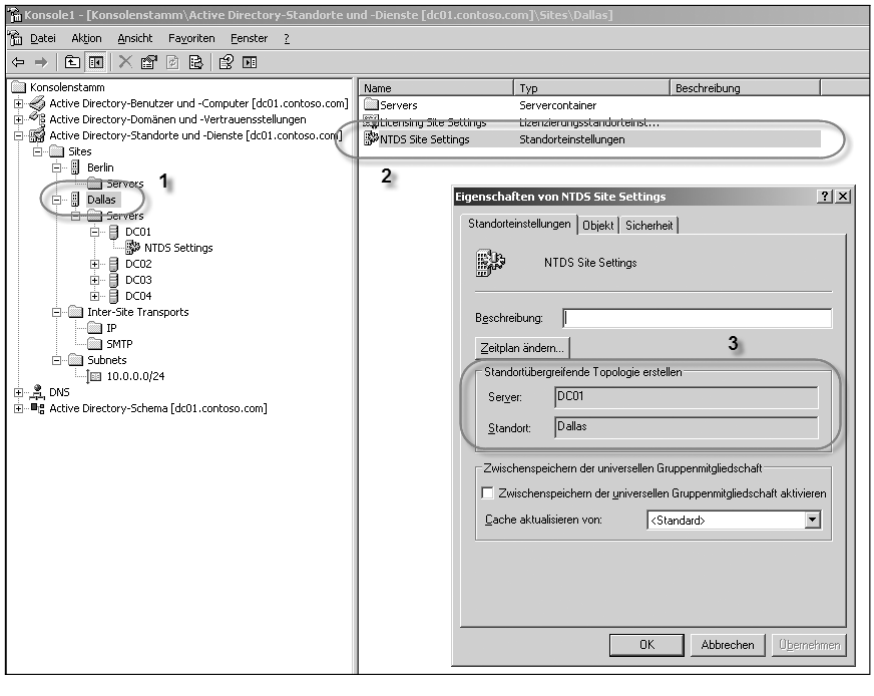
Innerhalb eines Standortes erstellt der KCC möglichst eine Ringtopologie, wobei zwischen zwei unterschiedlichen Domänencontrollern maximal drei andere Domänencontroller stehen sollten.

Zwischen verschiedenen Standorten werden die Active Directory-Daten nicht von allen Domänencontrollern auf die anderen Domänencontroller der Standorte übertragen, sondern immer jeweils nur von einem Domänencontroller. Dieser Domänencontroller, auch *Brückenkopfserver (Bridgeheadserver)* genannt, repliziert sich mit den Bridgeheadservern der anderen Standorte automatisch. Der KCC legt automatisch fest, welche Domänencontroller in einer Niederlassung zum Bridgeheadserver konfiguriert werden, Sie müssen keine Eingaben oder Maßnahmen vornehmen.

Die Auswahl der Bridgeheadserver in einem Standort übernimmt der *Intersite Topology Generator (ISTG)*, ein Dienst, der zum KCC gehört. Der KCC wiederum legt für jeden Standort fest, welcher Domänencontroller der ISTG sein soll.

Klicken Sie einen Standort im Snap-In *Active Directory-Standorte und -Dienste* an, wird auf der rechten Seite der Menüpunkt *NTDS Site Settings* angezeigt. Rufen Sie die Eigenschaften dieses Menüpunktes auf, wird Ihnen im Bereich *Standortübergreifende Topologie erstellen* der derzeitige ISTG angezeigt (siehe *Abbildung 3.16*).

**Abbildung 3.16:** Anzeigen des ISTG eines Standortes




Standardmäßig überprüft der KCC automatisch alle 15 Minuten die Funktionalität der Routingtopologie. Haben Sie Änderungen an der Routingtopologie durchgeführt, besteht die Möglichkeit, die Routingtopologie sofort erstellen zu lassen.

Am besten kann die Routingtopologie vom derzeitigen ISTG-Rolleninhaber aus überprüft werden. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Snap-In *Active Directory-Standorte und -Dienste.*
2. Navigieren Sie zu dem Standort, von dem aus Sie die Überprüfung starten wollen.
3. Klicken Sie auf das Pluszeichen des derzeitigen ISTG-Rolleninhabers des Standortes.
4. Klicken Sie mit der rechten Maustaste auf den Menüpunkt *NTDS-Settings* und wählen aus dem Menü *Alle Aufgaben/Replikationstopologie überprüfen* (siehe *Abbildung 3.17*).



