- Installation und Migration
- Connectoren und Datenbanken
- Backup, Diagnose, Troubleshooting
- Forefront TMG 2010
- Forefront Protection 2010
- Spam- und Virenschutz
- DAG und Cluster
- Archivierung
- Virtualisierung
- Windows Mobile 6 und 6.5
- Unified Messaging

Service Pack 1

Exchange Server 2010

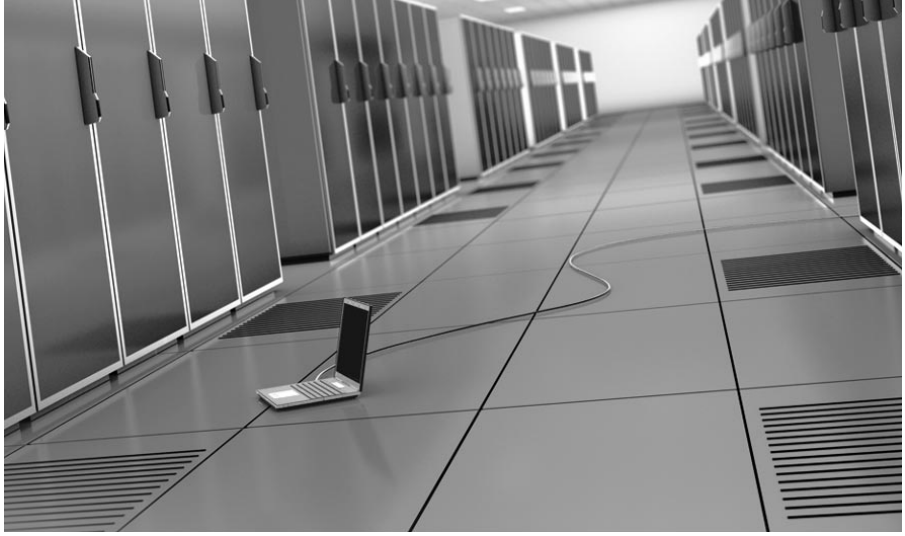
Planung, Installation, Migration und Betrieb

THOMAS JOOS

Markt+Technik

Video-Lektionen

KOMPENDIUM



Kapitel 16
Rollenbasierte Berechtigungen und Delegierung (RBAC)

Mit Exchange Server 2010 hat Microsoft das Berechtigungsmodell noch mal deutlich überarbeitet, auch im Vergleich zu Exchange Server 2007. In diesem Kapitel gehen wir ausführlicher auf die Delegation von Administratorrechten ein. Exchange Server 2010 arbeitet dazu mit Rollengruppen. Administratoren mit entsprechenden Rechten können andere Anwender diesen Gruppen hinzufügen, aber auch eigene Gruppen mit speziellen Rechten erstellen. Die Verwaltung der Berechtigungen in Exchange Server 2010 lassen sich nur in der Exchange-Verwaltungsshell durchführen. Eine Pflege in der Exchange-Verwaltungskonsole ist ohne das Service Pack 1 für Exchange Server 2010 nicht möglich. Neben zahlreichen Verbesserungen integriert Microsoft mit dem Service Pack 1 auch mehr Möglichkeiten in die Exchange-Verwaltungskonsole. Vor allem die Exchange-Systemsteuerung, die Sie über die Adresse *https://* < *Servername* > */ecp* erreichen, erhält mehr Funktionen. Nach der Installation von Service Pack 1 lassen sich in der Exchange-Systemsteuerung Transport- und Journalregeln anlegen. Auch die rollenbasierte Berechtigung (RBAC) lässt sich jetzt in der Systemsteuerung von Exchange anpassen.

Aus diesem Grund sollten Administratoren genau den Zusammenhang zwischen Verwaltungsrollen, Verwaltungsrollengruppen, Zuweisungsrichtlinien und Verwaltungsbereichen verstehen. Wir gehen in diesem Kapitel grundlegend auf diese neuen Möglichkeiten ein. Sie starten die Verwaltung der rollenbasierten Berechtigung über die genannte URL oder über die Exchange-Verwaltungskonsole, indem Sie den Menüpunkt *Benutzereditor für die rollenbasierte Zugriffsteuerung* über die

Toolbox aufrufen. Eingeschränkt können Sie zwar auch ohne das Service Pack 1 bereits einige Aufgaben durchführen, zum Beispiel Benutzerkonten in Verwaltungsrollengruppen aufnehmen, aber Sie können keine neuen Verwaltungsrollengruppen erstellen oder Verwaltungsrollen zu Verwaltungsrollengruppen hinzufügen, Gruppen einschränken oder Verwaltungsrollen und Verwaltungsrollengruppen kopieren.

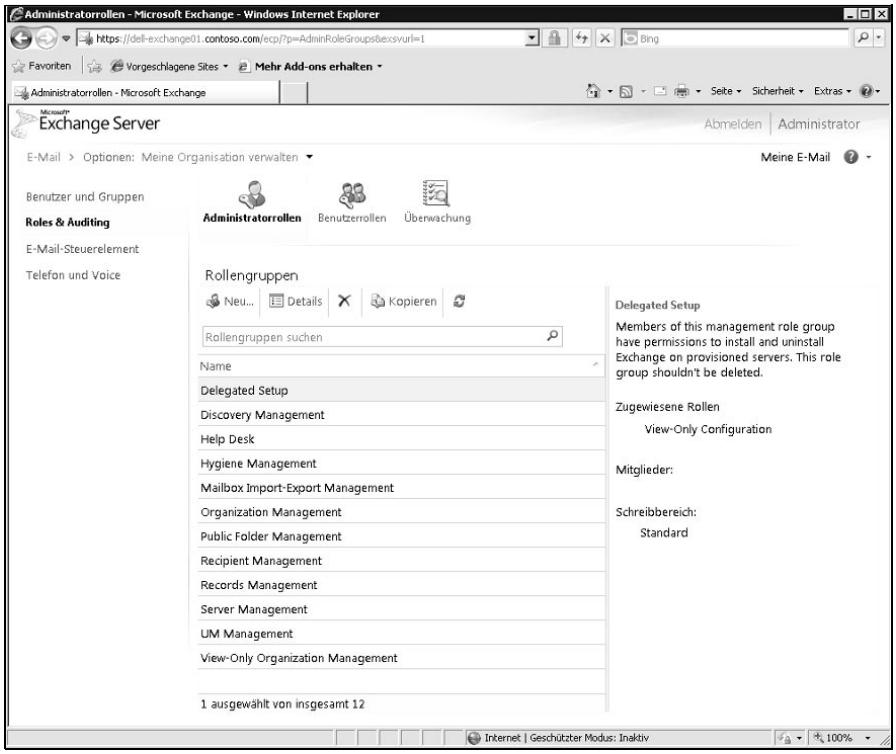


Abbildung 16.1: Die rollenbasierten Berechtigungen lassen sich mit Service Pack 1 für Exchange Server 2010 auch in der Exchange-Systemsteuerung verwalten.

16.1 Verwaltungsrollengruppen verstehen und einsetzen

Auch Administratoren, die bereits mit Exchange Server 2007 arbeiten, müssen für die Berechtigungsstruktur in Exchange Server 2010 umdenken. In Exchange Server 2010 führen Sie alle Exchange-Aufgaben über die Exchange-Verwaltungskonsole, die Exchange-Verwaltungsshell oder die Exchange-Webverwaltungsschnittstelle durch. Diese Verwaltungstools verwenden die *rollenbasierte Zugriffssteuerung* (*Role Based Access Control*, *RBAC*) zur Autorisierung. Mit RBAC müssen Sie keine Zugriffssteuerungslisten (Access Control Lists, ACLs) wie bei Exchange Server 2007 mehr pflegen. Mit RBAC können Sie sehr effizient und differenziert Rechte erteilen. In Exchange Server 2010 können Sie durch RBAC administrative Aufgaben delegieren, aber auch Rechte der Benutzer für ihr Postfach

und die Verwaltung von Verteilergruppen. Bei RBAC spielen Verwaltungsrollengruppen und Richtlinien für die Zuweisung von Verwaltungsrollen die wichtigste Rolle. Sie können auch mit der direkten Benutzerrollenzuweisung arbeiten. Lässt RBAC eine Aktion zu, führt Exchange diese Aufgabe im Kontext des *Vertrauenswürdigen Exchange-Teilsystems* (*Exchange Trusted Subsystem*) und nicht im Kontext des Benutzers durch. Das Vertrauenswürdige Exchange-Teilsystem ist eine universelle Sicherheitsgruppe mit Berechtigungen, die Lese- und Schreibzugriff auf jedes Exchange-bezogene Objekt in der Exchange-Organisation besitzt. Außerdem gehört sie zur lokalen Sicherheitsgruppe *Administratoren* und zur Gruppe *Exchange-Windows-Permissions*, die Exchange das Erstellen und Verwalten von Active Directory-Objekten ermöglicht.

16.1.1 Verwaltungsrollengruppen im Überblick

Verwaltungsrollengruppen sind universelle Sicherheitsgruppen (Universal Security Group, USG), die Sie bei der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) in Exchange Server 2010 verwenden. Rollengruppen definieren wichtige Verwaltungsaufgaben und ermöglichen den Mitgliedern verschiedene Rechte. Auf Edge-Transport-Server verwalten die lokalen Administratoren die Einstellungen. Hier steuern Sie die Berechtigung über die Mitgliedschaft der lokalen Administratorengruppe. Fügen Sie ein Postfach einer Rollengruppe als Mitglied hinzu, weist Exchange dem Postfach alle von der Verwaltungsrolle bereitgestellten Berechtigungen hinzu.

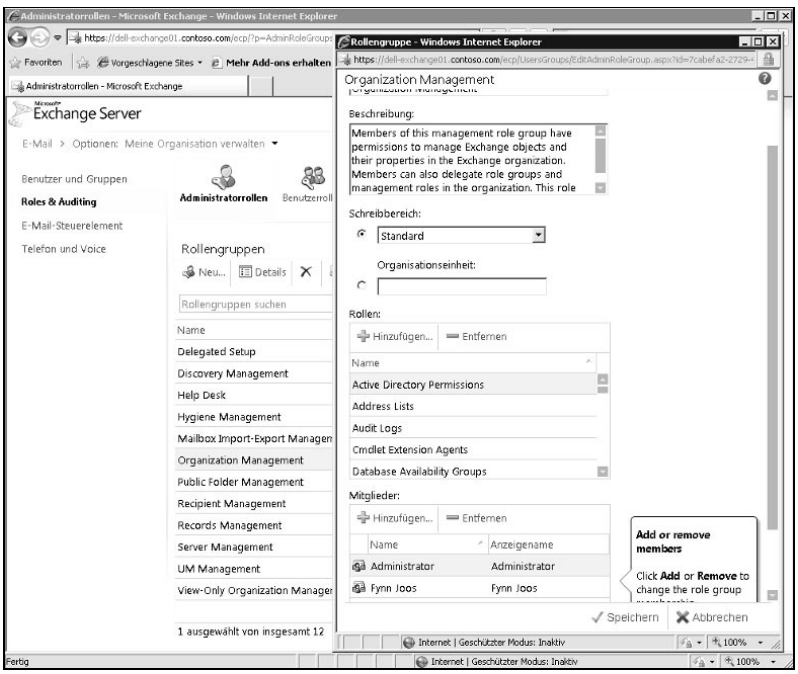


Abbildung 16.2: Durch das Hinzufügen zu Verwaltungsrollengruppen, erhalten Administratoren Rechte in der Organisation.

Eine Verwaltungsrollenzuweisung verknüpft eine Verwaltungsrolle und eine Rollengruppe. Durch das Zuweisen einer Verwaltungsrolle zu einer Rollengruppe können die Mitglieder der Rollengruppe die in der Verwaltungsrolle definierten CMDlets und Optionen verwenden, zum Beispiel beim Exportieren von Postfächern. Ein Verwaltungsrollenbereich ist der Geltungsbereich einer Rolle und schränkt ein, was Mitglieder der Rollengruppe verwalten können. Ein Bereich kann aus Servern, Organisationseinheiten oder Filtern auf Server- oder Empfängerobjekten bestehen. Das heißt, Sie vergeben Rechte nicht auf alle Objekte wie in Exchange Server 2007, sondern Sie legen genau fest, auf welchem Bereich die Rechte Gültigkeit haben. Eine Verwaltungsrolle ist eine Gruppe verschiedener Verwaltungsrolleneinträge. Mit solchen Rollen können Sie spezifische Aufgaben festlegen, die Mitglieder einer Rollengruppe ausführen dürfen.

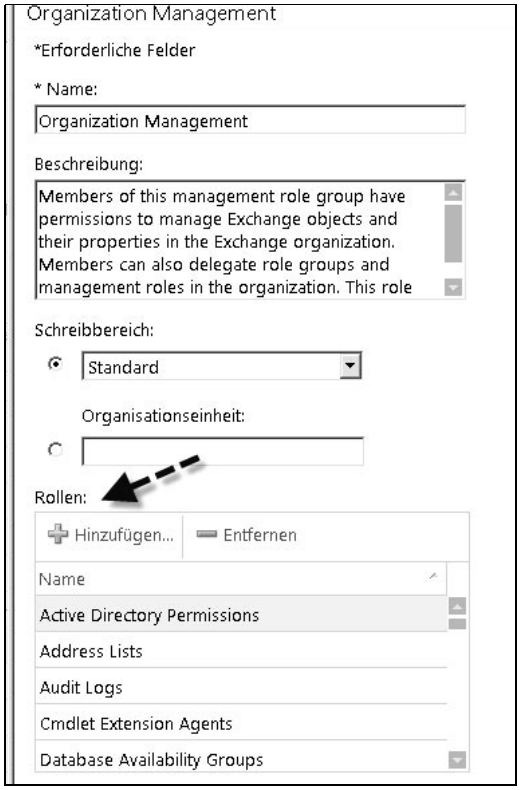


Abbildung 16.3: Die einer Verwaltungsrollengruppe zugewiesenen Verwaltungsrollen bestimmen, welche Rechte die Mitglieder der Verwaltungsrollengruppe tatsächlich haben.

Verwaltungsrolleneinträge wiederum sind die einzelnen Rechte in einer Verwaltungsrolle. Erstellen Sie eine Rollengruppe, also eine universelle Sicherheitsgruppe, legen Sie die Zuweisungen zwischen der Rollengruppe und den von Ihnen gewünschten Verwaltungsrollen fest. Sie können optional auch einen Verwaltungsbereich für die Rollenzuweisungen festlegen. Integrierte Rollengruppen sind die Rollen, die standardmäßig bereits in Exchange Server 2010 enthalten sind. Sie

finden diese Gruppen über *Active Directory-Benutzer- und -Computer* in der OU *Microsoft Exchange Security Groups*. In dieser OU finden Sie auch systemeigene Sicherheitsgruppen, die Exchange für eine stabile Infrastruktur benötigt. Sie können Benutzer allen integrierten Rollengruppen hinzufügen oder aus diesen entfernen, die Gruppen aber selbst sollten Sie nicht löschen, da Exchange ansonsten nicht mehr korrekt funktioniert. Außerdem sollten Sie die Gruppen möglichst nicht in andere OUs verschieben.

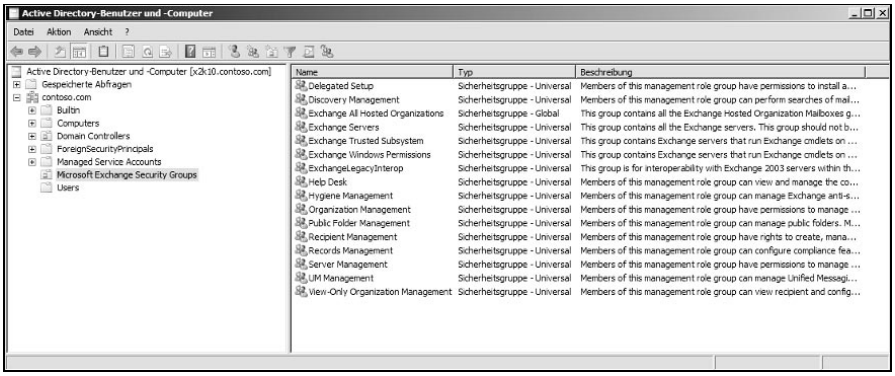


Abbildung 16.4: Verschiedene Sicherheitsgruppen in Exchange Server 2010

TIPP

In der Exchange-Verwaltungsshell können Sie sich alle Verwaltungsrollengruppen anzeigen lassen, wenn Sie den Befehl *Get-RoleGroup* eingeben. Mit dem Befehl *Get-RoleGroup |fl* erhalten Sie detaillierte Informationen. Mit dem CMDlet *Get-RoleGroupMember* und dem Namen der Gruppe als Parameter können Sie sich die aktuellen Mitglieder der Gruppe anzeigen lassen, etwa mit *Get-RoleGroupMember »Organization Management«*. Sie können sich die Verwaltungsrollengruppen auch in der Exchange-Systemsteuerung anzeigen lassen. Diese erreichen Sie über `https://<Servernama>/ecp`.

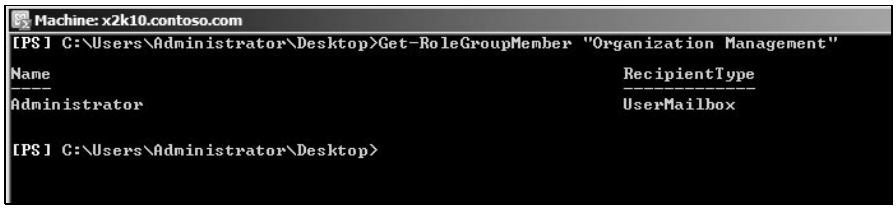
Abbildung 16.5: Anzeigen von Verwaltungsrollengruppen in der Exchange-Verwaltungsshell

Organisationsverwaltung (Organization Management)

Dieser Rollengruppe entspricht die Exchange-Rolle *Organisationsadministratoren* in Exchange Server 2007. Diese Administratoren besitzen Administratorzugriff auf die gesamte Exchange-2010-Organisation und können nahezu alle Aufgaben für alle Exchange-2010-Objekte ausführen. Mit diesem Recht ist es auch möglich, selbst Rechte in der Organisation zu vergeben. Standardmäßig darf nur die Rollengruppe

Organisationsverwaltung anderen Rollenempfängern Rollen zuweisen. Mitglied dieser Gruppe ist nur das Benutzerkonto, mit dem Sie Exchange Server 2010 installiert haben. Sie können dieser Rollengruppe weitere Benutzer hinzufügen oder andere Rollengruppen erstellen und ihnen delegierende Rollenzuweisungen zuweisen. Standardmäßig dürfen Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu Rollengruppen hinzufügen und daraus entfernen. Wollen Sie Benutzern, die keine Mitglieder der Rollengruppe *Organisationsverwaltung* sind, das Hinzufügen und Entfernen von Rollengruppenmitgliedern ermöglichen, verwenden Sie die Rollengruppendelegierung. Die Rollengruppendelegierung steuern Sie durch die Eigenschaft *ManagedBy (ManagedBy)* der jeweiligen Rollengruppe.