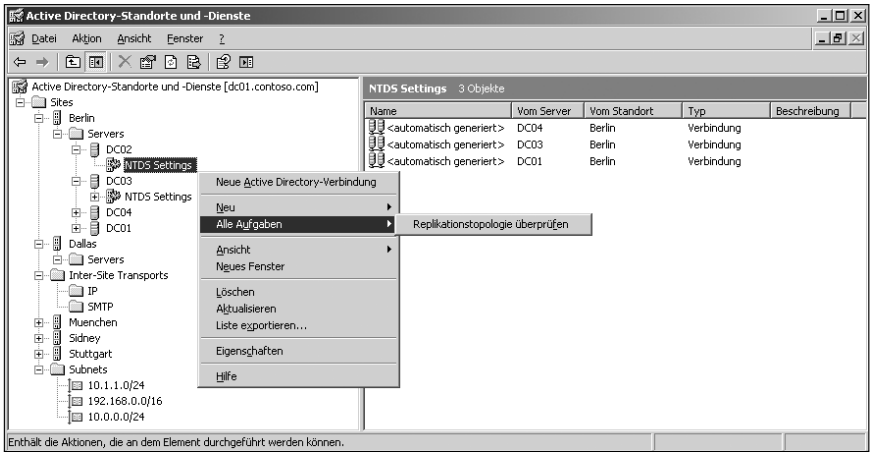



**Abbildung 3.17:** Manuelles Starten der Routingtopologie

Die Überprüfung dauert einige Zeit, abhängig von der Anzahl der Standorte und Domänencontroller.

Alle Verbindungen werden überprüft und gegebenenfalls neu erstellt. Sie erhalten eine entsprechende Meldung (siehe *Abbildung 3.18*).

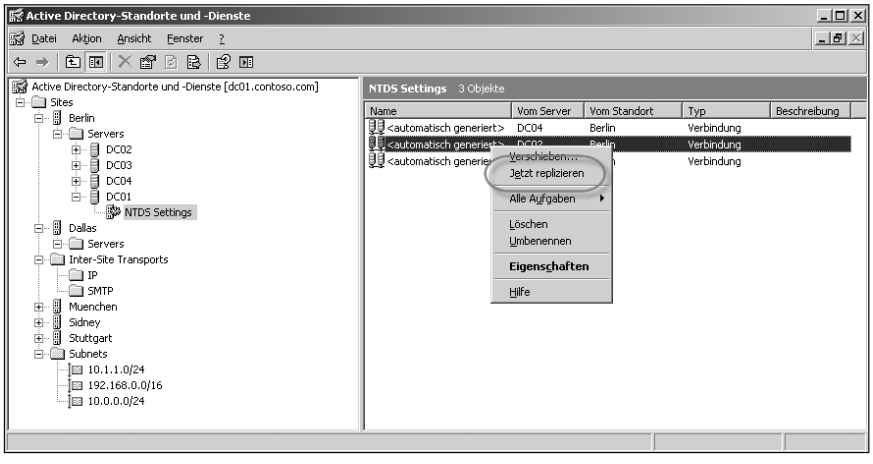

**Abbildung 3.18:** Meldung der manuellen Überprüfung der Replikation

## 3.2.4 Starten der manuellen Replikation

Sie können die Replikation zwischen zwei Domänencontrollern jederzeit manuell starten. Die Verbindungen, die der KCC erstellt hat, werden als *<automatisch generiert>* angezeigt (siehe *Abbildung 3.19*).

Klicken Sie eine solche Verbindung mit der rechten Maustaste an, können Sie die Replikation zu diesem Server mit der Option *Jetzt replizieren* sofort ausführen.

**Abbildung 3.19:** Manuelle Replikation der Active Directory-Verbindungen




Starten Sie die Replikation zu einem Domänencontroller, der in einem anderen Standort sitzt, wird die Replikation allerdings nicht sofort durchgeführt, sondern erst zum nächsten Zeitpunkt, den der Zeitplan zulässt.

Bevor die Daten repliziert werden, stellt der Domänencontroller zunächst sicher, ob er eine Verbindung zu dem Domänencontroller herstellen kann, zu dem die Daten repliziert werden. Kann mit dem Replikationspartner erfolgreich kommuniziert werden, erhalten Sie eine entsprechende Erfolgsmeldung (siehe *Abbildung 3.20*).

**Abbildung 3.20:** Erfolgreiche Replikation


Kann der Replikationspartner nicht erreicht werden, erhalten Sie eine Fehlermeldung.

## 3.3 Systemdienste von Exchange Server 2007

Bei Exchange Server 2007 gibt es einige neue Dienste, während Dienste von Exchange 2000 und 2003 weggefallen sind. Im folgenden Abschnitt gehe ich ausführlicher auf die einzelnen Systemdienste von Exchange Server 2007 ein. Sie finden die Dienste am schnellsten über *Start/Ausführen/services.msc (siehe Abbildung 3.21)*.

Abhängig von den installierten Rollen werden nicht immer alle Dienste installiert oder gestartet. Im folgenden Abschnitt gehe ich auch darauf ein, welche Dienste auf welchen Serverrollen gestartet sein müssen.

- *Microsoft Exchange-Antispamaktualisierung* – Dieser Dienst ist für das Download der Antispamdefinitionen notwendig (siehe Kapitel 13).
- *Microsoft Exchange Active Directory-Topologiedienst* – Da Exchange Server 2007 stärker mit den Active Directory-Standorten zusammenarbeitet als seine Vor-

gängerversionen, wurde ein neuer Dienst benötigt, der für die Synchronisierung der Daten mit dem Active Directory zuständig ist. Dieser Dienst hat keine Abhängigkeiten und läuft auf allen Servern mit den Rollen Mailbox, Client-Access, Hub-Transport und Unified Messaging.

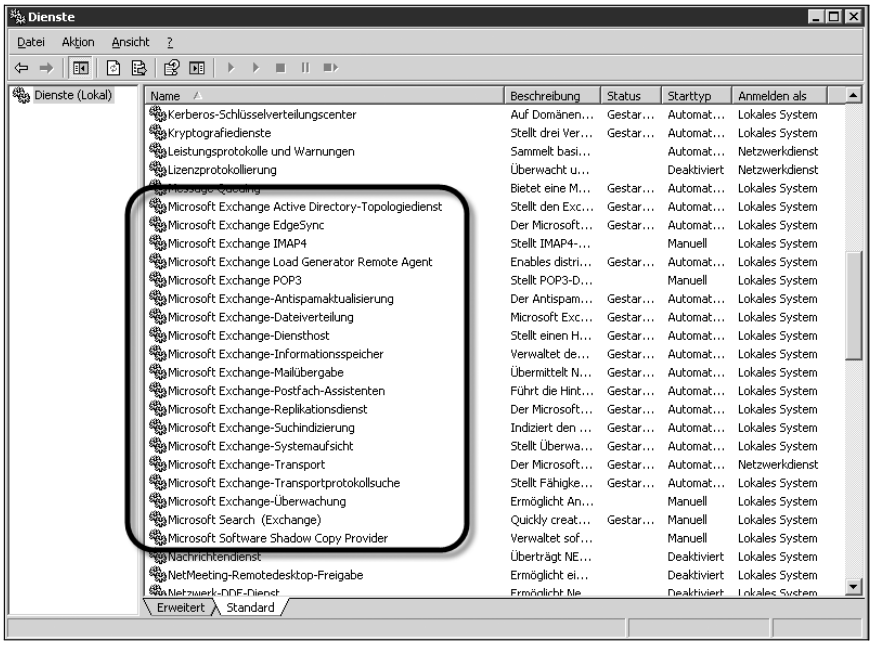



**Abbildung 3.21:** Anzeigen der Systemdienste von Exchange Server 2007

- *Microsoft Exchange EdgeSync* – Dieser Dienst dient zur Synchronisation von Daten mit eventuell vorhandenen Edge-Transport-Servern. Dieser Dienst spielt im Bereich des Spamschutzes eine Rolle, da hierüber auch die Daten der Empfänger mit Outlook synchronisiert werden, welche die vertrauten Absender betreffen. Dieser Dienst ist vom Systemdienst *Microsoft Exchange Active Directory-Topologiedienst* abhängig und ist auch für die Synchronisierung von ADAM-Daten per LDAP zwischen Edge-Transport-Servern und Hub-Transport-Servern zuständig. Der Dienst läuft ausschließlich auf Servern mit der Rolle Hub-Transport.
- *Microsoft Exchange-Dateiverteilung* – Dieser Dienst läuft auf Servern mit der Client-Access-Server-Rolle und ist dafür zuständig, den Inhalt des Offline-Adressbuches von dem Exchange-Server zu replizieren, der für die Erstellung des Offline-Adressbuches zuständig ist. Der Dienst läuft auf Servern mit den Rollen Client-Access und Unified Messaging.
- *Microsoft Exchange IMAP4* und *Microsoft Exchange POP3* – Diese Dienste steuern den Zugriff von Benutzern über das POP3- oder IMAP-Protokoll auf den Servern. Outlook verwendet zum Zugriff MAPI und liest demnach direkt den Informationsspeicher. Sollen Anwender auch per IMAP oder POP3 auf Ihre Postfächer zugreifen können (zum Beispiel über das Internet), werden diese beiden Dienste benötigt. Dieser Dienst werden ausschließlich auf Client-Access-Servern (CAS) benötigt.