Abbildung 16.6: Anzeigen der Mitglieder einer Rollengruppe



Sie können dieser Rollengruppe jede Rolle hinzufügen oder entfernen. Jede Rolle muss aber mindestens eine delegierende Rollenzuweisung für eine Rollengruppe oder universale Gruppe besitzen, bevor Sie die delegierende Rollenzuweisung aus dieser Rollengruppe entfernen können. Die Rolle *Rollenverwaltung* muss mindestens eine reguläre Rollenzuweisung für eine Rollengruppe oder universale Gruppe besitzen, bevor Sie die reguläre Rollenzuweisung aus dieser Rollengruppe entfernen können. Verschiedene Rollenzuweisungen der Rollengruppe *Organisationsverwaltung* sind delegierende Rollenzuweisungen. Diese Rollen ermöglichen zum Beispiel den Zugriff auf Inhalt von Postfächern, die Erstellung von Verwaltungsrollen ohne Bereichseinschränkung. Mitglieder der Rolle *Organisationsverwaltung* erhalten standardmäßig keine Berechtigungen, die von diesen Rollen abgedeckt sind. Mitglieder können aber sich selbst jede Rolle zuweisen und auf diesem Weg die Rechte nutzen.

Organisationsverwaltung – nur Leserechte (View-Only Organization Management)

Administratoren mit diesen Rechten dürfen die Eigenschaften aller Objekte in der Exchange-Organisation lesen, aber keine Änderungen vornehmen. Diese Rolle entspricht der Exchange-Administratorrolle *Nur Ansicht* in Exchange Server 2007. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle *Überwachung*
- Rolle *Konfiguration (nur Anzeige)*
- Rolle *Empfänger mit Leserechten*

Empfängerverwaltung (Recipient Management)

Administratoren mit diesem Recht dürfen Empfänger erstellen, löschen und bearbeiten, aber keine systeminternen Einstellungen wie Connectoren bearbeiten. Diese Rollengruppe entspricht der Exchange-Rolle *Empfängeradministrator* in Exchange Server 2007. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Erstellen in Ihrer Organisation andere Administratoren Benutzerkonten, die nicht Exchange verwalten dürfen, können Sie eine Rollengruppe erstellen und die Rollen *Erstellung von E-Mail-Empfängern* und *Sicherheitsgruppenerstellung und -mitgliedschaft* in die neue Rollengruppe aufnehmen. Das verhindert, dass Mitglieder der Empfängerverwaltung-Rollengruppe Active Directory-Objekte erstellen dürfen, ermöglicht aber weiterhin, dass diese Administratoren für existierende Benutzerkonten E-Mail aktivieren dürfen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle *Verteilergruppen*
- Rolle *E-Mail-aktivierte Öffentliche Ordner*
- Rolle *Erstellung von E-Mail-Empfängern*
- Rolle *Nachrichtenempfänger*
- Rolle *Nachrichtenverfolgung*
- Rolle *Migration*
- Rolle *Postfächer verschieben*
- Rolle *Empfängerrichtlinien*

UM-Verwaltung (UM Management)

Administratoren, die Mitglied der Rollengruppe *UM-Verwaltung* sind, können die Unified-Messaging-Funktionen in der Exchange-Organisation verwalten. Dazu gehören die Servereinstellungen, aber auch die UM-Einstellungen der Empfänger. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »UM-Postfächer«
- Rolle »UM-Ansagen«
- Rolle »Unified Messaging«

Erkennungsverwaltung (Discovery Management)

Mit diesem Recht können Administratoren Suchvorgänge für Postfächer in der Exchange-Organisation ausführen. Außerdem können Mitglieder eine rechtliche Aufbewahrungspflicht für Postfächer konfigurieren (*Legal Hold*). Mitglieder der Rollengruppe *Organisationsverwaltung* müssen sich selbst als Mitglieder dieser

Rollengruppe hinzufügen. Das Recht zur Aufnahme in diese Gruppe besteht, aber die Gruppe hat noch keine Mitglieder. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »Gesetzliche Aufbewahrungspflicht«
- Rolle »Postfachsuche«

Datensatzverwaltung (Records Management)

Mit diesem Recht dürfen Benutzer Funktionen im Bereich Aufbewahrungsrichtlinientags, Nachrichtenklassifikationen und Transportregeln konfigurieren. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »Überwachungsprotokolle«
- Rolle »Journal«
- Rolle »Nachrichtenverfolgung«
- Rolle »Aufbewahrungsmanagement«
- Rolle »Transportregeln«

Serververwaltung (Server Management)

Mit diesem Recht dürfen alle Einstellungen auf dem jeweiligen Server verwaltet werden, aber keine Empfängerkonfiguration. Zu den Möglichkeiten gehören Unified-Messaging-, Clientzugriffs- und Postfachfunktionen, Datenbankkopien, Zertifikate, Transportwarteschlangen, Sendeconnectoren, virtuelle Verzeichnisse und Clientzugriffsprotokolle. Diese Rollengruppe ist ähnlich zur Gruppe *Exchange-Serveradministratoren* in Exchange Server 2007. Die Rollengruppe ermöglicht zusätzlich den Zugriff auf die Konfiguration aller Server in der Organisation, nicht nur auf einen. Wollen Sie Administratoren nur die Verwaltung bestimmter Server ermöglichen, können Sie die Verwaltungsbereiche der Rollengruppe ändern. Alternativ können Sie eine neue Rollengruppe auf der Grundlage der Rollengruppe *Serververwaltung* erstellen und die Verwaltungsbereiche für die neue Rollengruppe anpassen. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Sie können dazu einfach die Verwaltungsrollengruppe *Server Management* kopieren und die Rechte der kopierten Verwaltungsrollengruppe anpassen. Haben Sie das Service Pack 1 für Exchange Server 2010 installiert, können Sie das Kopieren in der Exchange-Systemsteuerung durchführen. Ohne das Service Pack 1 müssen Sie auf die Exchange-Verwaltungsshell zurückgreifen. Wie das geht, zeigen wir Ihnen in den folgenden Abschnitten noch genauer.

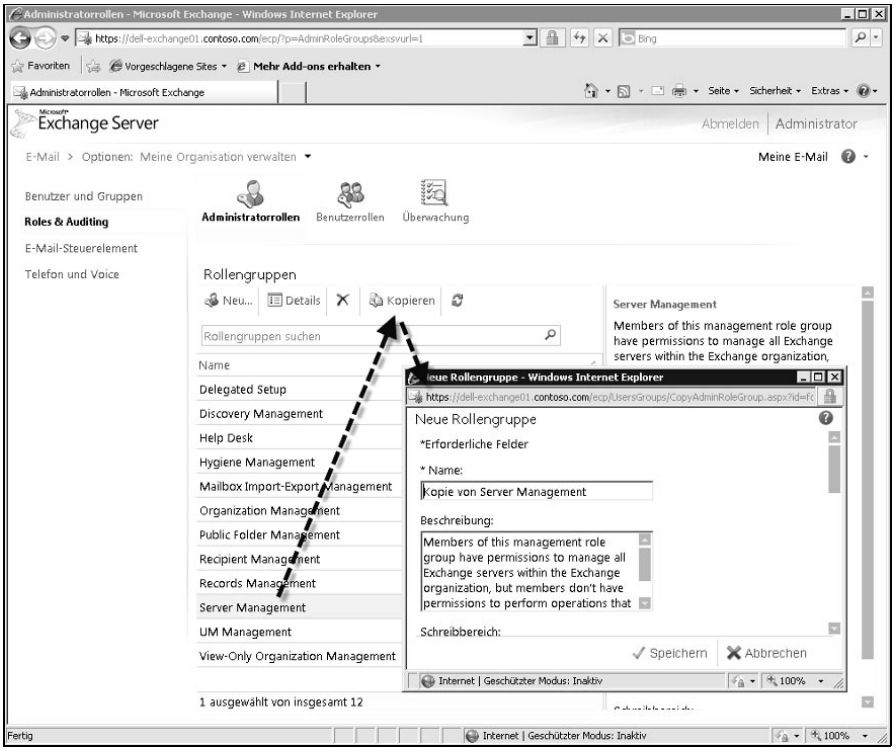


Abbildung 16.7: Kopieren einer Verwaltungsrollengruppe

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »Datenbankkopien«
- Rolle »Datenbanken«
- Rolle »Exchange-Connectors«
- Rolle »Exchange Server-Zertifikate«
- Rolle »Exchange-Server«
- Rolle »Virtuelle Exchange-Verzeichnisse«
- Rolle »Überwachung«
- Rolle »POP3- und IMAP4-Protokolle«
- Rolle »Empfangsconnector«
- Rolle »Transportwarteschlangen«

Help Desk

Mit diesem Recht dürfen Administratoren Empfänger bearbeiten, die veränderbaren Einstellungen sind dabei allerdings eingeschränkt. Die Rollengruppe ermöglicht das Anzeigen und Ändern der Outlook Web App-Optionen aller Benutzer in der Organisation, allerdings nur für die Optionen, die Anwender selbst ändern können. Kann der Held Desk auf die Exchange-Verwaltungsshell zugreifen, können Mitarbeiter alle Outlook Web App-Optionen für alle Benutzer ändern. Zu die-

sen Optionen gehören das Ändern des Anzeigenamens, der Adresse, der Telefonnummer und weitere Einstellungen des Benutzers. Optionen, die in den Outlook Web App-Optionen nicht verfügbar sind, wie zum Beispiel die Änderung der Postfachgröße oder die Konfiguration der Postfachdatenbank, lassen sich nicht verwalten. Sollen die Mitglieder der Rollengruppe Postfächer, E-Mail-Kontakte und E-Mail-aktivierte Benutzer verwalten, weisen Sie dieser die Verwaltungsrolle *E-Mail-Empfänger* zu. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »Benutzeroptionen«
- Rolle »Empfänger mit Leserechten«

Verwaltung von Nachrichtenschutz (Hygiene Management)

Mit diesem Recht dürfen Administratoren Anti-Spam-Features in Exchange verwalten. Drittanbieterprogramme können dieser Rollengruppe Dienstkonten hinzufügen, damit die entsprechenden Programme Zugriff auf die CMDlets haben, die zum Konfigurieren der Exchange-Konfiguration erforderlich sind. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »ApplicationImpersonation«
- Rolle »Empfangsconnectors«
- Rolle »Transport-Agents«
- Rolle »Transportschutz«
- Rolle »Konfiguration (nur Anzeige)«
- Rolle »Empfänger mit Leserechten«

Verwaltung Öffentlicher Ordner (Public Folder Management)

Mitglieder dieser Gruppe dürfen die öffentlichen Ordner und die Datenbanken der öffentlichen Ordner verwalten. Auch Rechte für öffentliche Ordner lassen sich mit diesem Recht bearbeiten, genauso wie neue Ordner erstellen oder Ordner löschen. Auch Grenzwerte und die E-Mail-Aktivierung steuern Sie mit diesem Recht. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »E-Mail-aktivierte Öffentliche Ordner«
- Rolle »Öffentliche Ordner«

Delegiertes Setup

Mit diesem Recht dürfen Administratoren Exchange Server 2010 auf bereitgestellten Servern installieren (siehe auch Kapitel 2). Server können durch ein Mitglied der Rollengruppe *Organisationsverwaltung* bereitgestellt werden. Mitglieder der Rollengruppe können den Server nach der Bereitstellung nicht verwalten. Zur Verwaltung muss der Administrator Mitglied der Rollengruppe *Serververwaltung* sein. Standardmäßig dürfen nur Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu dieser Rollengruppe hinzufügen oder daraus entfernen.

Dieser Rollengruppe zugewiesene Verwaltungsrollen:

- Rolle »Konfiguration (nur Anzeige)«

16.1.2 Hinzufügen, Entfernen und Anzeigen von Mitgliedern zu einer Rollengruppe

Wollen Sie einem Benutzer Berechtigungen erteilen, fügen Sie der entsprechenden Rollengruppe das Postfach des Benutzers als Mitglied hinzu. Die Rechte werden in Exchange durch Verwaltungsrollen abgebildet. Diese haben wir in einem eigenen Absatz und der Tabelle 16.1 ausführlich behandelt.

INFO

Ist ein Benutzer Mitglied mehrerer Rollengruppen, fasst Exchange die Verwaltungsrollen der einzelnen Rollengruppen zusammen und weist diese dem Benutzer zu. Mitglieder von Rollengruppen können einzelne Benutzer, universelle Sicherheitsgruppen und andere Rollengruppen sein. Nur Benutzer, die Mitglied der Rollengruppe *Organisationsverwaltung* oder *Rollenverwaltung* sind, dürfen Rollengruppenmitgliedschaften verwalten.

Verwaltungsrollen sind wiederum Verwaltungsrollengruppen zugeordnet. Die Standardgruppen in Exchange Server 2010 finden Sie am Anfang des Kapitels. Einzelne Benutzer nehmen Sie dann in die Verwaltungsrollengruppen mit auf. Einzelne Verwaltungsrollen lassen sich zwar auch direkt Benutzern zuordnen, allerdings besteht die Gefahr, dass Ihre Rechtestruktur dann schnell durcheinandergerät.

INFO

Wollen Sie Benutzer zu einer Verwaltungsrollengruppe hinzufügen, müssen Sie die Exchange-Verwaltungsshell verwenden. Sie können die rollenbasierte Berechtigung von Exchange Server 2010 nicht in der Exchange-Verwaltungskonsole anpassen. Erst wenn Sie das Service Pack 1 für Exchange Server 2010 installiert haben, können Sie über die Exchange-Systemsteuerung die Rechte entsprechend anpassen. Ohne das Service Pack 1 lassen sich in der Exchange-Systemsteuerung aber zumindest Empfänger zu Verwaltungsrollengruppen hinzufügen. Sie können aber keine weiteren Einstellungen vornehmen.

Der Befehl für die Exchange-Verwaltungsshell zur Aufnahme eines Benutzers zu einer Rollengruppe ist:

Add-RoleGroupMember <Verwaltungsrollengruppe> -Member <Benutzerpostfach>

Wollen Sie Mitglieder aus einer Verwaltungsrollengruppe entfernen, verwenden Sie den Befehl:

Remove-RoleGroupMember <Verwaltungsrollengruppe> -Member <Benutzerpostfach>

Sie können zum Hinzufügen das CMDlet *Get-User* verwenden und einen Filter einsetzen. Die Ausgabe des CMDlets können Sie dann für die Gruppenaufnahme verwenden. Das CMDlet *Add-RoleGroupMembers* akzeptiert standardmäßig nicht die Ausgabe von *Get-User*. Sie müssen die Daten über eine *ForEach*-Anweisung übergeben. Die Vorgehensweise dabei ist folgende:

1. Sie filtern mit *Get-User* und der Option *Filter* die Postfächer, die Sie zur Verwaltungsrollengruppe aufnehmen wollen, und speichern die Ausgabe in einer Variable: *$Mailboxes = Get-User -Filter { RecipientType -Eq »UserMailbox« -and <Festgelegter Filter> }*. In der Tabelle 16.3 finden Sie entsprechende Operatoren zu Filtern. Alle Kriterien von Postfächern können Sie sich mit dem Befehl *get-user |fl* anzeigen lassen und diese in den Filter einbauen.
2. Mit dem Befehl *$Mailboxes* zeigen Sie die gefilterten Postfächer an.

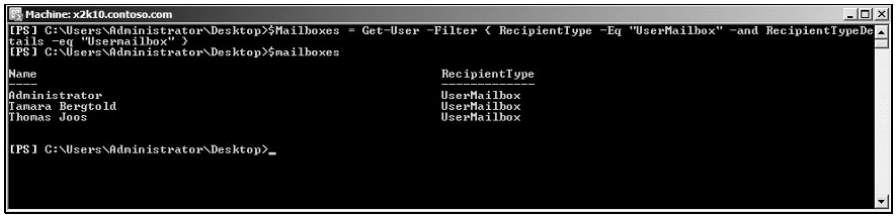


Abbildung 16.8: Erstellen eines Filters für die Anzeige von Postfächern und Anzeige des Variableninhalts

3. Sie übergeben den Inhalt der Variablen *$Mailbox* an das CMDlet *Add-RoleGroupMember* über eine *ForEach*-Anweisung: *$Mailboxes | ForEach { Add-RoleGroupMember <Verwaltungsrollengruppe> -Member $_.Name }*

Beispiel:

$Mailboxes = Get-User -Filter { RecipientType -Eq »UserMailbox« -and Department -Eq »IT-Abteilung Exchange« }

$Mailboxes | ForEach { Add-RoleGroupMember »Organization Management« -Member $_.Name }

```
Machine: x2k10.contoso.com
[PS] C:\Users\Administrator\Desktop>Get-RoleGroupMember "Organization Management"

Name                                                    RecipientType
----                                                    -------------
Administrator                                           UserMailbox
Tamara Bergtold                                         UserMailbox
Thomas Joos                                             UserMailbox

[PS] C:\Users\Administrator\Desktop>_
```

Abbildung 16.9: Anzeigen der Mitglieder einer Rollengruppe

INFO

Standardmäßig zeigt die Exchange-Verwaltungsshell maximal 1.000 Rollengruppenmitglieder an. Wollen Sie mehr Mitglieder anzeigen, verwenden Sie die Option *ResultSize* des CMDlet *Get-RoleGroupMember.* Sie können entweder einen Wert oder *unlimited* eingeben. Geben Sie *unlimited* ein, zeigt die Shell alle Mitglieder der Rollengruppe an.

In der Exchange-Systemsteuerung können Sie Empfänger über die *Details* einer Verwaltungsrollengruppe hinzufügen oder entfernen.

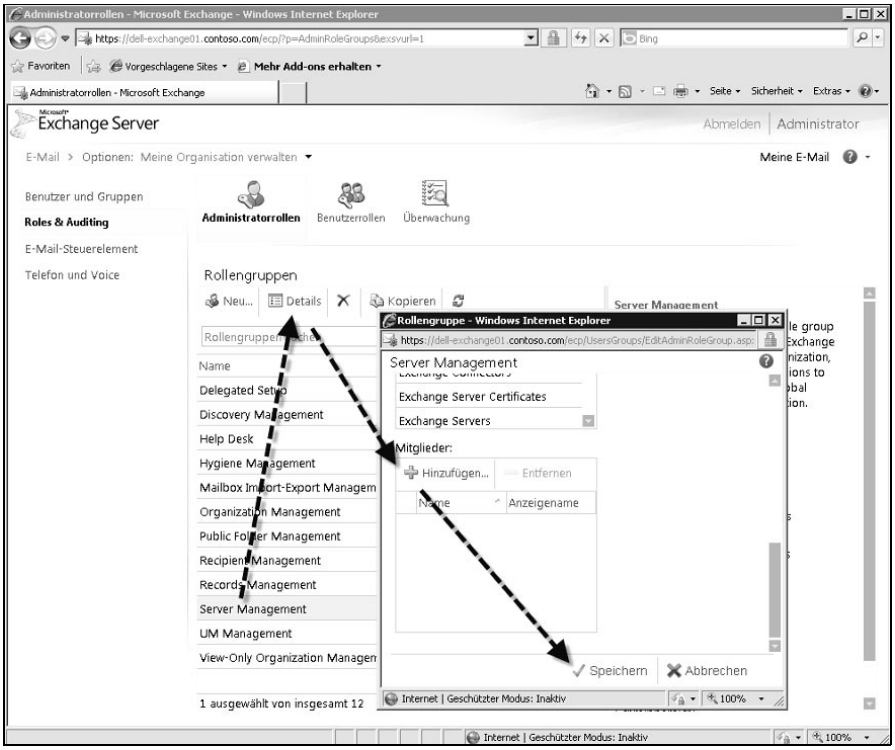


Abbildung 16.10: Hinzufügen von Empfängern zu Verwaltungsrollengruppen

16.1.3 Rollengruppenstellvertreter hinzufügen und entfernen

Stellvertreter von Verwaltungsrollengruppen können Mitglieder zu Verwaltungsrollengruppen hinzufügen oder aus ihnen entfernen und Eigenschaften einer Rollengruppe anpassen. Standardmäßig dürfen Mitglieder der Rollengruppe *Organisationsverwaltung* Mitglieder zu Rollengruppen hinzufügen und daraus entfernen. Wollen Sie Benutzern, die keine Mitglieder der Rollengruppe *Organisationsverwaltung* sind, das Hinzufügen und Entfernen von Rollengruppenmitgliedern ermöglichen, verwenden Sie die Rollengruppendelegierung. Diese steuern Sie durch die Eigenschaft *ManagedBy* der jeweiligen Rollengruppe. Die Benutzer auf dieser Registerkarte haben keine von der Rollengruppe erteilten Berechtigungen, sondern dürfen die Gruppe nur verwalten. Haben Sie einem Benutzer die Verwaltungsrolle *Rollenverwaltung* zugewiesen, ohne dass dieser Stellvertreter der Rollengruppe ist, muss er bei den CMDlets *Add-RoleGroupMember*, *Remove-RoleGroupMember*, *Update-RoleGroupMember* und *Set-RoleGroup* die Option *BypassSecurityGroupManagerCheck* verwenden, um die Rollengruppe verwalten zu dürfen. Die Konfiguration des Stellvertreters erfolgt durch die Option *ManagedBy* für die CMDlets *Set-RoleGroup* oder *New-RoleGroup*. Sollen die Benutzer auch die Rechte der Gruppe erhalten, müssen diese Mitglieder sein.

Mit delegierenden Rollenzuweisungen können Mitglieder diese Rolle einer anderen Rollengruppe, Zuweisungsrichtlinie oder universellen Sicherheitsgruppe zuweisen. Mitglieder der Rollengruppe können nur die Rolle zuweisen und nicht die Rollengruppe selbst delegieren. Das funktioniert nur, wenn die Rollengruppe als *ManagedBy* festgelegt ist.

INFO

Die Option *ManagedBy* für das CMDlet *Set-RoleGroup* überschreibt die gesamte Stellvertreterliste für eine Rollengruppe.

Wollen Sie einzelne Stellvertreter zu einer Rollengruppe hinzufügen, ohne die gesamte Stellvertreterliste zu löschen, gehen Sie folgendermaßen vor:

1. Sie speichern die Rollengruppe mit einem Befehl in eine Variable: *$RoleGroup = Get-RoleGroup <Verwaltungsrollengruppe>*
2. Sie fügen den Stellvertreter zu der Rollengruppe hinzu, die Sie als Variable gespeichert haben: *$RoleGroup.ManagedBy += (Get-User <Postfach das Sie hinzufügen wollen>).Identity*. Wollen Sie eine universelle Gruppe hinzufügen, verwenden Sie das CMDlet *Get-Group*.
3. Wiederholen Sie Schritt 2 für jeden Stellvertreter, den Sie hinzufügen wollen.
4. Die Liste in der Variablen müssen Sie noch in die echte Verwaltungsrollengruppe hinzufügen: *Set-RoleGroup <Verwaltungsrollengruppe> -ManagedBy $RoleGroup.ManagedBy*

In diesem Beispiel wollen Sie den Benutzer Thomas Joos als Stellvertreter der Rollengruppe *Organisationsverwaltung* hinzufügen:

$RoleGroup = Get-RoleGroup »Organization Management«

$RoleGroup.ManagedBy += (Get-User »Thomas Joos«).Identity

Set-RoleGroup »Organization Management« -ManagedBy $RoleGroup.ManagedBy

Um ein Mitglied von der Stellvertreterliste einer Verwaltungsrollengruppe zu entfernen, gehen Sie folgendermaßen vor:

1. Sie speichern die Rollengruppe mit einem Befehl in eine Variable: *$RoleGroup = Get-RoleGroup < Verwaltungsrollengruppe >*
2. Sie entfernen den Stellvertreter aus der Rollengruppe, die Sie als Variable gespeichert haben: *$RoleGroup.ManagedBy -= (Get-User < Benutzer den Sie entfernen wollen >).Identity*. Wollen Sie eine universelle Gruppe entfernen, verwenden Sie das CMDlet *Get-Group*.
3. Wiederholen Sie Schritt 2 für jeden Stellvertreter, den Sie entfernen wollen.
4. Die Liste in der Variablen müssen Sie noch in die echte Verwaltungsrollengruppe hinzufügen: *Set-RoleGroup < Verwaltungsrollengruppe > -ManagedBy $RoleGroup.ManagedBy*

In diesem Beispiel wollen Sie den Benutzer Thomas Joos als Stellvertreter von der Rollengruppe *Organisationsverwaltung* entfernen:

$RoleGroup = Get-RoleGroup »Organization Management«

$RoleGroup.ManagedBy -= (Get-User »Thomas Joos«).Identity

Set-RoleGroup »Organization Management« -ManagedBy $RoleGroup.ManagedBy

16.1.4 Verwaltungsrollengruppen erstellen und löschen

Neben den Standardgruppen können Sie auch selbst Verwaltungsrollengruppen erstellen und diesen Benutzer zuordnen. Jeder Verwaltungsrollengruppe müssen Sie natürlich auch Verwaltungsrollen zuweisen. Im folgenden Abschnitt gehen wir im Rahmen eines Beispiels auf die Vorgänge bei der Erstellung einer Rollengruppe ein. Neue Verwaltungsrollengruppen erstellen Sie mit dem CMDlet *New-RoleGroup.*

Beispiel:

New-RoleGroup -Name »Contoso Recipient Management« -Roles »Mail Recipients«, »Distribution Groups«, »Move Mailboxes«, »UM Mailboxes«, »Reset Password« -CustomRecipientWriteScope »Contoso Users«, -ManagedBy »Thomas«, »Tami«, »Fynn« -Members »Stefan«, »Marc«, »Marco«, »Hans«, »Michael«, »Lukas«, »Flo«, »Lukas«, »Isabel«, »Manuela«, »Thomas«, »Karl«

Der Befehl führt Folgendes aus:

- Exchange erstellt eine neue Rollengruppe mit der Bezeichnung *Contoso Recipient Management*.
- Sie fügen die Postfächer der Benutzer Stefan, Marc, Marco, Hans, Michael, Lukas, Flo, Lukas, Isabel, Manuela, Thomas und Karl als Mitglieder der Rollengruppe hinzu. Diese Benutzer erhalten die von dieser Rollengruppe bereitgestellten Berechtigungen.
- Sie fügen die Benutzer Thomas, Tami und Fynn der Eigenschaft *ManagedBy* der Rollengruppe hinzu. Diese Benutzer dürfen Mitglieder zur Rollengruppe hinzufügen und daraus entfernen, damit erhalten diese jedoch keinerlei von der Rollengruppe bereitgestellten Berechtigungen, wenn sie keine Mitglieder sind. Da Thomas auch ein Mitglied der Rollengruppe ist, darf er Mitglieder zur Rollengruppe hinzufügen und daraus entfernen und erhält darüber hinaus die von der Rollengruppe bereitgestellten Berechtigungen.
- Sie erstellen verschiedene Verwaltungsrollenzuweisungen und weisen der Rollengruppe jede im Befehl angegebene Verwaltungsrolle zu.
- Sie fügen den Verwaltungsbereich »Contoso Users« zu jeder Rollenzuweisung hinzu (zu den Bereichen kommen wie in Abschnitt 16.3). Verwaltungsbereiche legen fest, welche Objekte in der Exchange-Organisation die Mitglieder der Verwaltungsrollengruppe verwalten dürfen. Auf diese Weise können Sie bestimmte Rechte zum Beispiel auf Basis von Organisationseinheiten festlegen. Der Name der einzelnen Rollenzuweisungen besteht aus einer Kombination der zugewiesenen Verwaltungsrolle und des Rollengruppennamens.

Sie können Verwaltungsrollengruppen auch mit benutzerdefinierten Empfängerbereichen oder benutzerdefinierten Konfigurationsverwaltungsbereichen erstellen:

New-RoleGroup -Name <Verwaltungsrollengruppe> -Roles <Verwaltungsrollen, die Sie zuweisen wollen> -CustomRecipientWriteScope <Empfängerbereich> -CustomConfigWriteScope <Konfigurationsbereich>

Sie können Verwaltungsrollengruppen auch erstellen, deren Bereich auf eine bestimmte Organisationseinheit festgelegt ist:

New-RoleGroup -Name <Verwaltungsrollengruppe> -Roles <Verwaltungsrollen, die Sie zuweisen wollen> -RecipientOrganizationalUnitScope <Name der OU>.

Beispiel:

In diesem Beispiel erstellen Sie eine Verwaltungsrollengruppe, welche die Verwaltung von Empfängern in der Organisationseinheit »Berlin« zulässt.

New-RoleGroup -Name »Berlin-Empfänger-Verwaltung« -Roles »Mail Recipients« -RecipientOrganizationalUnitScope »Berlin«

Wollen Sie eine Verwaltungsrollengruppe löschen, verwenden Sie das CMDlet *Remove-RoleGroup <Verwaltungsrollengruppe>*

TIPP

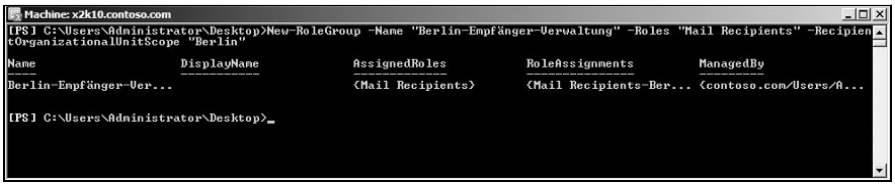


Abbildung 16.11: Erstellen einer neuen Verwaltungsrollengruppe

Haben Sie das Service Pack 1 für Exchange Server 2010 installiert, können Sie neue Verwaltungsrollengruppen auch in der Exchange-Systemsteuerung erstellen. Klicken Sie dazu einfach auf *Neu*, wenn Sie in der Verwaltung der Administratorrollen sind.

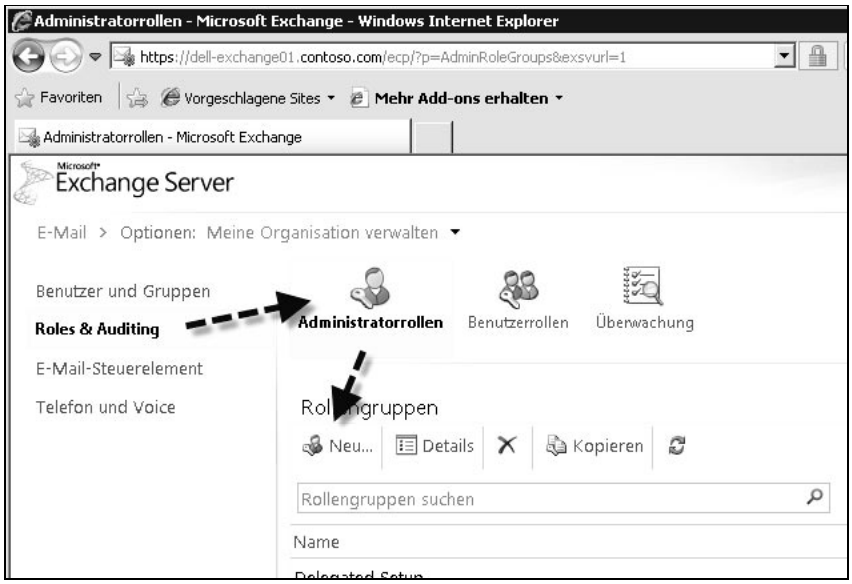


Abbildung 16.12: Erstellen einer neuen Verwaltungsrollengruppe

Im neuen Fenster können Sie dann einen Namen für die neue Verwaltungsrollengruppe, eine Beschreibung und den Bereich, in dem Mitglieder Änderungen vornehmen dürfen, eingeben. Außerdem nehmen Sie über das Fenster Verwaltungsrollen auf und Mitglieder, die der Verwaltungsrollengruppe zugewiesen sind.

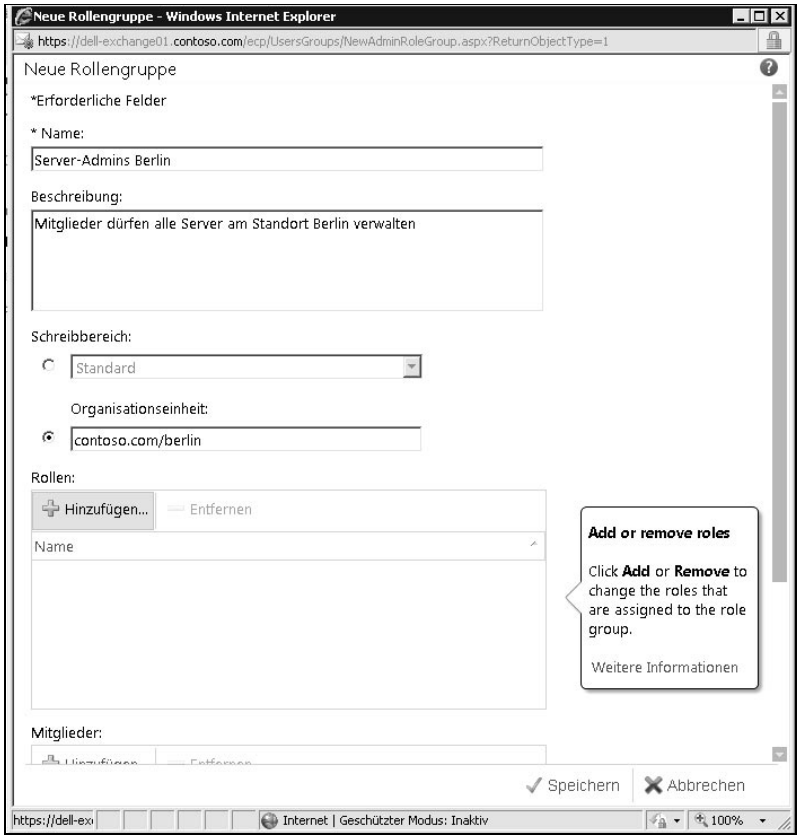


Abbildung 16.13: Erstellen einer neuen Verwaltungsrollengruppe

16.2 Verwaltungsrollen verstehen

Rollen sind eine Gruppe von CMDlets, die das Verwalten verschiedener Exchange-Aufgaben ermöglichen. Verwaltungsrollen können Sie zu Verwaltungsrollengruppen und Zuweisungsrichtlinien für Verwaltungsrollen zusammenfügen. Rollengruppen und Rollenzuweisungsrichtlinien weisen Administratoren und Benutzern Berechtigungen zu. Sie müssen Verwaltungsrollen zuweisen, damit sie wirksam werden. Sie können die Rollen beliebig kombinieren. Meistens weisen Sie Rollen Rollengruppen oder Rollenzuweisungsrichtlinien zu. Sie können Empfängern Verwaltungsrollen auch direkt zuweisen, allerdings ist das nicht empfohlen, da die Berechtigungsstruktur dann schnell unübersichtlich wird. Rollenzuweisungsrichtlinien können Sie aber nur den Endbenutzerverwaltungsrollen zuweisen. Integrierte Verwaltungsrollen können Sie nicht ändern, aber Sie können Verwaltungsrollen auf Grundlage von integrierten Verwaltungsrollen erstellen und diese dann Rollengruppen oder Rollenzuweisungsrichtlinien zuweisen. Erstellen Sie eine neue benutzerdefinierte Verwaltungsrolle, erbt die neue untergeordnete Rolle

alle Verwaltungsrolleneinträge der übergeordneten Rolle. Sie können nur Verwaltungsrolleneinträge in der neuen untergeordneten Rolle verwenden, die auch in der übergeordneten Rolle enthalten sind.

16.2.1 Verwaltungsrollen im Überblick

Mit den standardmäßigen Verwaltungsrollen, die den bereits besprochenen Verwaltungsrollengruppen zugeordnet sind, legen Sie fest, welche Rechte die einzelnen Administratoren haben. Benutzerkonten, die Sie zu einer Verwaltungsrollengruppe hinzufügen, erhalten die Rechte, die in den Verwaltungsrollen hinterlegt sind, welche Bestandteile der Verwaltungsrollengruppen sind. Im vorangegangenen Abschnitt haben wir Ihnen gezeigt, welche Verwaltungsrollengruppen es in Exchange Server 2010 gibt und welche Verwaltungsrollen den einzelnen Verwaltungsrollengruppen zugewiesen sind. Um Berechtigungen für eine Rolle zu erteilen, müssen Sie diese einem Rollenempfänger zuweisen. Dabei kann es sich um eine Rollengruppe (siehe vorangegangener Abschnitt), einen Benutzer oder eine universelle Sicherheitsgruppe handeln. Die Zuweisung erfolgt über Verwaltungsrollenzuweisungen. Sie können Verwaltungsrollen über die Exchange-Verwaltungsshell zu Verwaltungsrollengruppen hinzufügen (zuweisen) oder nach der Installation von Service Pack 1 für Exchange Server 2010 über die Exchange-Systemsteuerung über die Details einer Verwaltungsrollengruppe. Rollenzuweisungen verbinden Rollenempfänger und Verwaltungsrollen miteinander. Benutzer können auch mehrere Verwaltungsrollen erhalten. In der folgenden Tabelle gehen wir auf die Verwaltungsrollen ein, die Sie zu Gruppen zusammenfassen können.

Bei Verwaltungsrollen gibt es die beiden Rechte *regulär* und *delegierend*. Weisen Sie eine Verwaltungsrolle regulär einem Rollenempfänger zu, hat dieser das Recht, die Rolle und damit verbundene CMDlets zu nutzen. Der Rollenempfänger darf aber keinerlei andere Rollenempfänger berechtigen. Weisen Sie einem Rollenempfänger ein delegierendes Recht der Verwaltungsrolle zu, darf der Empfänger nicht die CMDlets nutzen, aber dafür Rechte der Rolle verwalten.