- *Microsoft Exchange Mailübergabe* – Dieser Dienst ist dafür zuständig, E-Mails von Mailbox-Servern zu Hub-Transport-Servern zu transportieren. Hub-Transport-Server transportieren dann die E-Mails zu den jeweiligen Hub-Transport-Servern im Active Directory-Standort des Empfängers. Dieser Dienst ist vom Systemdienst *Microsoft Exchange Active Directory-Topologiedienst* abhängig. Der Dienst läuft auf Servern mit der Rolle Mailbox.
- *Microsoft Exchange-Postfach-Assistenten* – Dieser Dienst stellt verschiedene Funktionen für Kalender und die Planung von Ressourcen für Besprechungsanfragen bereit. Er wird auch für den Abwesenheits-Assistenten benötigt. Dieser Dienst ist vom Systemdienst *Microsoft Exchange Active Directory-Topologiedienst* abhängig. Der Dienst läuft auf Servern mit der Rolle Mailbox.
- *Microsoft Exchange Replikationsdienst* – Dieser Dienst wird für die forlaufende lokale Sicherung (Local Continuous Replication, LCR) benötigt. Dieser Dienst ist vom Systemdienst *Microsoft Exchange Active Directory-Topologiedienst* abhängig. Der Dienst läuft auf Servern mit der Rolle Mailbox. Ist dieser Dienst nicht gestartet, werden keine Daten mehr für LCR epliziert (siehe Kapitel 6).
- *Microsoft Search (Exchange)* – Dieser Dienst verwaltet die Indizierung auf dem Server sowie die Suche nach E-Mails. Verwenden Sie keine Indizierung, benötigen Sie diesen Dienst nicht. Haben Sie jedoch die Indizierung einzelner Informationsspeicher aktiviert, steht der Index lediglich dann zur Verfügung, wenn dieser Dienst gestartet ist. Der Dienst läuft auf Servern mit der Rolle Mailbox.
- *Microsoft Exchange-Suchindizierung* – Dieser Dienst ist für die Indizierung der Postfachspeicherdatenbanken zuständig.
- *Microsoft Exchange-Transport* – Dieser Dienst stellt den SMTP-Server des Exchange-Servers zur Verfügung und ist für den Transport-Stack des Servers zuständig. Der Dienst läuft auf Servern der Rolle Hub-Transport und Edge-Transport. Beenden Sie den Dienst, ist der Server über Port 25 nicht mehr erreichbar.
- *Microsoft Exchange Transportprotokollsuche* – Dieser Dienst wird für die Nachrichtenverfolgung (Message Tracking) und das Durchsuchen der Protokolle für den Nachrichtenversand zuständig (nicht verwechseln mit den Transaktionsprotokollen der Datenbank). Der Dienst läuft auf Servern mit den Rollen Mailbox, Hub-Transport und Edge-Transport.
- *Microsoft Exchange-Diensthost* – Dieser Dienst ist für das virtuelle RPC-Verzeichnis im IIS zuständig und damit für die Outlook Anywhere (RPC über HTTP)-Funktionalität von Exchange Server 2007 (siehe Kapitel 9). Der Dienst läuft auf Servern mit den Rollen Mailbox und Client-Access.
- *Microsoft Exchange-Informationsspeicher* – Der Informationsspeicher ist für die Verbindung zu den Exchange-Datenbanken zuständig. Er ermöglicht den Benutzern Zugriff auf den Postfachspeicher und den Speicher für die öffentlichen Ordner. Ohne diesen Dienst ist kein Zugriff auf die Postfächer der Benutzer möglich. Er wird nur auf Mailbox-Servern benötigt.
- *Microsoft Exchange-Systemaufsicht* – Dieser Dienst ist für die Überwachung und Verwaltung von Exchange Server 2007 zuständig. Außerdem koordiniert dieser Dienst die Active Directory-Abfragen der verschiedenen Systemdienste von Exchange Server 2007. Der Dienst wird auf Mailbox-Servern benötigt.