INFO

Zum besseren Verständnis zeigen wir Ihnen in der folgenden Tabelle die einzelnen Verwaltungsrollen mit der deutschen Übersetzung. Wollen Sie die Rollen verwalten, müssen Sie in der Exchange-Verwaltungsshell die englischen Begriffe verwenden, die Sie sich in der Exchange-Verwaltungsshell und in der Exchange-Systemsteuerung anzeigen lassen können. In der Exchange-Systemsteuerung erhalten Sie nach Installation von Service Pack 1 für Exchange Server 2010 eine ausführliche Hilfe zu den einzelnen Verwaltungsrollen. In der Tabelle 16.2 finden Sie die englischen Bezeichnungen, noch mal eine kleine Beschreibung und den Geltungsbereich der Verwaltungsrolle.

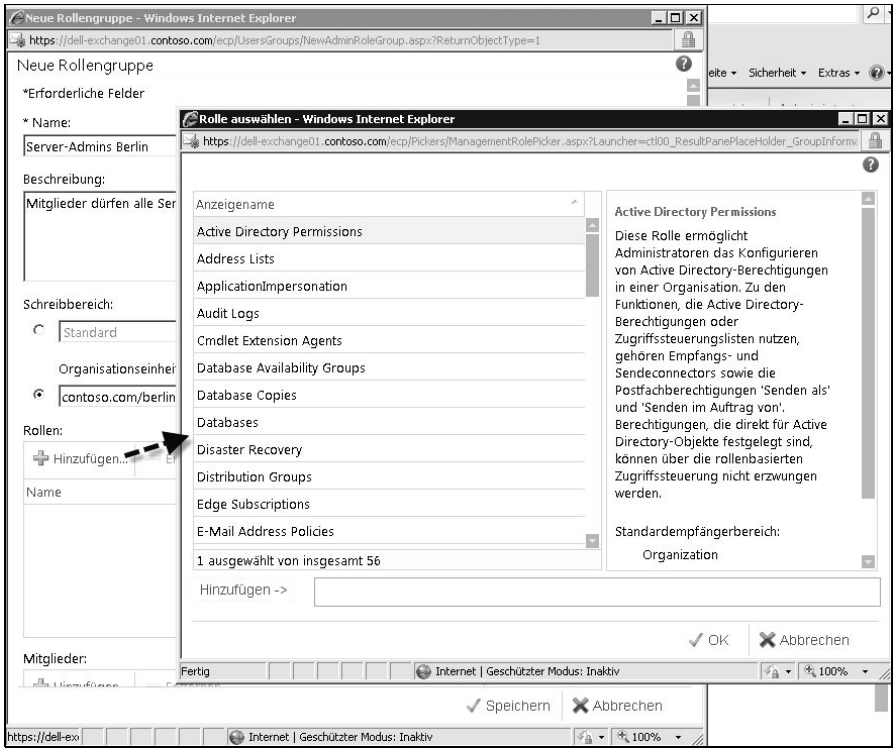


Abbildung 16.14: Hinzufügen von Verwaltungsrollen zu Verwaltungsrollengruppen

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010

Verwaltungsrolle	Aufgaben
Active Directory-Berechtigungen	Mitglieder dürfen Active Directory-Berechtigungen in einer Organisation konfigurieren. Beispiele sind Empfangs- und Sendeconnectoren (siehe Kapitel 5) sowie die Berechtigungen *Senden als* und *Senden im Auftrag von* für Postfächer (siehe Kapitel 9). Mitglieder anzeigen: *Get-ManagementRoleAssignment -Role »Active Directory Permissions«* Standardmitglieder: *Organisationsverwaltung*
Adresslisten	Die Verwaltungsrolle ermöglicht das Erstellen, Ändern, Anzeigen und Entfernen von Adresslisten, globalen Adresslisten und Offline-Adresslisten in einer Organisation (siehe Kapitel 9). Standardmitglieder: *Organisationsverwaltung*
ApplicationImpersonation	Die Verwaltungsrolle ermöglicht das Annehmen der Identität anderer Benutzer in einer Organisation, um im Namen dieser Benutzer Aufgaben auszuführen. Standardmitglieder: *Verwaltung von Nachrichtenschutz, Organisationsverwaltung*
Überwachungsprotokolle	Mit der Verwaltungsrolle können Administratoren das Überwachungsprotoll der Server konfigurieren (siehe Kapitel 18). Standardmitglieder: *Organisationsverwaltung*, *Datensatzverwaltung*

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010 (Forts.)

Verwaltungsrolle	Aufgaben
CMDlet-Erweiterungs-Agents	Die Verwaltungsrolle ermöglicht Administratoren das Aktivieren, Deaktivieren und Festlegen der Priorität von CMDlet-Erweiterungs-Agents. Diese benötigen Exchange-2010-CMDlets. Die Agents erweitern die Funktionen der CMDlets. Zum Beispiel akzeptiert das CMDlet *New-Mailbox* die Option *Database*, mit dem Sie die Postfachdatenbank angeben, in der Sie das neue Postfach erstellen wollen. In Exchange Server 2007 schlägt der Befehl fehl, wenn Sie bei *New-Mailbox* nicht die Datenbank angeben. In Exchange Server 2010 ruft das CMDlet *New-Mailbox* bei seiner Ausführung den Mailbox Resources Management-Agent auf. Geben Sie die Option *Database* nicht an, bestimmt der Agent automatisch eine geeignete Postfachdatenbank und ergänzt den Befehl automatisch. CMDlet-Erweiterungs-Agents funktionieren nur mit Exchange-2010-CMDlets. Standardmitglieder: *Organisationsverwaltung*
Datenbankverfügbarkeits-gruppe	Mit dieser Rollengruppe dürfen Administratoren Datenbankverfügbarkeitsgruppen verwalten (siehe Kapitel 23). Standardmitglieder: *Organisationsverwaltung*
Datenbankkopien	Hinzufügen, Entfernen, Anhalten, Fortsetzen, Anzeigen und Aktualisieren von Datenbankkopien auf einzelnen Servern, die zu einer Hochverfügbarkeitsgruppe gehören (siehe Kapitel 23) Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Datenbanken	Erstellen, Verwalten und Bereitstellen von Postfach- und Öffentliche-Ordner-Datenbanken auf Servern (siehe Kapitel 7) Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Wiederherstellung nach Datenverlust	Wiederherstellen von Postfächern und Datenbankverfügbarkeitsgruppen, Erstellen von Postfachdatenbanken und das Starten und Beenden von Datenbankverfügbarkeitsgruppen (siehe Kapitel 17 und 23) Standardmitglieder: *Organisationsverwaltung*
Verteilergruppen	Erstellen, Ändern, Anzeigen und Entfernen von Verteilergruppen sowie das Hinzufügen oder Entfernen von Mitgliedern in Verteilergruppen (siehe Kapitel 9) Standardmitglieder: *Organisationsverwaltung* und *Empfängerverwaltung*
Edge-Abonnements	Verwalten der Edge-Synchronisierung und Abonnementkonfiguration zwischen Edge-Transport- und Hub-Transport-Servern (siehe Kapitel 12 und 13) Standardmitglieder: *Organisationsverwaltung*
E-Mail-Adressrichtlinien	Verwalten von E-Mail-Adressrichtlinien (siehe Kapitel 9) Standardmitglieder: *Organisationsverwaltung*
Exchange-Connectors	Erstellen, Ändern, Anzeigen und Entfernen von Routinggruppenconnectoren und Zustellungs-Agent-Connectoren. Diese Agents benötigt Exchange beim Zustellen von E-Mails an Fremdsysteme, die kein SMTP verwenden. Jeder Zustellungs-Agent verfügt über einen eigenen Zustellungs-Agent-Connector. Mit dieser Rolle können Sie keine Sende- und Empfangsconnectoren verwalten. Dazu verwenden Sie die Rollen *Sendeconnectors* und *Empfangsconnectors*. Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010 (Forts.)

Verwaltungsrolle	Aufgaben
Exchange-Server-Zertifikate	Erstellen, Importieren, Exportieren und Verwalten von Exchange-Serverzertifikaten auf einzelnen Servern (siehe Kapitel 2 und 4) Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Exchange-Server	Ermöglicht verschiedene Verwaltungsaufgaben auf einzelnen Exchange-Servern: – Hinzufügen und Entfernen von Datenbankverfügbarkeitsgruppen – Aktivieren und Deaktivieren von Unified-Messaging-Servern – Aktivieren und Deaktivieren von Outlook Anywhere auf Clientzugriffsservern – Ändern der Postfach-, Hub-Transport-, Clientzugriffs- und Unified-Messaging-Serverkonfiguration – Ändern der Outlook-Anywhere-Konfiguration auf Clientzugriffsservern – Ändern der Konfiguration für Inhaltsfilter auf Hub-Transport-Servern – Ändern der allgemeinen Exchange-Serverkonfiguration – Anzeigen der Konfiguration für jede einzelne Serverrolle Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Virtuelle Exchange-Verzeichnisse	Verwalten der virtuellen Verzeichnisse für Outlook Web App, Exchange ActiveSync, Offlineadressbücher, AutoDiscovery und PowerShell (siehe Kapitel 11 und 22) Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Verbundfreigabe	Verbundfreigaben zwischen Organisationen verwalten. Mit Verbundfreigaben können Benutzer Kontakte und die Frei/Gebucht-Zeiten der Kalender auch zwischen verschiedenen Exchange-Organisationen freigeben. Dazu müssen Administratoren die Freigabe aber erst durch die Verbindung der Exchange-Organisationen einrichten (siehe Kapitel 24). Standardmitglieder: *Organisationsverwaltung*
Verwaltung von Informationsrechten	Verwalten von Informationsrechten innerhalb einer Organisation. Mit der Verwaltung von *Informationsrechten* (*IRM*) lassen sich E-Mails und Anlagen schützen. Dazu verwendet IRM die *Active Directory-Rechteverwaltungsdienste* (*AD RMS*). Benutzer können festlegen, welche Rechte die Empfänger von E-Mails haben. Mit IRM lassen sich Aktionen der Empfänger wie Weiterleiten oder Drucken einschränken. IRM-Schutz steht in Outlook 2010 und Outlook Web App zur Verfügung (siehe Kapitel 25). Standardmitglieder: *Organisationsverwaltung*
Journal	Erstellen, Ändern, Aktivieren, Deaktivieren, Anzeigen und Entfernen von Journalregeln (siehe Kapitel 5) Standardmitglieder: *Organisationsverwaltung* und *Datensatzverwaltung*
Gesetzliche Aufbewahrungspflicht	Konfigurieren von Legal Hold für Postfächer (siehe Kapitel 10) Standardmitglieder: *Organisationsverwaltung* und *Erkennungsverwaltung*
E-Mail-aktivierte öffentliche Ordner	Erlaubt die E-Mail-Aktivierung, oder Deaktivierung von öffentlichen Ordnern (siehe Kapitel 8). Andere Eigenschaften lassen sich nur verwalten, wenn noch die Rolle *Öffentliche Ordner* zugewiesen ist. Standardmitglieder: *Organisationsverwaltung, Verwaltung öffentlicher Ordner* und *Empfängerverwaltung.*

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010 (Forts.)

Verwaltungsrolle	Aufgaben
Erstellung von E-Mail-Empfängern	Erstellen von Postfächern, E-Mail-Benutzern, E-Mail-Kontakten und Verteilergruppen Standardmitglieder: *Organisationsverwaltung* und *Empfängerverwaltung*
Nachrichtenempfänger	Verwalten vorhandener Postfächer, E-Mail-Benutzer und E-Mail-Kontakte. Wollen Sie neue Empfänger erstellen, ist noch die Rolle *Erstellung von E-Mail-Empfängern* notwendig. Standardmitglieder: *Organisationsverwaltung* und *Empfängerverwaltung*
E-Mail-Infos	E-Mail-Infos sind Meldungen, die Benutzer beim Erstellen von E-Mails erhalten. Erkennt Exchange ein Problem, erscheint in Outlook 2010 eine Meldung in der Kopfzeile der E-Mail. Dazu gehören Meldungen, wenn Absender eine E-Mail an sehr viele Empfänger auf einmal senden, die Nachricht und Anlagen sehr groß sind oder Empfänger einer E-Mail den Abwesenheitsassistenten aktiviert haben. Standardmitglieder: *Organisationsverwaltung*
Postfachimport/-export	Importieren und Exportieren von Postfachinhalten sowie das Entfernen unerwünschter Inhalte aus einem Postfach. Mehr zu diesem Ablauf finden Sie in Kapitel 7. Standardmitglieder: *Organisationsverwaltung* (aber nur delegierend, also mit der Möglichkeit, sich selbst die Rechte zu geben)
Postfachsuche	Durchsuchen des Inhalts eines oder mehrerer Postfächer in einer Organisation Standardmitglieder: *Organisationsverwaltung* und *Erkennungsverwaltung*
Nachrichtenverfolgung	Ermöglicht das Nachverfolgen von E-Mails in der Organisation (siehe Kapitel 5) Standardmitglieder: *Organisationsverwaltung, Empfängerverwaltung* und *Datensatzverwaltung*
Migration	Postfächer zwischen Exchange-Server verschieben (siehe auch Kapitel 4 und 9). Wollen Sie Postfächer zwischen Servern in verschiedenen Organisationen verschieben, ist noch die Rolle *Postfächer verschieben* notwendig. Standardmitglieder: *Organisationsverwaltung* und *Empfängerverwaltung*
Überwachung	Ermöglicht das Überwachen der Exchange-Dienste und Exchange-Komponenten auf den Servern. Diese Rolle benötigen oft auch Anwendungen zur Serverüberwachung zum Erfassen von Zustandsinformationen für Exchange-Server. Standardmitglieder: *Organisationsverwaltung, Organisationsverwaltung – Nur Leserechte* und *Serververwaltung*
Postfächer verschieben	Verschieben von Postfächern zwischen Servern einer Organisation und zwischen Servern von verschiedenen Organisationen Standardmitglieder: *Organisationsverwaltung* und *Empfängerverwaltung*
MyBaseOptions	Ermöglicht Benutzern das Anpassen ihres eigenen Postfachs und verschiedener Einstellungen im eigenen Postfach. Standardmitglieder: *Standard-Rollenzuweisungsrichtlinie*
MyContactInformation	Einzelne Benutzer dürfen ihre eigenen Kontaktinformationen ändern, zum Beispiel Adresse und Telefonnummern. Standardmitglieder: *Standard-Rollenzuweisungsrichtlinie*

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010 (Forts.)

Verwaltungsrolle	Aufgaben
MyDiagnostics	Diagnose eigener Postfachfunktionen wie die Kalenderdiagnose Standardmitglieder: *Organisationsverwaltung* (nur delegierend)
MyDistributionGroup Membership	Berechtigt einzelne Benutzer, ihre Mitgliedschaften in Verteilergruppen anzuzeigen und zu bearbeiten, entsprechende Konfigurationen der Verteilergruppe vorausgesetzt (siehe Kapitel 9). Standardmitglieder: *Standard-Rollenzuweisungsrichtlinie*
MyDistributionGroups	Verteilergruppen erstellen, ändern und anzeigen sowie Mitglieder ändern, anzeigen, entfernen und hinzufügen, wenn die Verteilergruppe entsprechend konfiguriert ist (siehe Kapitel 9) Standardmitglieder: *Organisationsverwaltung (nur delegierend)*
MyProfileInformation	Ändern des eigenen Namens Standardmitglieder: *Organisationsverwaltung (nur delegierend)*
MyRetentionPolicies	Aufbewahrungstags anzeigen und Einstellungen und Standardwerte für die Aufbewahrungstags ändern (siehe Kapitel 10) Standardmitglieder: *Organisationsverwaltung (nur delegierend)*
MyTextMessaging	Erstellen, Anzeigen und Ändern ihrer Textnachrichteneinstellungen, also der Zusammenarbeit mit Mobiltelefonen und dem SMS-Versand Standardmitglieder: *Standard-Rollenzuweisungsrichtlinie*
MyVoiceMail	Voicemail-Einstellungen anzeigen und ändern Standardmitglieder: *Standard-Rollenzuweisungsrichtlinie*
Organisationsclientzugriff	Ermöglicht Administratoren das Verwalten von Clientzugriffsserver-Einstellungen. Standardmitglieder: *Organisationsverwaltung*
Organisationskonfiguration	Verwalten von Einstellungen für die Organisation, zum Beispiel: – URL der Homepage verwalteter Ordner – SMTP-Adresse und alternative E-Mail-Adressen von Microsoft-Exchange-Empfängern – Eigenschaftenschemakonfiguration für das Ressourcenpostfach – Hilfe-URLs für die Exchange-Verwaltungskonsole und Outlook Web App Standardmitglieder: *Organisationsverwaltung*
Organisationstransporteinstellungen	Verwalten von Systemnachrichten, der Standortkonfiguration und einige Transporteinstellungen. Die Rolle erlaubt nicht die Konfiguration von Empfangs- oder Sendeconnectoren, Warteschlangen, Remote- und akzeptierten Domänen. Standardmitglieder: *Organisationsverwaltung*
POP3- und IMAP4-Protokolle	Verwalten der POP3- und IMAP4-Konfiguration Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Öffentliche-Ordner-Replikation	Starten und Beenden der Replikation öffentlicher Ordner Standardmitglieder: *Organisationsverwaltung*

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010 (Forts.)

Verwaltungsrolle	Aufgaben
Öffentliche Ordner	Verwalten der öffentlichen Ordner. Die Rolle erlaubt aber nicht die Festlegung, ob öffentliche Ordner E-Mail-aktiviert sind, und ermöglicht es auch nicht, die Replikation öffentlicher Ordner anzupassen. Für diese beiden Aufgaben benötigen Sie die beiden Rollen *E-Mail-aktivierte Öffentliche Ordner* und *Öffentliche Ordner-Replikation*. Standardmitglieder: *Organisationsverwaltung* und *Verwaltung Öffentlicher Ordner*
Empfangsconnectors	Verwalten von Empfangsconnectoren, zum Beispiel die Festlegung von Größenbeschränkungen für einzelne Server Standardmitglieder: *Verwaltung von Nachrichtenschutz*, *Organisationsverwaltung* und *Serververwaltung*
Empfängerrichtlinien	Verwalten von Empfängerrichtlinien (siehe Kapitel 4, 5, 7 und 9) Standardmitglieder: *Organisationsverwaltung* und *Empfängerverwaltung*
Remote- und akzeptierte Domänen	Verwalten von Remote- und akzeptierten Domänen der Organisation Standardmitglieder: *Organisationsverwaltung*
Aufbewahrungsmanagement	Verwaltung von Aufbewahrungsrichtlinien in der Organisation (siehe Kapitel 10) Standardmitglieder: *Organisationsverwaltung* und *Datensatzverwaltung*
Rollenverwaltung	Verwalten von Verwaltungsrollengruppen, Rollenzuweisungsrichtlinien und Verwaltungsrollen, inklusive der Rolleneinträge, -zuweisungen und -Verwaltungsbereiche in der Organisation Standardmitglieder: *Organisationsverwaltung*
Sicherheitsgruppenerstellung und -mitgliedschaft	Erstellen und Verwalten universeller Sicherheitsgruppen und Verwalten der Mitgliedschaften Standardmitglieder: *Organisationsverwaltung*
Sendeconnectoren	Verwalten der Sendeconnectoren in der Organisation (siehe Kapitel 5) Standardmitglieder: *Organisationsverwaltung*
Diagnoseunterstützung	Ermöglicht die Diagnose von Servern, zusammen mit dem Microsoft-Support. Standardmitglieder: *Organisationsverwaltung*
Transport-Agents	Verwalten der Transportagenten, zum Beispiel für den Spamschutz (siehe Kapitel 4, 13, 14 und 15) Standardmitglieder: *Organisationsverwaltung* und *Verwaltung von Nachrichtenschutz*
Transportschutz	Verwalten der Antiviren- und Antispamfunktionen (siehe Kapitel 14 und 15) Standardmitglieder: *Organisationsverwaltung* und *Verwaltung von Nachrichtenschutz*
Transportwarteschlangen	Verwalten der Warteschlangen einzelner Server (siehe Kapitel 5) Standardmitglieder: *Organisationsverwaltung* und *Serververwaltung*
Transportregeln	Verwalten der Transportregeln der Organisation (siehe Kapitel 5) Standardmitglieder: *Organisationsverwaltung* und *Datensatzverwaltung*

Tabelle 16.1: Übersicht der Verwaltungsrollen in Exchange Server 2010 (Forts.)

Verwaltungsrolle	Aufgaben
UM-Postfächer	Verwalten der UM-Einstellungen für Postfächer (siehe auch Kapitel 20) Standardmitglieder: *Organisationsverwaltung* und *UM-Verwaltung*
UM-Ansagen	Verwalten der automatischen Ansagen von Exchange im Bereich Unified Messaging (siehe Kapitel 20) Standardmitglieder: *Organisationsverwaltung* und *UM-Verwaltung*
Unified Messaging	Verwalten von UM-Servern. Die Rolle ermöglicht es nicht, Postfachkonfigurationen oder UM-Ansagen zu verwalten. Dazu benötigen Administratoren die beiden Rollen *UM-Postfächer* und *UM-Ansagen*. Standardmitglieder: *Organisationsverwaltung* und *UM-Verwaltung*
Rollenverwaltung ohne Bereichseinschränkung	Erstellen und Verwalten von Verwaltungsrollen oberster Ebene ohne Bereichseinschränkung in der Organisation. Rollen auf oberster Ebene ohne Bereichseinschränkung sind Verwaltungsrollen, mit denen Sie Zugriff auf benutzerdefinierte Skripten und auf CMDlets, bei denen es sich nicht um Exchange-CMDlets handelt, erteilen können. Die normalen Verwaltungsrollen ermöglichen nur den Zugriff auf Exchange-CMDlets. Standardmitglieder: *Organisationsverwaltung*
Benutzeroptionen	Anzeige der Outlook Web App-Optionen eines Benutzers (siehe Kapitel 11) Standardmitglieder: *Organisationsverwaltung* und *Helpdesk*
Konfiguration (nur Anzeige)	Anzeige aller nicht empfängerbezogenen Exchange-Konfigurationseinstellungen, zum Beispiel Serverkonfigurationen, Transportkonfigurationen, Datenbankkonfigurationen und unternehmensweite Konfigurationen Standardmitglieder: *Delegiertes Setup, Verwalten von Nachrichtenschutz, Organisationsverwaltung* und *Organisationsverwaltung – nur Leserechte*
Empfänger mit Leserechten	Anzeigen der Konfiguration von Empfängern, zum Beispiel Postfächer, E-Mail-Benutzer, E-Mail-Kontakte und Verteilergruppen Standardmitglieder: *Helpdesk, Verwalten von Nachrichtenschutz, Organisationsverwaltung* und *Organisationsverwaltung – nur Leserechte*

Wollen Sie Verwaltungsrollen zu Verwaltungsrollengruppen hinzufügen, müssen Sie in der Exchange-Verwaltungsshell die englischen Bezeichnungen verwenden. Auch für diese Aktion steht ohne das Service Pack 1 für Exchange Server 2010 keine Möglichkeit in der Exchange-Verwaltungskonsole zur Verfügung. Nach der Installation des Service Pack 1 können Sie die Zuweisungen auch in der Exchange-Systemsteuerung durchführen. In der Exchange-Systemsteuerung sehen Sie auch die Berechtigungen, welche die Verwaltungsrolle ermöglicht.

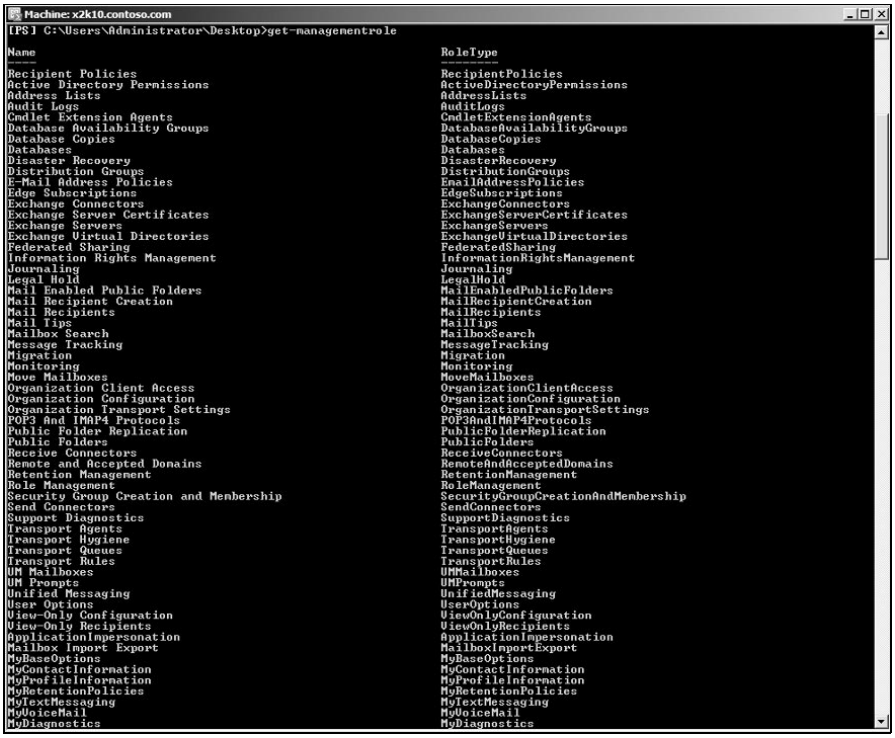


Abbildung 16.15: Anzeigen der Verwaltungsrollen in der Exchange-Verwaltungsshell

16.2.2 Verwaltungsrollenzuweisungen im Überblick

Verwaltungsrollenzuweisungen sind eine Verknüpfung zwischen einer Verwaltungsrolle und einem Rollenempfänger. Ein Rollenempfänger ist eine Verwaltungsrollengruppe, eine Rollenzuweisungsrichtlinie, ein Benutzer oder eine universelle Sicherheitsgruppe. Fügen Sie Rollenzuweisungen für Rollenempfänger hinzu oder entfernen beziehungsweise ändern Sie diese, können Sie festlegen, welche Berechtigungen Benutzer mit administrativen Aufgaben erhalten sollen. Sie können Rollen auch Benutzern oder universellen Sicherheitsgruppen direkt zuweisen, allerdings ist das nicht zu empfehlen. Am besten verwenden Sie Rollengruppen und Rollenzuweisungsrichtlinien, um Berechtigungen zu erteilen. Sie können Rollen einer Rollengruppe oder Rollenzuweisungsrichtlinie hinzufügen und Mitglieder der Rollengruppe hinzufügen oder aus ihr entfernen, um Rechte zu steuern.

INFO

Rollenzuweisungsrichtlinien können Sie nur Endbenutzer-Verwaltungsrollen zuweisen. Bei der Erstellung einer Rollenzuweisung für Rollenzuweisungsrichtlinien können Sie keine eigenen Verwaltungsbereiche angeben.

Delegierende Rollenzuweisungen im Überblick

Durch das Delegieren von Rollenzuweisungen erteilen Sie keinen Zugriff auf die Verwaltung von Funktionen, sondern Sie ermöglichen es dem Rollenempfänger, die angegebene Rolle anderen Rollenempfängern zuzuweisen. Handelt es sich bei dem Rollenempfänger um eine Rollengruppe, kann jedes Mitglied der Rollengruppe die Rolle einem anderen Rollenempfänger zuweisen. Standardmäßig darf nur die Rollengruppe *Organisationsverwaltung* anderen Rollenempfängern Rollen zuweisen. Mitglied dieser Gruppe ist nur das Benutzerkonto, mit dem Sie Exchange Server 2010 installiert haben. Sie können dieser Rollengruppe weitere Benutzer hinzufügen oder andere Rollengruppen erstellen und ihnen delegierende Rollenzuweisungen zuweisen. Soll ein Administrator eine bestimmte Funktion verwalten und die Rolle auch anderen Benutzern zuweisen können, müssen Sie folgende Aufgaben durchführen:

1. Sie müssen eine Rollenzuweisung für jede Verwaltungsrolle erstellen, mit der der Zugriff auf die zu verwaltenden Funktionen erteilt wird.
2. Sie erstellen eine delegierende Rollenzuweisung für jede Verwaltungsrolle, für die Sie die Zuweisung zu anderen Rollenempfängern zulassen.

Reguläre Rollenzuweisungen und delegierende Rollenzuweisungen müssen daher nicht identisch sein. Ein Benutzer, der Rechte vergibt, muss nicht zwingend selbst Rechte haben, die entsprechende Funktion auch selbst verwalten zu können. Allerdings könnte er sich selbst das Recht erteilen, indem er sich selber der Rolle zuweist. Erstellen Sie eine reguläre oder delegierende Verwaltungsrollenzuweisung, können Sie die Zuweisung mit einem Verwaltungsbereich einschränken. Auf diesem Weg können zum Beispiel Administratoren in einer Niederlassung nur Empfänger in derselben Niederlassung verwalten oder Administratoren in einer anderen Niederlassung nur Server an ihrem Active Directory-Standort. Zusätzlich gibt es noch exklusive Bereiche. Diese exklusiven Rollenzuweisungen sind notwendig, wenn Sie einen exklusiven Bereich einer Rollenzuweisung zuordnen. Exklusive Bereiche verwenden Sie wie reguläre Bereiche. Diese ermöglichen es Rollenempfängern, Empfänger zu verwalten, die zu dem exklusiven Bereich gehören, alle anderen Rollenempfänger dürfen den Empfänger im exklusiven Bereich nicht verwalten.

16.2.3 Verwaltungsrollenzuweisungen: Verwaltungsrollen zu Verwaltungsrollengruppen hinzufügen oder entfernen

Welche Rechte Benutzer haben, die Sie einer Verwaltungsrollengruppe hinzufügen, hängt von den Verwaltungsrollen ab, die mit der entsprechenden Verwaltungsrollengruppe verknüpft sind. Im ersten Abschnitt des Kapitels haben wir Ihnen die standardmäßig vorhandenen Verwaltungsgruppen in Exchange Server 2010 gezeigt sowie die zugeordneten Verwaltungsrollen. In der Tabelle 16.1 sehen Sie die stan-

dardmäßig vorhandenen Verwaltungsrollen und welchen Verwaltungsgruppen diese standardmäßig zugeordnet sind.

INFO

Sie können den standardmäßig vorhandenen Verwaltungsrollengruppen keine weiteren Verwaltungsrollen hinzufügen.

Verwaltungsrollen zu Verwaltungsgruppen hinzufügen

Weisen Sie eine Verwaltungsrolle einer Verwaltungsrollengruppe hinzu, müssen Sie noch den Namen dieser Zuweisung festlegen. Der Vorgang hat folgende Syntax:

New-ManagementRoleAssignment -Name <Name der Zuweisung> -SecurityGroup <Verwaltungsrollengruppe> -Role <Verwaltungsrolle>

Haben Sie einen Verwaltungsbereich (siehe Kapitel 16.3) erstellt, können Sie mit der Option *CustomRecipientWriteScope* den Verwaltungsbereich der Verwaltungsrolle zuweisen, wenn Sie die Verwaltungsrolle wiederum in eine Verwaltungsrollengruppe aufnehmen. Neben einem Verwaltungsbereich für Empfänger, können Sie den Befehl auch mit einem Konfigurationsverwaltungsbereich kombinieren. Dazu verwenden Sie dann die Option *CustomConfigWriteScope*. Verwaltungsbereiche für Empfänger schränken den Wirkungsbereich der Verwaltungsrolle auf einen Bereich von bestimmten Empfängern ein, die auch auf verschiedenen Servern positioniert sein können. Ein Verwaltungsbereich für die Konfiguration ermöglicht das Einschränken auf Basis von Servern oder der Organisation.

New-ManagementRoleAssignment -Name <Name der Zuweisung> -SecurityGroup <Verwaltungsrollengruppe> -Role <Verwaltungsrolle> -CustomRecipientWriteScope <Verwaltungsbereich>

Wollen Sie den Bereich einer Verwaltungsrolle auf eine Organisationseinheit beschränken, können Sie die Organisationseinheit mit der Option *RecipientOrganizationalUnitScope* angeben. Sie können als Pfad für die OU auch eine Domäne und eine übergeordnete OU mitgeben, mit folgender Syntax:

New-ManagementRoleAssignment -Name <Name der Zuweisung> -SecurityGroup <Verwaltungsrollengruppe> -Role <Verwaltungsrolle> -RecipientOrganizationalUnitScope <FQDN der Domäne>/<Übergeordnete OU>/<Untergeordnete OU>

Beispiel:

New-ManagementRoleAssignment -Name »Migration-Admins-Berlin« -SecurityGroup »Berlin-Empfänger-Verwaltung« -Role »Migration« -RecipientOrganizationalUnitScope contoso.com/Berlin

Nach der Installation von Service Pack 1 für Exchange Server 2010 können Sie in der Exchange-Systemsteuerung über die Details von Verwaltungsrollengruppen einzelne Verwaltungsrollen hinzufügen. Die Exchange-Systemsteuerung zeigt für alle Verwaltungsrollen eine Hilfe an.

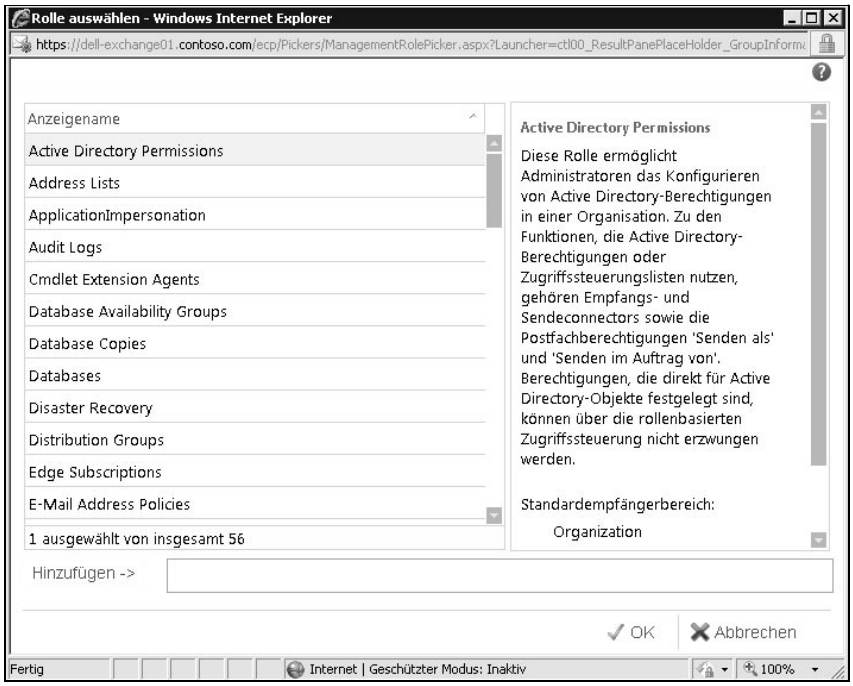
```
Machine: x2k10.contoso.com
[PS] C:\Users\Administrator\Desktop>New-ManagementRoleAssignment -Name "Migration-Admins-Berlin" -SecurityGroup "Berlin-
Empfänger-Verwaltung" -Role "Migration" -RecipientOrganizationalUnitScope contoso.com/Berlin

Name                           Role            RoleAssigneeName  RoleAssigneeType  AssignmentMethod  EffectiveUserNam
                                                                                                   e
----                           ----            ----------------  ----------------  ----------------  ----------------
Migration-Admins-Berlin        Migration       Berlin-Empfäng... RoleGroup         Direct

[PS] C:\Users\Administrator\Desktop>
```

Abbildung 16.16: Zuweisen einer Verwaltungsrolle zu einer Verwaltungsrollengruppe auf Basis einer OU

Abbildung 16.17: Verwaltungsrollen in der Exchange-Systemsteuerung zu Verwaltungsrollengruppen hinzufügen



Verwaltungsrollen von Verwaltungsrollengruppen entfernen

INFO

Die Berechtigungen eines Benutzers mit administrativen Rechten setzen sich als Summe aller Verwaltungsrollen zusammen, die den Verwaltungsrollengruppen zugewiesen sind, bei denen er Mitglied ist. Wenn er Mitglied mehrerer Verwaltungsrollengruppen ist und eine bestimmte Verwaltungsrolle mehreren Verwaltungsgruppen zugewiesen ist, hat er auch dann noch das Recht, eine Verwaltungsrolle zu nutzen, wenn Sie diese aus einer Verwaltungsrollengruppe entfernen. Wollen Sie ihm das Recht einer Verwaltungsrolle komplett verweigern, müssen Sie ihn aus allen Verwaltungsrollengruppen entfernen, welche die bestimmte Verwaltungsrolle enthalten, oder Sie müssen die Verwaltungsrolle von allen Verwaltungsrollengruppen entfernen, in denen der Benutzer Mitglied ist.

Mit dem Befehl *Get-ManagementRoleAssignment -RoleAssignee <Verwaltungsrollengruppe>* lassen Sie sich den Namen der Zuweisung anzeigen, mit der Sie die Verwaltungsrolle der entsprechenden Verwaltungsrollengruppe zugewiesen haben.

Abbildung 16.18: Anzeigen der Verwaltungsrollen, die einer Verwaltungsrollengruppe zugeordnet sind

Mit dem Befehl *Remove-ManagementRoleAssignment <Name der Zuweisung>* entfernen Sie die entsprechende Verwaltungsrolle über deren Zuweisung von der Verwaltungsrollengruppe. Sie können Verwaltungsrollen auch über die Exchange-Systemsteuerung von Verwaltungsrollengruppen entfernen. Dazu muss auf dem Server aber das Service Pack 1 für Exchange Server 2010 installiert sein.