- *Microsoft Exchange-Überwachung* – Dieser Dienst stellt den RPC-Server für die in Kapitel 2 beschriebenen *CMDlets* zur Verfügung, die für die Diagnose verwendet werden. Dieser Dienst läuft auf allen Serverrollen.
- *Microsoft Exchange ADAM* – Dieser Dienst ist auf Edge-Transport- Servern für die Synchronisierung der Active Directory-Daten mit dem ADAM auf dem Edge-Transport-Server zuständig. Dieser Dienst verwaltet die ADAM-Instanz, die während der Installation eines Edge-Transport-Servers automatisch angelegt wird.
- *Microsoft Exchange Credential Service* – Dieser Dienst ist für die Anmeldedaten zuständig, die zwischen ADAM und den Edge-Transport-Servern synchronisiert werden müssen. Er läuft nur auf Edge-Transport-Servern.
- *Microsoft Exchange Speech Engine* – Dieser Dienst wird auf Unified Messaging-Servern benötigt. Er ist für die Verwendung der Outlook Voice Access (OVA)-Funktion notwendig.
- *Microsoft Exchange-Unified Messaging* – Dieser Dienst stellt die Unified Messaging-Funktionen bereit. Er routet eingehende Faxe und Sprachnachrichten in die Postfächer der Anwender. Der Dienst läuft nur auf Unified Messaging Servern und ist von den beiden Diensten *Microsoft Exchange Active Directory Topologiedienst* und *Microsoft Exchange Speech Engine* abhängig.



## 3.4 Verzeichnisstruktur von Exchange Server 2007

Auch wenn die verschiedenen Verzeichnisse von Exchange Server 2007 nicht ständig zur Verwaltung benötigt werden, sollten Administratoren zumindest oberflächlich die Funktion der einzelnen Unterordner im Exchange Server 2007-Installationsverzeichnis kennen. Ich komme in den einzelnen Kapiteln dieses Buches noch auf das eine oder andere Verzeichnis zu sprechen. Im folgenden Abschnitt gehe ich auf die wichtigsten Verzeichnisse ein.

Standardmäßig wird Exchange Server 2007 im Verzeichnis *C:\Programme\Microsoft\Exchange-Server* installiert. Sie können das Installationsverzeichnis jedoch frei wählen. Unabhängig vom Installationsverzeichnis gibt es Unterordner mit verschiedenen Funktionen. Die Verzeichnisstruktur wurde im Vergleich zu Exchange 2000/2003 deutlich verändert *(siehe Abbildung 3.22)*.

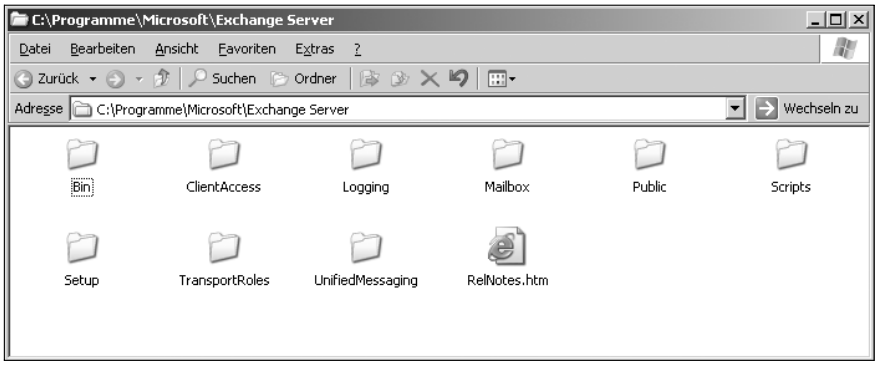
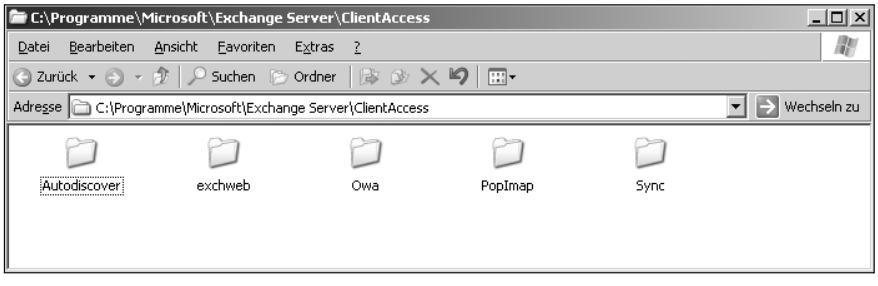