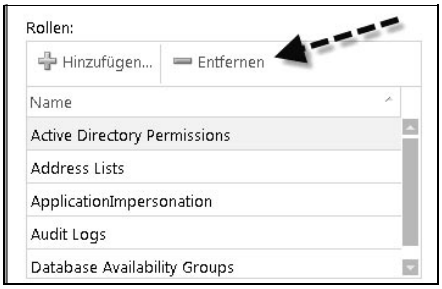


Abbildung 16.19: Entfernen von Verwaltungsrollen aus Verwaltungsrollengruppen

16.2.4 Ändern des Bereichs von Rollenzuweisungen in einer Rollengruppe

Rollenzuweisungen zwischen einer Verwaltungsrollengruppe und einer Verwaltungsrolle sind auf Verwaltungsbereiche begrenzt, die festlegen, welche Objekte Mitglieder der Verwaltungsrollengruppe verwalten dürfen. Diesen Bereich können Sie anpassen. Nach dem Erstellen einer Rollengruppe können Sie die Verwaltungsbereiche in den Rollenzuweisungen über das CMDlet *Set-ManagementRoleAssignment* anpassen. Wollen Sie den Verwaltungsbereich aller Rollenzuweisungen zwischen einer Verwaltungsrollengruppe und den enthaltenen Verwaltungsrollen gleichzeitig anpassen, rufen Sie zunächst die Rollenzuweisungen für die Verwaltungsgruppe auf und geben Sie dann den neuen Bereich für jede Zuweisung an. Dazu verwenden Sie das CMDlet *Get-ManagementRoleAssignment*, um die Rollenzuweisungen anzuzeigen, und übergeben nach dem Abrufen die Liste an das CMDlet *Set-ManagementRoleAssignment*:

Get-ManagementRoleAssignment -RoleAssignee <Verwaltungsrollengruppe> | Set-ManagementRoleAssignment -CustomRecipientWriteScope <Empfängerbereich> -CustomConfigWriteScope <Konfigurationsbereich> -RecipientRelativeScopeWriteScope <MyDistributioGroups | Organization | Self> -ExclusiveRecipientWriteScope <Exklusiver Empfängerbereich> -ExclusiveConfigWriteScope <Exklusiver Verwaltungsbereich> -RecipientOrganizationalUnitScope <Organisationseinheit>

Sie müssen natürlich nur die Optionen verwenden, die Sie zum Abrufen benötigen.

Beispiel:

Get-ManagementRoleAssignment -RoleAssignee »Berlin-Empfänger-Verwaltung« | Set-ManagementRoleAssignment -CustomRecipientWriteScope »Vertriebsmitarbeiter«

Mit der Option *WhatIf* können Sie überprüfen was der Befehl ausführen würde, ohne tatsächlich Änderungen vorzunehmen. Nach dem erfolgreichen Test können Sie die Option *WhatIf* entfernen, um die Änderungen anzuwenden.

In der Exchange-Systemsteuerung können Sie nach der Installation von Service Pack 1 für Exchange Server 2010 auch Schreibbereiche einer Verwaltungsrollengruppe hinzufügen. Sie können entweder den Standard-Schreibbereich verwenden, eine Organisationseinheit verwenden oder einen benutzerdefinierten Schreibbereich hinterlegen, den Sie aber zuvor in der Exchange-Verwaltungsshell erstellen müssen.

16.2.5 Anzeigen der Verwaltungsrollen und der Details in einer Verwaltungsrollengruppe

Mit *Get-RoleGroup* lassen Sie sich zunächst alle erstellten Verwaltungsrollengruppen anzeigen. Anschließend können Sie mit dem Befehl *(Get-RoleGroup <Verwaltungsrollengruppe>).Roles* die Verwaltungsrollen anzeigen, die mit der Verwaltungsrollengruppe verknüpft sind. Nach der Installation von Service Pack 1 für Exchange Server 2010 können Sie diese Details auch in der Exchange-Systemsteuerung aufrufen. Sie finden die Einstellungen auch über die *Toolbox* in der Exchange-Verwaltungskonsole, wenn Sie auf *Benutzereditor für die rollenbasierte Zugriffssteuerung* klicken.

Mit dem CMDlet *Get-ManagementRoleAssignment* können Sie detailliertere Informationen über die Rollenzuweisungen anzeigen. Geben Sie dazu den Befehl *Get-ManagementRoleAssignment -RoleAssignee <Verwaltungsrollengruppe>* ein.

Neben den Verwaltungsrollen einer bestimmten Verwaltungsrollengruppe können Sie Verwaltungsrollen auch auf Basis eines bestimmten Rollentyps oder nur Rollen mit bestimmten enthaltenen CMDlets und Optionen anzeigen. Sie können auch nur Details einer bestimmten Verwaltungsrolle anzeigen. Die Details einer

Rolle lassen sich auch durch das Anzeigen einer bestimmten Rolle mit dem CMDlet *Get-ManagementRole* und durch Umleiten der Ausgabe an das CMDlet *Format-List* anzeigen:

Get-ManagementRole < *role name* > | *Format-List*

Beispiel:

Get-ManagementRole »Mail Recipients« | *Format-List*

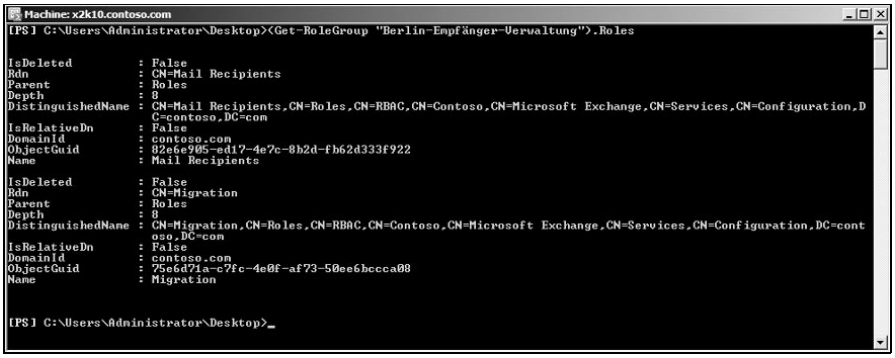


Abbildung 16.20: Anzeigen der Verwaltungsrollen einer Verwaltungsrollengruppe

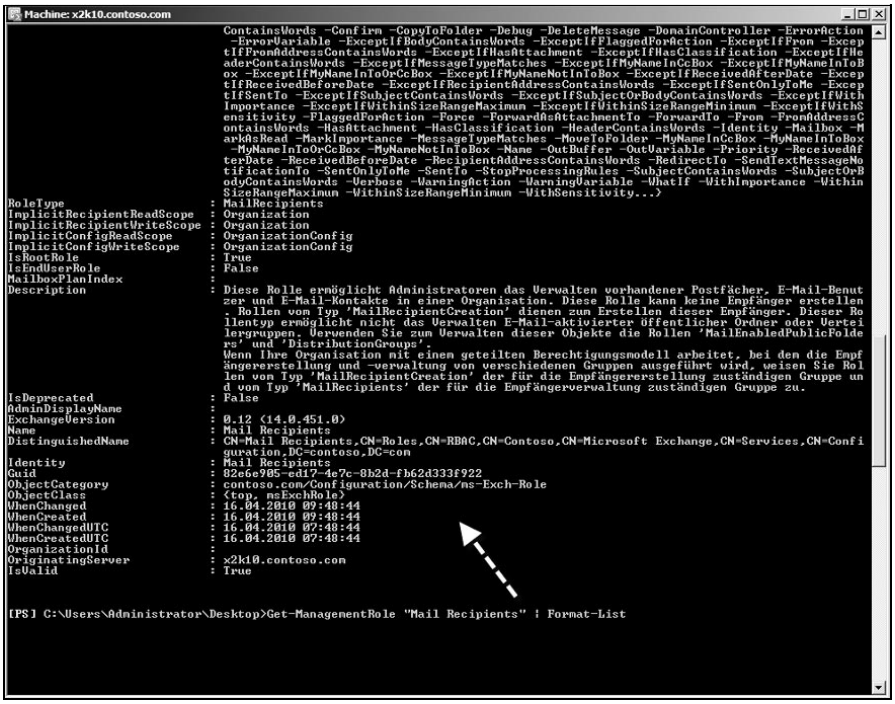


Abbildung 16.21: Anzeigen der Details einer bestimmten Verwaltungsrolle

Alle Verwaltungsrollen zeigen Sie an, wenn Sie das CMDlet *Get-ManagementRole* ohne Angabe von Rollen verwenden. Wollen Sie eine Liste der spezifischen Eigenschaften für alle Rollen in der Organisation anzeigen, verwenden Sie die folgende Syntax:

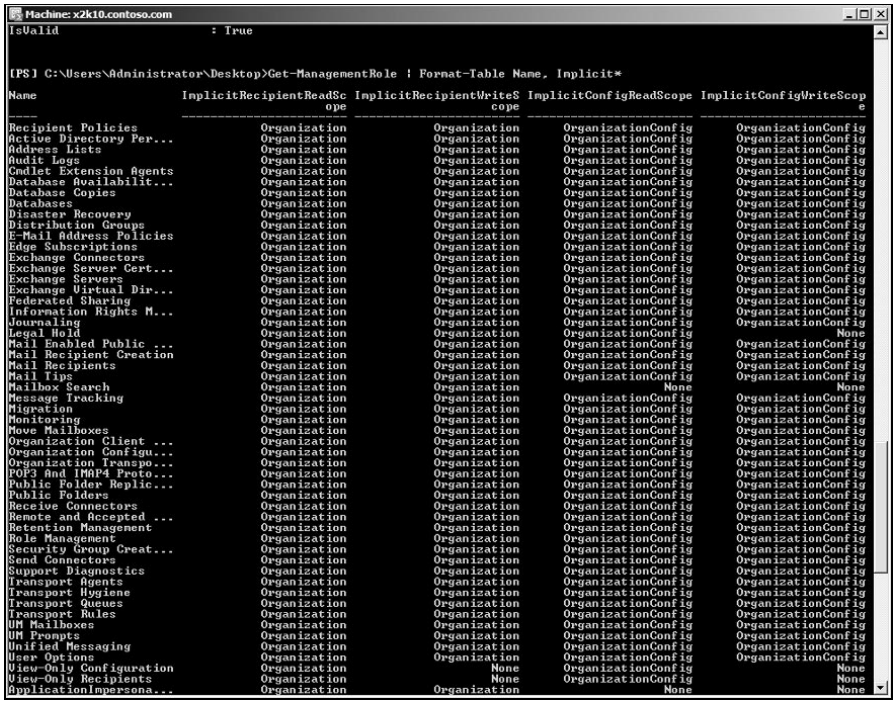
Get-ManagementRole | Format-Table <Eigenschaft 1>, <Eigenschaft 2...>

Beispiel:

Eine Liste aller Rollen und Anzeige der Eigenschaften *Name* und aller Eigenschaften, deren Bezeichnung mit der Zeichenfolge *Implicit* beginnt:

*Get-ManagementRole | Format-Table Name, Implicit**

Abbildung 16.22: Anzeigen einer formatierten Liste von Verwaltungsrollen



Sie können auch eine Liste von Verwaltungsrollen anzeigen, die ein bestimmtes CMDlet enthalten, indem Sie die Option *Cmdlet* für das CMDlet *Get-ManagementRole* verwenden:

Get-ManagementRole -Cmdlet <CMDlet>

Beispiel:

Get-ManagementRole -Cmdlet New-Mailbox

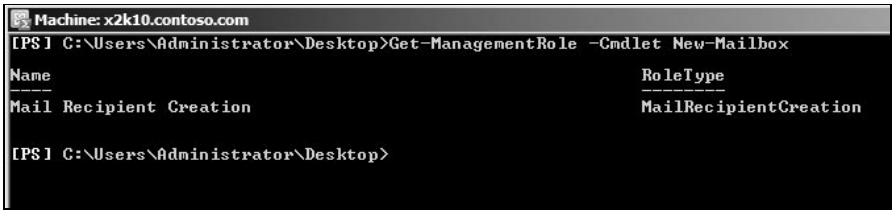


Abbildung 16.23: Anzeigen aller Verwaltungsrolle mit einem bestimmten CMDlet

Sie können auch eine Liste von Verwaltungsrollen anzeigen, die eine angegebene Option eines CMDlets enthalten, indem Sie die Option *CmdletParameters* für das CMDlet *Get-ManagementRole* verwenden. Verwenden Sie *CmdletParameters* zusammen mit der Option *Cmdlet*, zeigt die Shell nur Rollen an, die die für das ausgewählte CMDlet angegebenen Optionen enthalten. Verwenden Sie die Option *Cmdlet* nicht, zeigt die Shell auch Rollen an, welche die angegebenen Optionen enthalten, unabhängig davon, zu welchem CMDlet sie gehören:

Get-ManagementRole [-Cmdlet <CMDlet>] -CmdletParameters <Option 1>, <Option 2…>

Beispiel:

Get-ManagementRole -CmdletParameters Database, Server

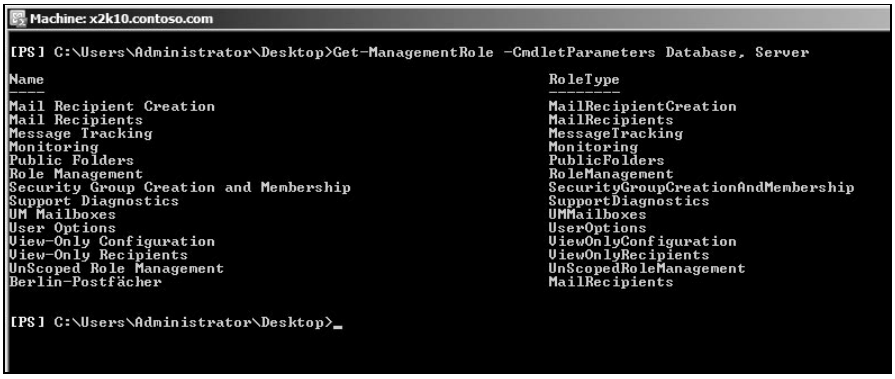


Abbildung 16.24: Anzeigen aller Verwaltungsrollen, deren CMDlets die Optionen Database und Server enthalten

Get-ManagementRole -Cmdlet Set-Mailbox -CmdletParameters EmailAddresses

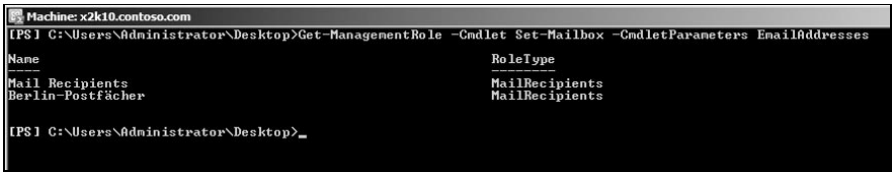


Abbildung 16.25: Anzeigen aller Verwaltungsrollen, die ein bestimmtes CMDlet mit einer bestimmten Option enthalten

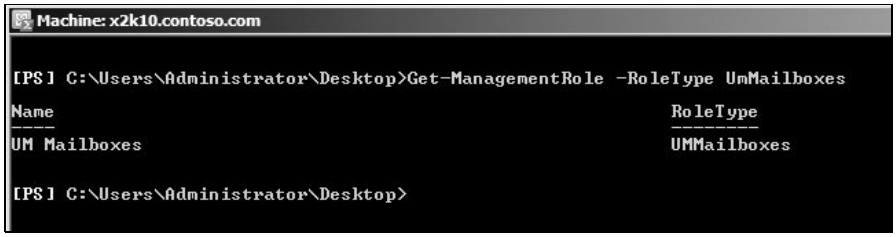
Sie können auch das Platzhalterzeichen (*) mit den Optionen *Cmdlet* oder *Cmdlet-Parameters* verwenden. Wollen Sie alle Rollen mit einem bestimmten Rollentyp anzeigen, verwenden Sie die Option *RoleType* für das CMDlet *Get-ManagementRole*:

Get-ManagementRole -RoleType <Rollentyp>

Beispiel:

Get-ManagementRole -RoleType UmMailboxes

Abbildung 16.26: Anzeigen von Verwaltungsrollen mit bestimmten Rollentypen



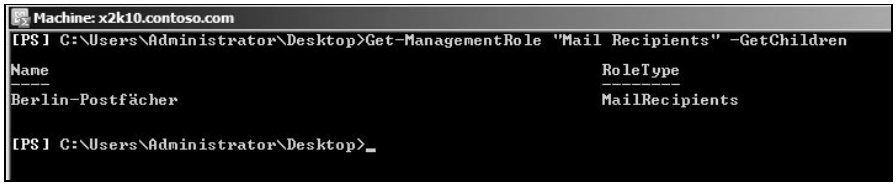
Eine Liste von untergeordneten Verwaltungsrollen einer angegebenen übergeordneten Rolle erhalten Sie mit der Option *GetChildren* für das CMDlet *Get-ManagementRole:*.

Get-ManagementRole <Übergeordnete Rolle> -GetChildren

Beispiel:

Get-ManagementRole »Mail Recipients« -GetChildren

Abbildung 16.27: Anzeigen der untergeordneten Verwaltungsrolle einer bestimmten übergeordneten Verwaltungsrolle



Auch eine Liste aller untergeordneten Verwaltungsrollen einer angegebenen übergeordneten Rolle bis zur letzten untergeordneten Rolle in der Kette können Sie anzeigen, indem Sie die Option *Recurse* für das CMDlet *Get-ManagementRole* verwenden. Der Option legt fest, dass die Shell jede Beziehung zwischen übergeordneter und untergeordneter Rolle sucht, bis die letzte untergeordnete Rolle erreicht ist. Die übergeordnete Rolle ist ebenfalls Bestandteil der Liste:

Get-ManagementRole <Name der übergeordneten Rolle> -Recurse

16.2.6 Erstellen, Entfernen und Verwalten eigener Verwaltungsrollen

Neben den standardmäßig vorhandenen Verwaltungsrollen in Exchange Server 2010 können Sie auch eigene Verwaltungsrollen erstellen. Allerdings ist das selten sinnvoll, da die meisten notwendigen Aufgaben bereits in den angelegten Verwaltungsrollen abgebildet sind. Neue Verwaltungsrollen basieren auf vorhandenen Verwaltungsrollen. Erstellen Sie eine neue Verwaltungsrolle, kopieren Sie eine vorhandene Verwaltungsrolle und deren Verwaltungsrolleneinträge in die neue Rolle. Die vorhandene Rolle wird dabei zur übergeordneten Rolle der neuen untergeordneten Rolle. Untergeordnete Rollen können keine Verwaltungsrolleneinträge enthalten, die in der übergeordneten Rolle nicht vorhanden sind. Um eine neue Verwaltungsrolle zu erstellen, verwenden Sie folgenden Befehl:

New-ManagementRole -Parent <Existierende übergeordnete Verwaltungsrolle> -Name <Name der neuen Verwaltungsrolle>

Beispiel:

New-ManagementRole -Parent »Mail Recipients« -Name »Berlin-Postfächer«

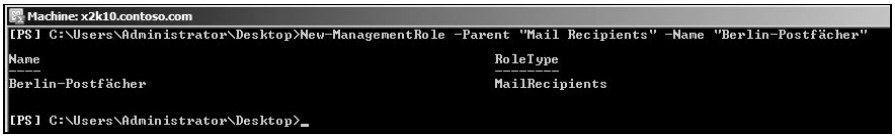


Abbildung 16.28: Anlegen einer neuen Verwaltungsrolle

Wenn Sie eine neue Verwaltungsrolle erstellt haben, können Sie Einträge der Verwaltungsrolle ändern. Löschen Sie einen Rolleneintrag, können Administratoren, denen die Rolle zugewiesen ist, auf das zugehörige CMDlet nicht mehr zugreifen. Sie können auch einzelne Optionen aus einem Rolleneintrag entfernen, um den Zugriff auf die Option im zugehörigen CMDlet einzuschränken oder zu verweigern. Rolleneinträge, die in der übergeordneten Rolle nicht enthalten sind, lassen sich auch in der untergeordneten Verwaltungsrolle nicht hinzufügen. Neue Verwaltungsrollen übernehmen die Lese- und Schreib-Verwaltungsrollenbereiche der übergeordneten Rolle als sogenannte implizite Bereiche. Erstellen Sie einen neuen benutzerdefinierten Bereich, deaktivieren Sie den impliziten Schreibbereich der Rolle. Der implizite Lesebereich der Rolle ändert sich dadurch nicht. Sie können benutzerdefinierte Bereiche oder einen exklusiven Bereich erstellen, vordefinierte Bereiche einsetzen oder einen Bereich für eine Zuweisung zu einer Organisationseinheit festlegen.