**Abbildung 3.22:** Exchange Server 2007-Verzeichnis-Struktur

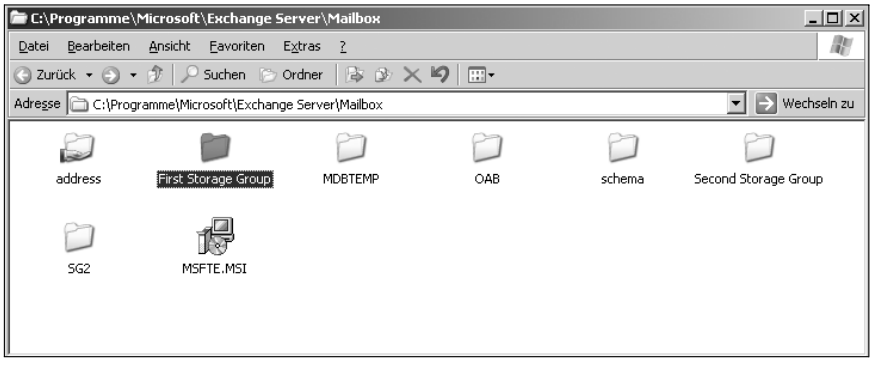
- *\bin* – In diesem Verzeichnis werden die Verwaltungsprogramme und Zusatzprogramme von Exchange Server 2007 gespeichert. Hier finden Sie die ausführenden Dateien und wichtigsten Programme sowie die Systemdateien von Exchange Server 2007.
- *\ClientAccess* – In diesem Verzeichnis befindet sich die Konfiguration der Client-Access-Rolle eines Exchange-Servers. Dieses Verzeichnis spielt nur auf Client-Access-Servern eine Rolle. In diesem Verzeichnis befinden sich zum Beispiel die notwendigen Ordner für die Autodiscover-Funktion von Outlook 2007 und die Verzeichnisse *OWA, Exchweb*, sowie *POPImap* und *Sync (siehe Abbildung 3.23)*. Diese Verzeichnisse enthalten dann wiederum die Installations- und Konfigurationsdateien der entsprechenden Funktion.

**Abbildung 3.23:** Verzeichnis ClientAccess auf Client-Access-Servern




- *\Logging* – In diesem Verzeichnis befinden sich verschiedene Logdateien von Exchange Server 2007, allerdings nicht die Transaktionsprotokolle der Datenbank (siehe Kapitel 6). Die Transaktionsprotokolle werden im Verzeichnis *Mailbox* abgelegt.
- *\Mailbox* – Dieses Verzeichnis enthält alle wichtigen Dateien, die zur Exchange-Datenbank gehören. Dieses Verzeichnis spielt hauptsächlich auf Mailbox-Servern eine Rolle. In diesem Verzeichnis liegen die Transaktionsprotokolle und die restlichen Dateien der Exchange-Datenbanken *(siehe Abbildung 3.24)*. Hier finden Sie auch die *.dll-Dateien für die Erstellung von E-Mail-Adressen. Hier werden auch die Daten des Offline-Adressbuches gespeichert. In diesem Verzeichnis liegen weiterhin die Daten und Konfigurationen der öffentlichen Ordner.

**Abbildung 3.24:** Mailbox-Verzeichnis auf Mailbox-Servern



- *\Public* – In diesem Verzeichnis liegen keine Daten von öffentlichen Ordnern, sondern die XML-Dateien und Treiber, die von Hub- Transport- und Edge-Transport-Servern benötigt werden, um E-Mails zu versenden. Aus diesem Grund spielt dieses Verzeichnis nur auf Hub-Transport- und Edge-Transport-Servern eine Rolle.
- *\Scripts* – Dieses Verzeichnis enthält die Skripte, welche die Exchange-Verwaltungsshell für automatisierte Aufgaben verwendet.
- *\Setup* – Dieses Verzeichnis enthält die beiden Unterordner *Data* und *Perf*. Diese Ordner enthalten wiederum notwendige XML-Dateien die für die Konfiguration von Exchange Server 2007 benötigt werden.