Entfernen einer Verwaltungsrolle

Sie können nur Verwaltungsrollen löschen, die Sie erstellt haben. Die standardmäßig vorhandenen Verwaltungsrollen lassen sich nicht entfernen. Vor dem Löschen einer Verwaltungsrolle müssen Sie alle Verwaltungsrollenzuweisungen entfernen. Um eine Verwaltungsrolle zu löschen, verwenden Sie folgenden Befehl:

Remove-ManagementRole < *Verwaltungsrolle* >

Wollen Sie eine Rolle mit untergeordneten Rollen löschen, müssen Sie auch die untergeordneten Rollen entfernen. Verwenden Sie dazu die Option *Recurse*, um auch alle untergeordneten Rollen der Verwaltungsrolle zu löschen. Mit der Option *WhatIf* können Sie testen, was passiert, ohne die Rolle tatsächlich zu löschen:

Remove-ManagementRole < *Verwaltungsrolle* > *-Recurse -WhatIf*

Wollen Sie eine Rolle ohne Bereichseinschränkung löschen (siehe nächster Abschnitt) können Sie genauso vorgehen. Zusätzlich müssen Sie noch die Option *UnScopedTopLevel* verwenden.

16.2.7 Rollen auf oberster Ebene ohne Bereichseinschränkung

Rollen auf oberster Ebene ohne Bereichseinschränkung sind Verwaltungsrollen, mit denen Sie Zugriff auf benutzerdefinierte Skripts und auf CMDlets, bei denen es sich nicht um Exchange-CMDlets handelt, erteilen können. Die normalen Verwaltungsrollen ermöglichen nur den Zugriff auf Exchange-CMDlets. Um eine Rolle auf oberster Ebene ohne Bereichseinschränkung zu erstellen, müssen Sie die Option *UnscopedTopLevel* des CMDlets *New-ManagementRole* verwenden. Rollen ohne Bereichseinschränkung sind immer innerhalb der gesamten Organisation gültig. Sie können Rollen ohne Bereichseinschränkung Rollengruppen, Verwaltungsrollen, Benutzern und universellen Sicherheitsgruppen zuweisen, aber keinen Zuweisungsrichtlinien für Verwaltungsrollen. Exchange-CMDlets können Sie nicht einer Rolle ohne Bereichseinschränkung hinzufügen. Die Rollengruppe *Organisationsverwaltung* verfügt standardmäßig nicht über die Berechtigungen zum Erstellen oder Verwalten von Rollengruppen ohne Bereichseinschränkung. Sie können sich die Verwaltungsrolle *Rollenverwaltung ohne Bereichseinschränkung* aber selbst zuweisen. Rolleneinträge der obersten Ebene ohne Bereichseinschränkung verwenden Sie zusammen mit Verwaltungsrollen auf oberster Ebene ohne Bereichseinschränkung. Jeder Rolleneintrag ohne Bereichseinschränkung ist einem einzigen benutzerdefinierten Skript oder einem Nicht-Exchange-CMDlet zugeordnet. Um einen Rolleneintrag ohne Bereichseinschränkung zu erstellen, verwenden Sie das CMDlet *New-ManagementRoleEntry* mit der Option *UnscopedTopLevel*. Sie müssen alle Optionen angeben, die Anwender mit dem Skript oder dem Nicht-Exchange-CMDlet verwenden dürfen. Fügen Sie Optionen hinzu, müssen Sie den Rolleneintrag manuell aktualisieren.

INFO

Skripte, die Sie einem Rolleneintrag ohne Bereichseinschränkung hinzufügen, müssen sich auf jedem Server im Verzeichnis für Exchange-Server 2010-Skripte befinden. Das Standardinstallationsverzeichnis für Skripte ist *C:\Programme\Microsoft\Exchange Server\V14\Scripts*.

Erstellen einer Rolle ohne Bereichseinschränkung

Bevor Sie eine Rolle ohne Bereichseinschränkung erstellen können, also eine Rolle, die PowerShell-CMDlets enthält, die grundsätzlich nichts mit der Exchange-Verwaltungsshell zu tun haben, müssen Sie sich selbst oder dem entsprechenden Administrator die Rolle *Rollenverwaltung ohne Bereichseinschränkung* (*Unscoped Role Management*) zuweisen. Diese Verwaltungsrolle ist standardmäßig noch keiner Verwaltungsrollengruppe zugewiesen. Um die Verwaltungsrolle der Verwaltungsrollengruppe *Organisationsverwaltung* zuzuweisen, verwenden Sie folgende Syntax:

New-ManagementRoleAssignment -Name »Rollen ohne Bereichseinschränkung« -SecurityGroup »Organization Management« -Role »Unscoped Role Management«

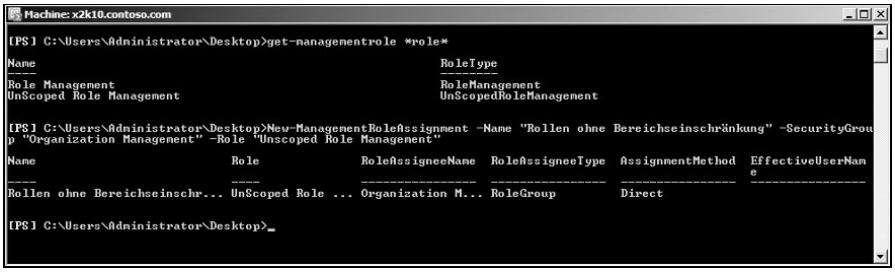


Abbildung 16.29: Abrufen von bestimmten Verwaltungsrollen mit Platzhalter und Hinzufügen einer Verwaltungsrolle zu einer Verwaltungsrollengruppe

INFO

Nach dem Zuweisen einer Verwaltungsrolle zu einer Verwaltungsrollengruppe müssen Sie die Exchange-Verwaltungsshell neu starten, damit die Rechte übernommen werden.

Die Syntax zum Erstellen einer solchen Rolle ist:

New-ManagementRole <Verwaltungsrolle> -UnscopedTopLevel

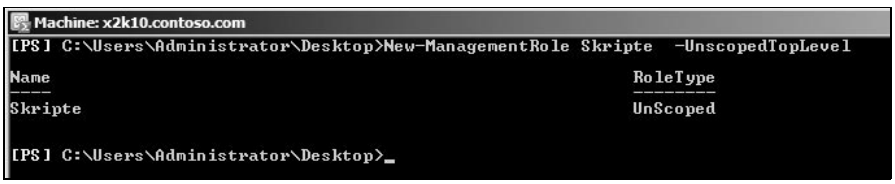


Abbildung 16.30: Erstellen einer Rolle ohne Bereichseinschränkung

Nach der Erstellung der Verwaltungsrolle müssen Sie dieser noch Einträge, also CMDlets oder Skripte, in Form von Verwaltungsrolleneinträgen hinzufügen (siehe nächster Abschnitt). Skripte, die Sie hinzufügen, müssen sich im Exchange

Server 2010-Installationspfad im Verzeichnis *Scripts* auf jedem Server mit Exchange Server 2010 befinden, auf denen Sie das Skript ausführen wollen. Haben Sie das Skript auf die Exchange-Server kopiert, erstellen Sie den Rolleneintrag mit der Syntax:

Add-ManagementRoleEntry <Erstellte Verwaltungsrolle>\<Name des Skripts> -Parameters <Option 1, Option 2> -Type Script -UnscopedTopLevel

Wollen Sie CMDlets statt Skripte hinzufügen, verwenden Sie die folgende Syntax:

Add-ManagementRoleEntry <Erstellte Verwaltungsrolle>\<Name des CMDlets> -PSSnapinName <Name des SnapIns der PowerShell, zu welcher das CMDlet gehört> -Parameters <Option 1, Option 2> -Type Cmdlet -UnscopedTopLevel

Anschließend können Sie die neue Rolle einer Rollengruppe, einem Benutzer oder einer universellen Sicherheitsgruppe zuweisen. Sie können auch untergeordnete Rollen ohne Bereichseinschränkung erstellen, wie bei normalen Verwaltungsrollen auch als Kopie einer übergeordneten Verwaltungsrolle ohne Bereichseinschränkung. Die untergeordneten Verwaltungsrollen ohne Bereichseinschränkung können eine Teilmenge der Skripten und CMDlets enthalten, die Bestandteil der übergeordneten Verwaltungsrollen ohne Bereichseinschränkung sind. Die Vorgehensweise dabei entspricht normalen Verwaltungsrollen, das gilt auch für die Einschränkungen. Die Syntax für den Befehl ist:

New-ManagementRole -Parent <Existierende Verwaltungsrolle> -Name <Neue Verwaltungsrolle>

16.2.8 Verwaltungsrolleneinträge bearbeiten

Für jede Verwaltungsrolle gibt es mindestens einen Verwaltungsrolleneintrag. Ein Eintrag besteht aus einem einzelnen CMDlet und dessen Optionen, einem Skript oder einer speziellen Berechtigung. Rollen, die auf integrierten Exchange-Rollen basieren, können nur Exchange Server 2010-CMDlets enthalten. Verwaltungsrolleneinträge können Sie nicht untergeordneten Rollen hinzufügen, wenn diese nicht in den übergeordneten Rollen enthalten sind. Die Namen von Verwaltungsrolleneinträgen bestehen aus der Verwaltungsrolle, dem Namen des CMDlets und sind durch einen umgekehrten Schrägstrich (\) getrennt, zum Beispiel *Mail Recipients\Set-Mailbox*.

Verwaltungsrolleneinträge anzeigen

Mit dem CMDlet *Get-ManagementRoleEntry* können Sie die Verwaltungsrolleneinträge einer Verwaltungsrolle anzeigen lassen:

Get-ManagementRoleEntry »<Verwaltungsrolle>«*

Sie können auch hier mit dem Platzhalter arbeiten und auch eine Zeichenfolge innerhalb eines CMDlets verwenden. Sie müssen den Text hinter *Get-ManagementRoleEntry* in Anführungszeichen schreiben.

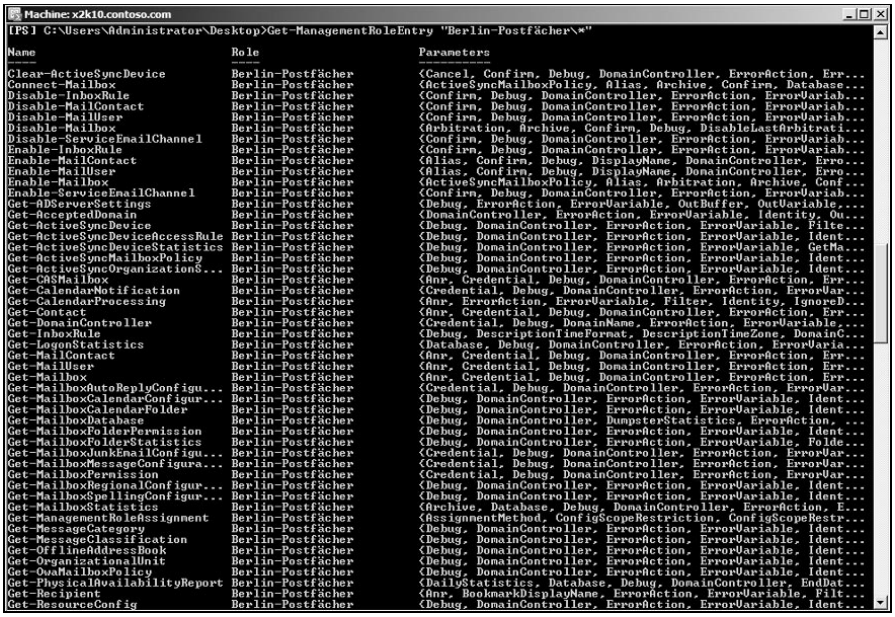


Abbildung 16.31: Anzeigen der Verwaltungsrolleneinträge einer Verwaltungsrolle

Sie können sich auch alle Verwaltungsrollen anzeigen lassen, die einen bestimmten Verwaltungsrolleneintrag aufweisen:

*Get-ManagementRoleEntry *\ < CMDlet >*

Beispiel:

*Get-ManagementRoleEntry *\Set-Mailbox*

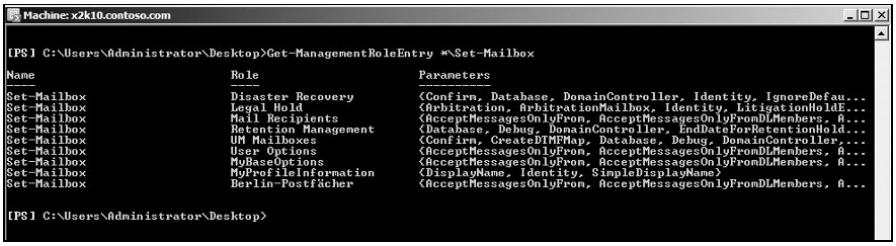


Abbildung 16.32: Anzeigen aller Verwaltungsrollen mit einem bestimmten Verwaltungsrolleneintrag

Kennen Sie nur einen Teil der Bezeichnung der Verwaltungsrolle oder des Verwaltungsrolleneintrags, können Sie auch mit dem Platzhalter * an verschiedenen Stellen arbeiten:

*Get-ManagementRoleEntry * < Teil des Namens der Verwaltungsrolle > ** < Teil des Namens der Verwaltungsrolleneintrags > **

Wollen Sie alle Optionen eines bestimmten Verwaltungsrolleneintrags anzeigen, verwenden Sie den Befehl:

(Get-ManagementRoleEntry < Verwaltungsrolle > \ < CMDlet >).Parameters

(Get-ManagementRoleEntry »Mail Recipients\Set-Mailbox«).Parameters

Verwaltungsrolleneinträge hinzufügen

Wollen Sie zusätzliche CMDlets den Administratoren zur Verfügung stellen, nehmen Sie diese als Verwaltungsrolleneinträge in eine Verwaltungsrolle auf. Den Standardrollen in Exchange Server 2010 können Sie keine weiteren Einträge hinzufügen, sondern nur selbst erstellten Verwaltungsrollen. Der Rolleneintrag, den Sie einer Verwaltungsrolle hinzufügen wollen, muss auch in der übergeordneten Verwaltungsrolle vorhanden sein. Um einen Eintrag hinzuzufügen, verwenden Sie folgenden Befehl:

Add-ManagementRoleEntry < Verwaltungsrolle > \ < CMDlet >

Wollen Sie einen Rolleneintrag hinzufügen, aber nur bestimmte Optionen des entsprechenden CMDlets in den Rolleneintrag aufnehmen, verwenden Sie die folgende Syntax:

Add-ManagementRoleEntry < Verwaltungsrolle > \ < CMDlet > -Parameters < Option 1 >, < Option 2 >,…

Wollen Sie einer Rolle mehrere Rolleneinträge auf einmal hinzufügen, rufen Sie eine Liste der Rolleneinträge von der übergeordneten Rolle ab, indem Sie den Platzhalter * nutzen. Dazu verwenden Sie das CMDlet *Get-ManagementRoleEntry*. Mit der Option *Overwrite* überschreiben Sie bereits vorhandene Einträge. Die Ausgabe leiten Sie dann an das CMDlet *Add-ManagementRoleEntry* weiter. Folgende Syntax ist dabei notwendig:

*Get-ManagementRoleEntry < Übergeordnete Verwaltungsrolle > * < Bezeichnung des CMDlets > * | Add-ManagementRoleEntry -Role < Untergeordnete Verwaltungsrolle > -overwrite*

Beispiel:

*Get-ManagementRoleEntry »Mail Recipients*Mailbox*« | Add-ManagementRoleEntry -Role »Berlin Mail Recipients«*

Sie können bereits vorhandene Verwaltungsrolleneinträge auch nachträglich bearbeiten. Wollen Sie zum Beispiel Optionen von CMDlets hinzufügen bzw. entfernen, verwenden Sie die Optionen *AddParameter* und *RemoveParameter* des CMDlets *Set-ManagementRoleEntry*. Alle Optionen in einer untergeordneten Verwaltungsrolle müssen auch in der übergeordneten Verwaltungsrolle vorhanden sein. Wollen Sie eine Option eines Eintrags in einer übergeordneten Verwaltungsrolle entfernen, müssen Sie die Option vorher in allen untergeordneten Verwaltungsrollen entfernen. Zum Hinzufügen einer Option verwenden Sie die Syntax:

Set-ManagementRoleEntry <Verwaltungsrolle>\<CMDlet> -Parameters <Option 1>, <Option 2>… -AddParameter

Zum Entfernen von Optionen aus einem Rolleneintrag verwenden Sie die Syntax:

Set-ManagementRoleEntry <Verwaltungsrolle>\<CMDlet> -Parameters <Option 1>, <Option 2>… -RemoveParameter

Wollen Sie alle Optionen eines Eintrags entfernen, zum Beispiel um später einzelne Einträge wieder manuell hinzuzufügen, verwenden Sie die Syntax:

Set-ManagementRoleEntry <Verwaltungsrolle>\<CMDlet> -Parameters $Null

Wollen Sie nur die Optionen für den Eintrag zur Verfügung stellen, die Sie im Befehl mitgeben, und alle vorhandenen entfernen, verwenden Sie nur die Option *Parameter* und lassen die Optionen *AddParameter* und *RemoveParameter* weg. Alle anderen Optionen entfernt der Befehl vom Verwaltungsrolleneintrag:

Set-ManagementRoleEntry <Verwaltungsrolle>\<CMDlet> -Parameters <Option 1>, <Option 2>

Entfernen von Verwaltungsrolleneinträgen

Mit folgendem Befehl entfernen Sie einen kompletten Verwaltungsrolleneintrag von einer Verwaltungsrolle:

Remove-ManagementRoleEntry <Verwaltungsrolle>\<Verwaltungsrolleneintrag>

Wollen Sie mehrere Rolleneinträge aus einer Verwaltungsrolle zu entfernen, verwenden Sie das CMDlet *Get-ManagementRoleEntry* und geben Sie die Ausgabe an das CMDlet *Remove-ManagementRoleEntry* weiter. Sie können an dieser Stelle auch mit dem Platzhalter * des CMDlets *Get-ManagementRoleEntry* arbeiten. Verwenden Sie folgende Syntax:

Get-ManagementRoleEntry <Verwaltungsrolle>\<Verwaltungsrolleneintrag> * | *Remove-ManagementRoleEntry -WhatIf*

Mit der Option *WhatIf* können Sie testen, was passiert, ohne die Änderung tatsächlich durchzuführen. Entfernen Sie –*WhatIf*, führt das CMDlet die Änderung tatsächlich durch.