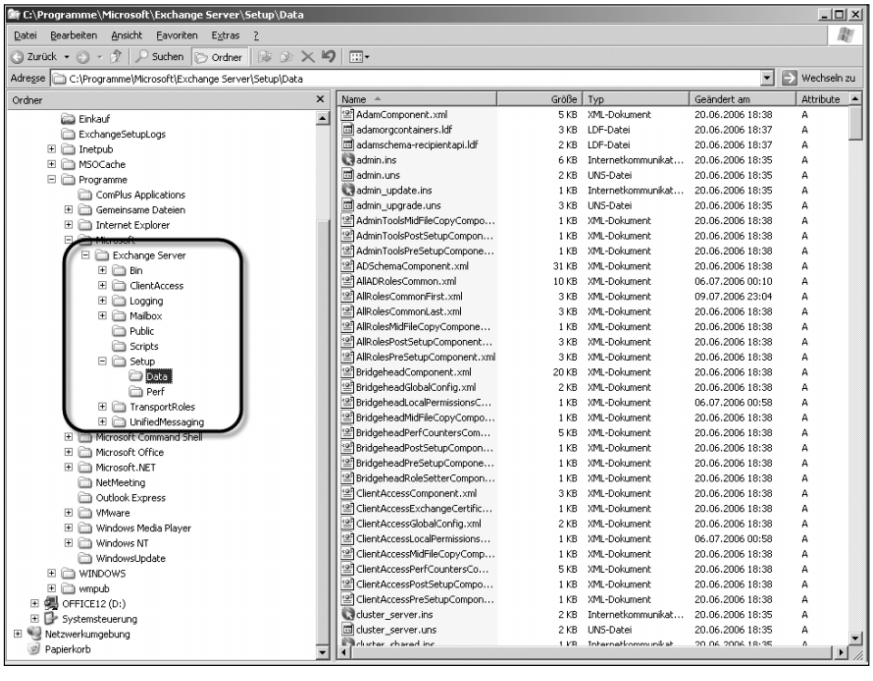



**Abbildung 3.25:** XML-Dateien für die Konfiguration von Exchange Server 2007

- *TransportRoles* – Dieses Verzeichnis enthält die Unterordner *Agent, data, Logs, Pickup, Replay* und *Shared*. Die beiden Verzeichnisse *Pickup* und *Shared* werden für den E-Mail-Versand benötigt. Alle Logdateien, die den E-Mail-Fluss von Hub-Transport- oder Edge-Transport-Servern betreffen, werden im Verzeichnis *Logs* gespeichert. Im Verzeichnis *Data* werden die Daten der IP-Filter-Datenbank und der Warteschlangen (siehe Kapitel 5 und 13) gespeichert. Ich gehe auf das Verzeichnis am Ende dieses Abschnitts noch ausführlicher ein, da gerade hier ein zentraler Punkt für den Nachrichtenfluss in Exchange Server 2007 liegt. Das Verzeichnis zur Verwaltung der Warteschlangen wird im Kapitel 5 besprochen, die Nachrichtenfilterung in Kapitel 13.
- *Unified Messaging* – Diese Daten enthalten die Daten für die Konfiguration der Unified Messaging-Rolle, der Spracherkennung und einige Skripte. Hier werden auch die Sprachnachrichten abgespeichert.

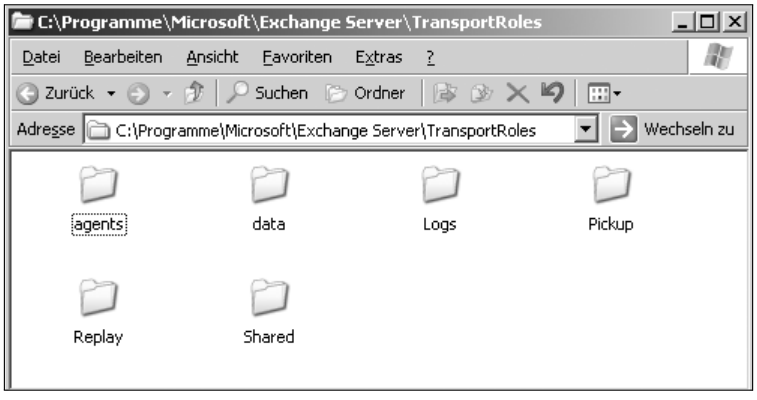



**Abbildung 3.26:** Verzeichnis TransportRoles in Exchange Server 2007

### Die Verzeichnisse Pickup und Replay für den Nachrichtenfluss verwalten

Die beiden wichtigsten Verzeichnisse unterhalb des Exchange-Verzeichnisses *TransportRoles* sind *Pickup* und *Replay*.

*Das Pickup-Verzeichnis für selbst erstellte E-Mails verwenden*

Legen Sie speziell formatierte E-Mail-Nachrichten als Dateien im *Pickup*-Verzeichnis ab, werden diese durch Exchange Server 2007 automatisch zugestellt. Diese Funktion können vor allem Administratoren zu Testzwecken, aber auch Applikationen verwenden, die E-Mail-Nachrichten über Exchange versenden wollen. Die Nachrichten werden als *.eml-Datei in das Pickup-Verzeichnis kopiert. Nach dem Kopiervorgang werden folgende Prozesse abgewickelt:

1. Exchange Server 2007 überprüft alle fünf Sekunden, ob sich im Pickup-Verzeichnis eine *.eml-Datei befindet. Dieser Intervall kann nicht verändert werden. Standardmäßig kann Exchange bis zu 100 Nachrichten pro Minute aus diesem Verzeichnis verwalten. Sie können diesen Grenzwert in der Exchange-Verwaltungsshell über den Befehl *Set-TransportServer* anpassen.
2. Im Anschluss überprüft Exchange, ob die Grenzwerte für Nachrichten in diesem Verzeichnis eingehalten worden sind, zum Beispiel maximale Empfänger und Größe des E-Mail-Headers. Auch diese Grenzwerte können über den Befehl *Set-TransportServer* steuern.
3. Als nächstes wird die aktuell verarbeitete *.eml-Datei in eine *.tmp-Datei umbenannt. Teilweise wird den Namen auch noch die aktuelle Zeit und das Datum angehängt, wenn bereits eine identische *.tmp-Datei existiert. Die Datei kann an dieser Stelle nicht mehr manuell gelöscht werden, sie wird durch das System gesperrt.
4. Als nächstes wird die Nachricht versendet und die *.tmp-Datei gelöscht. Wird der Dienst *Microsoft Exchange-Transport* während eines solchen Vorgangs neu gestartet, werden alle *.tmp-Dateien wieder in *.eml-Dateien umbenannt und der Prozess beginnt von vorne. Dieser Effekt kann in doppelt zugestellten E-Mail-Nachrichten resultieren.

Damit die Nachrichten über das Pickup-Verzeichnis zugestellt werden können, müssen die *.eml-Dateien entsprechende Voraussetzungen erfüllen:

- Die Nachricht muss als Textdatei dem SMTP-Format entsprechen (siehe *Listing 3.1*).
- Die Datei muss zwingend die Endung *.eml haben.
- Es muss mindestens ein Absender im *from:* Bereich der Datei existieren (siehe auch Kapitel 5).
- Es muss mindestens ein Empfänger im *To:*, *CC:*, oder *BCC:* -Bereich hinterlegt sein.
- Es muss eine Leerzeile zwischen Header und E-Mail-Body (dem Text der E-Mail existieren).



*Beispiel für eine Nachricht im Pickup-Verzeichnis:*

**Listing 3.1:** Beispiel einer *.eml-Datei zum Versenden über das Pickup-Verzeichnis.


```
To: administrator@contoso.com
From: test@contoso.com
Subject:Testnachricht

Das ist der E-Mail-Body mit dem Text.
```

Auch MIME-Nachrichten können im Verzeichnis abgelegt werden (siehe *Listing 3.2*). Diese Nachrichten werden dann allerdings eher von Applikationen erstellt, da sich diese nicht für Testzwecke eignen.

*Was ist MIME?*

In den Anfangszeiten des Internets bestand eine E-Mail nur aus einfachem Text im ASCII-Format. In der Zwischenzeit ist aber das Internet immer mehr gewachsen und der Wunsch, Texte mit Sonderzeichen, Umlauten usw. zu verschicken, kam immer mehr auf.

Auch möchte man sich nicht auf das Versenden von Text beschränken, sondern auch Grafiken, Audiofiles oder binäre Dateien versenden können. Für genau diese Zwecke wurde die *MIME (Multipurpose Internet Mail Extension)* Spezifikation festgelegt. Die MIME Spezifikation ergänzt den vorhandenen Standard um erweiterte Strukturen im Nachrichtentext und mit einer Definition zur Codierung von ASCII-fremden Nachrichten.

MIME ist ein Protokoll, welches ursprünglich dazu gedacht war, per E-Mail verschickte Dateien anhand ihrer Dateierweiterung zu erkennen und vor dem Verschicken mittels eines Headers zu kennzeichnen, um sie dann beim Empfänger mit der richtigen Software darzustellen oder wiederzugeben.

*Beispiel einer MIME-Datei im Pickup-Verzeichnis*:

**Listing 3.2:** Beispiel einer MIME-Datei


```
To: administrator@contoso.com
From: test@contoso.com
Subject: Message subject
MIME-Version: 1.0
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: 7bit
<HTML><BODY>
<TABLE>
```

```
<TR><TD>cell 1</TD><TD>cell 2</TD></TR>
<TR><TD>cell 3</TD><TD>cell 4</TD></TR>
</TABLE>
</BODY></HTML>
```

Kann eine Nachricht aus dem Pickup-Verzeichnis nicht zugestellt werden, bleibt die *.eml-Datei im Verzeichnis erhalten und es werden entsprechende Meldungen in der Ereignisanzeige im Anwendungsprotokoll protokolliert.

### Die Funktion des Replay-Verzeichnisses

Im Replay-Verzeichnis werden E-Mails abgelegt, die von Connectoren von Drittherstellern kommen oder in Exchange Server 2007 importiert wurden, um sie über den Server zu versenden. Grundsätzlich bietet aber das Replay-Verzeichnis die gleichen Funktionen und auch der Prozess für das Versenden von E-Mails ist identisch zum Pickup-Verzeichnis.