16.2.9 Verwaltungsrollentypen

Verwaltungsrollentypen dienen der Gruppierung zusammengehöriger Rollen und sind in die folgenden Kategorien unterteilt:

- *Administrator- oder Spezialistenrollen* – Rollen dieses Rollentyps ermöglichen die Ausführung von Aufgaben zur Verwaltung von Servern, Empfängern und die Konfiguration der Organisation.

- *Benutzerspezifische Rollen* – Rollen dieses Rollentyps ermöglichen die Ausführung von Aufgaben zur Konfiguration von Benutzerprofilen und die Verwaltung des eigenen Postfachs sowie die Verwaltung von Verteilergruppen. Die Bezeichnung von Rollen dieses Rollentyps beginnen mit *My*.
- *Sonderrollen* – Rollen dieses Rollentyps ermöglichen die Ausführung von Aufgaben, die nicht zu den Verwaltungsrollentypen oder benutzerspezifischen Rollentypen gehören. Diese Rollen ermöglichen die Ausführung von Nicht-Exchange-CMDlets und -Skripts.

In der folgenden Tabelle gehen wir auf wichtige Administratorrollen und deren Aufgaben ein. Wir haben bereits in Tabelle 16.1 alle Verwaltungsrollen und deren deutsche Bezeichnung aufgelistet. In der Tabelle 16.2 finden Sie die englischen Bezeichnungen und den Geltungsbereich der Aufgabe. Wollen Sie wissen, welche Verwaltungsrollengruppen die verschiedenen Verwaltungsrollen nutzen, finden Sie in der Tabelle 16.1 weitere Informationen.

TIPP

Übernehmen in Ihrem Unternehmen verschiedene Gruppen die Erstellung von Empfängern und die Verwaltung von Empfängern, können Sie verschiedene Rollentypen zuweisen. Die Gruppe, die für die Erstellung der Postfächer zuständig ist, benötigt die Rolle *MailRecipientCreation.* Die Gruppe, die Empfänger verwaltet, benötigt die Rolle *MailRecipients*.

Tabelle 16.2: Verschiedene Rollentypen für Administratorrechte

Verwaltungsrollen	Aufgabe	Geltungsbereich
ActiveDirectoryPermissions	Konfigurieren von Active Directory-Berechtigungen in der Organisation	Organisation
AddressLists	Verwaltung der Adresslisten und Offline-Adresslisten	Organisation
DatabaseAvailabilityGroups	Verwalten von Datenbankverfügbarkeitsgruppen	Organisation
DatabaseCopies	Verwalten der Datenbankkopien auf einzelnen Servern	Server
Databases	Verwalten der Datenbanken für Postfächer oder für öffentliche Ordner	Server
DisasterRecovery	Rechte für die Wiederherstellung auch für Datenbankverfügbarkeitsgruppen	Organisation
DistributionGroups	Verwalten von Verteilergruppen	Organisation
EdgeSubscriptions	Konfiguration von Edge-Synchronisation und -Abonnement zwischen Edge-Transport- und Hub-Transport-Servern	Organisation
EMailAddressPolicies	Verwalten der Richtlinien für E-Mail-Adressen	Organisation
ExchangeConnectors	Verwalten der Connectoren in einer Organisation, inklusive Sende- und Empfangsconnectoren	Organisation
ExchangeServerCertificates	Verwalten der Exchange-Serverzertifikate auf einzelnen Servern, inklusive Erstellen, Importieren und Exportieren	Server

Tabelle 16.2: Verschiedene Rollentypen für Administratorrechte (Forts.)

Verwaltungsrollen	Aufgabe	Geltungsbereich
ExchangeServers	Verwalten der Exchange-Serverkonfiguration auf einzelnen Servern	Server
ExchangeVirtualDirectories	Verwalten der virtuellen Verzeichnisse für Outlook Web App, ActiveSync, Offline-Adressbuch, AutoDiscovery und PowerShell	Server
FederatedSharing	Administratoren, die gesamtstruktur- und organisationsweiten Freigaben in einer Organisation verwalten können	Organisation
InformationRightsManagement	Verwalten der IRM-Funktionen (Information Rights Management) von Exchange	Organisation
Journaling	Verwalten der Journalkonfiguration	Organisation
LegalHold	Verwalten der LegalHold-Konfiguration im Bereich der Archivierung	Organisation
MailboxSearch	Postfächer in einer Organisation durchsuchen	Organisation
MailEnabledPublicFolders	Öffentliche Ordner in einer Organisation, E-Mail-aktivieren oder E-Mail-deaktivieren. Mit diesem Rollentyp können Sie nur die E-Mail-Eigenschaften von Öffentlichen Ordnern verwalten. Um andere Eigenschaften öffentlicher Ordner zu verwalten, muss eine Rolle des Rollentyps *PublicFolders* zugewiesen sein.	Organisation
MailRecipientCreation	Erstellen von Postfächern, Kontakten, Verteilergruppen. Kombination mit dem Rollentyp *MailRecipients* möglich, für die Erstellung und Verwaltung von Empfängern. Mit diesem Rollentyp können Sie keine öffentlichen Ordner E-Mail-aktivieren. Dazu benötigen Sie den Rollentyp *MailEnabledPublicFolders*.	Organisation
MailRecipients	Mit diesem Rollentyp dürfen bereits existierende Postfächer verwaltet werden. Empfänger können nicht erstellt werden. In Kombination mit Rollen des Rollentyps *MailRecipientCreation* sind auch die Erstellung und die Verwaltung von Empfängern möglich.	Organisation
MessageTracking	Nachverfolgen von E-Mails in der Organisation	Organisation
Migration	Postfächer in einen oder von einem Server migrieren	Server
Monitoring	Verfügbarkeit von Exchange-Diensten und -Komponenten überwachen. Überwachungsanwendungen von Drittanbietern verwenden die Rollen, um Informationen zum Status von Exchange-Servern zu erfassen.	Organisation
MoveMailboxes	Postfächer zwischen Servern innerhalb einer Organisation und zwischen mehreren Organisation verschieben	Organisation
OrganizationClientAccess	Einstellungen der Clientzugriffsserver verwalten	Organisation

Tabelle 16.2: Verschiedene Rollentypen für Administratorrechte (Forts.)

Verwaltungsrollen	Aufgabe	Geltungsbereich
OrganizationConfiguration	Organisationsweite Einstellungen verwalten. Der Rollentyp verfügt nicht über die in den Rollentypen *OrganizationClientAccess* oder *OrganizationTransportSettings* enthaltenen Berechtigungen.	Organisation
OrganizationTransport-Settings	Organisationsweite Transporteinstellungen verwalten. Die Rolle erlaubt es nicht, Transport-Empfangs- oder Sendeconnectoren oder Warteschlangen, Remote- und akzeptierte Domänen oder Rollen zu erstellen oder zu verwalten. Um die einzelnen Transportfunktionen zu erstellen oder zu verwalten, müssen Rollen der folgenden Rollentypen zugewiesen sein: *ReceiveConnectorsSendConnectors-TransportQueuesTransportHygieneTransportAgentsRemote-andAcceptedDomainsTransportRules*	Organisation
Pop3andIMAP4Protocols	Verwalten der POP3- und IMAP4-Konfiguration, zum Beispiel Authentifizierungs- und Verbindungseinstellungen auf einzelnen Servern	Server
PublicFolderReplication	Replikation öffentlicher Ordner starten und stoppen	Organisation
PublicFolders	Verwalten der öffentlichen Ordner. Mit diesem Rollentyp können Sie öffentliche Ordner nicht E-Mail-aktivieren und auch nicht die Replikation öffentlicher Ordner verwalten. Für die Konfiguration der Replikation öffentlicher Ordner muss eine Rolle des Rollentyps *PublicFolderReplication* zugewiesen sein.	Organisation
ReceiveConnectors	Empfangsconnectoren und die Größenbeschränkungen auf einem einzelnen Server verwalten	Server
RecipientPolicies	Empfängerrichtlinien verwalten	Organisation
RemoteandAccepted-Domains	Remote- und akzeptierte Domänen in einer Organisation verwalten	Organisation
Resetpassword	Kennwörter zurücksetzen	Organisation
RetentionManagement	Aufbewahrungsrichtlinien in einer Organisation verwalten	Organisation
RoleManagement	Verwaltungsrollengruppen, Rollenzuweisungsrichtlinien, Verwaltungsrollen, Rolleneinträge, Zuweisungen und Bereiche in einer Organisation verwalten. Benutzer dürfen Rollengruppen konfigurieren oder einer Rollengruppe Mitglieder hinzufügen oder entfernen.	Organisation
SecurityGroupCreationand-Membership	Universelle Sicherheitsgruppen und die Mitgliedschaft erstellen und verwalten	Organisation
SendConnectors	Sendeconnectoren in einer Organisation verwalten	Organisation
SupportDiagnostics	Diagnosefunktionen unter Anleitung der Microsoft Support Services in einer Organisation ausführen	Organisation
TransportAgents	Transport-Agents verwalten	Organisation

Verwaltungsrollen	Aufgabe	Geltungsbereich
TransportHygiene	Antiviren- und Antispamfunktionen in einer Organisation verwalten	Organisation
TransportQueues	Transportwarteschlangen verwalten	Server
TransportRules	Transportregeln in einer Organisation verwalten	Organisation
UMMailboxes	UM-Konfiguration von Postfächern und anderen Empfängern in einer Organisation verwalten	Organisation
UMPrompts	Benutzerdefinierte UM-Sprachansagen in einer Organisation erstellen und verwalten	Organisation
UnifiedMessaging	UM-Server in einer Organisation verwalten. Diese Rolle ermöglicht es nicht, UM-spezifische Postfachkonfigurationen oder UM-Ansagen zu verwalten. Dafür sind die beiden Rollentypen *UMMailboxes* und *UMPrompts* zuständig.	Organisation
UnScopedRoleManagement	Verwaltungsrollen auf oberster Ebene ohne Bereichseinschränkung in einer Organisation erstellen und verwalten	Organisation
UserOptionsSupport	Outlook Web App-Optionen eines Benutzers in einer Organisation anzeigen. Rollen dieses Rollentyps können dazu verwendet werden, Benutzer bei der Diagnose von Problemen in Zusammenhang mit ihrer Konfiguration zu unterstützen.	Organisation
ViewOnlyConfiguration	Konfigurationseinstellungen in einer Organisation anzeigen, zum Beispiel Serverkonfigurationen, Transportkonfigurationen, Datenbankkonfigurationen und unternehmensweite Konfigurationen. Zusammen mit Rollen des Rollentyps *ViewOnlyRecipients* können alle Objekte in einer Organisation angezeigt werden.	Organisation
ViewOnlyRecipients	Konfiguration von Empfängern	Organisation

Tabelle 16.2: Verschiedene Rollentypen für Administratorrechte (Forts.)

16.3 Verwaltungsrollenbereiche verstehen

Verwaltungsrollenbereiche ermöglichen die Festlegung eines Einflussbereichs für eine Verwaltungsrolle. Hierbei handelt es sich um eine Einschränkung des Bereichs, in dem Rechte einer Verwaltungsrolle ausgeübt werden dürfen. Aktivieren Sie einen Bereich, kann ein Administrator nur die in diesem Bereich enthaltenen Objekte ändern. Normalerweise gibt eine Verwaltungsrolle bereits an, welche Objekte Sie erstellen oder ändern können. Ein Verwaltungsrollenbereich legt fest, wo Administratoren etwas erstellen oder ändern können. Sie können Administratoren den Zugriff auf Objekte innerhalb eines exklusiven Bereichs verweigern. Jede Rolle kann folgende Bereichstypen haben:

- *Empfängerlesebereich* – Dieser Bereich bestimmt, welche Empfängerobjekte der Administrator aus dem Active Directory lesen kann.

- *Empfängerschreibbereich* – Dieser Bereich legt fest, welche Empfängerobjekte der Administrator im Active Directory ändern kann.
- *Konfigurationslesebereich* – Der Konfigurationslesebereich bestimmt, welche Konfigurationsobjekte der Administrator aus dem Active Directory lesen kann.
- *Konfigurationsschreibbereich* – Der Bereich legt fest, welche Organisations- und Serverobjekte der Administrator im Active Directory ändern kann.

16.3.1 Bereichsfilter für Verwaltungsrollen

Mit Bereichsfiltern können Sie einen benutzerdefinierten Bereich erstellen. Für Bereichsfilter können Sie fast alle Eigenschaften von Empfängern oder Serverobjekten verwenden. Bereichsfilter erstellen Sie mit dem CMDlet *New-ManagementScope*. Sie können mit dem CMDlet verschiedene Optionen verwenden, um die Bereiche zu unterteilen. Die Bereiche sind in Empfänger und Konfiguration sowie in reguläre und exklusive Bereiche unterteilt. Dazu verwenden Sie folgende Optionen des CMDlets *New-ManagementScope*:

- Regulärer gefilterter Empfängerbereich – *RecipientRestrictionFilter*
- Exklusiver gefilterter Empfängerbereich – *RecipientRestrictionFilter* und Option *Exclusive*
- Regulärer gefilterter serverbasierter Konfigurationsbereich – *ServerRestrictionFilter*
- Exklusiver gefilterter serverbasierter Konfigurationsbereich – *ServerRestrictionFilter* und Option *Exclusive*

Erstellen Sie einen eigenen benutzerdefinierten Bereich, verwenden Sie einen Filter, der nach Objekten innerhalb des impliziten Lesebereichs der Verwaltungsrolle sucht. Ein Bereichsfilter ist daher immer eine Einschränkung des implizierten Bereichs der Rolle, also von den Objekten, die Sie mit der Verwaltungsrolle ohnehin nur verwalten können. Eine Ausweitung des implizierten Bereichs durch einen Bereichsfilter ist daher nicht möglich. Geben Sie mit der Option *Recipient RestrictionFilter* des CMDlets *New-ManagementScope* einen Empfängerfilter an, können Sie mit *RecipientRoot* noch eine Organisationseinheit zur Filterung verwenden. Empfänger- und Konfigurationsfilter verwenden die gleiche Syntax, die mindestens folgende Bereiche enthalten muss:

1. Eine öffnende geschweifte Klammer ({) steht am Beginn der Filterabfrage.
2. Der Filterwert des Objekts, nach dem Sie filtern, zum Beispiel Servernamen, Werte des Postfachs, Abteilung usw.
3. Der Vergleichsoperator in Kombination mit dem Vergleichswert. Eine Liste aller Operatoren, die Sie in der Exchange-Verwaltungsshell verwenden können, finden Sie in der Tabelle 16.3.

4. Mit dem Vergleichswert vergleichen Sie, zusammen mit dem Vergleichsoperator, den Wert in den Eigenschaften des Objekts, zum Beispiel *Abteilung* als *Filterwert*, *-Like* als *Vergleichsoperator* und *Einkauf* als *Vergleichswert*.
5. Die schließende geschweifte Klammer (}) steht am Ende der Filterabfrage.

Beispiel für eine solche Abfrage:

{*City -Eq »Berlin«*}

Tabelle 16.3: In der Exchange-Verwaltungsshell verfügbare Vergleichsoperatoren

Operator	Aufgabe
-eq	Gleich (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-ne	Ungleich (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-lt	Kleiner als (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-gt	Größer als (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-le	Kleiner als oder gleich (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-ge	Größer als oder gleich (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-cge	Größer als oder gleich (unterscheidet zwischen Groß- und Kleinschreibung)
-ceq	Gleich (unterscheidet zwischen Groß- und Kleinschreibung)
-cne	Ungleich (unterscheidet zwischen Groß- und Kleinschreibung)
-clt	Kleiner als (unterscheidet zwischen Groß- und Kleinschreibung)
-cgt	Größer als (unterscheidet zwischen Groß- und Kleinschreibung)
-cle	Kleiner als oder gleich (unterscheidet zwischen Groß- und Kleinschreibung)
-contains	Enthält (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-ccontains	Enthält (unterscheidet zwischen Groß- und Kleinschreibung)
-notcontains	Enthält nicht (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-cnotcontains	Enthält nicht (unterscheidet zwischen Groß- und Kleinschreibung)
-and	Und
-or	Oder
-not	Nicht
-match	Zeichenfolgen mit regulären Ausdrücken vergleichen (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-notmatch	Zeichenfolgen mit regulären Ausdrücken vergleichen (unterscheidet nicht zwischen Groß- und Kleinschreibung)
-cmatch	Zeichenfolgen mit regulären Ausdrücken vergleichen (unterscheidet zwischen Groß- und Kleinschreibung)

Tabelle 16.3: In der Exchange-Verwaltungsshell verfügbare Vergleichsoperatoren (Forts.)

Operator	Aufgabe
-cnotmatch	Zeichenfolgen mit regulären Ausdrücken vergleichen (unterscheidet zwischen Groß- und Kleinschreibung)
-like	Zeichenfolgen mithilfe von Platzhalterzeichenregeln vergleichen
-notlike	Zeichenfolgen mithilfe von Platzhalterzeichenregeln vergleichen
-clike	Zeichenfolgen mithilfe von Platzhalterzeichenregeln vergleichen (unterscheidet zwischen Groß- und Kleinschreibung)
-cnotlike	Zeichenfolgen mithilfe von Platzhalterzeichenregeln vergleichen (unterscheidet zwischen Groß- und Kleinschreibung)

Neben den notwendigen Funktionen in einem Bereichsfilter können Sie auch optionale Komponenten einbauen, um die Abfrage zu verfeinern:

- Sie können in der Abfrage auch Klammern verwenden, um die Reihenfolge festzulegen, in der die Abfrage erfolgen soll. Exchange verwendet die Werte in den innersten Klammern zuerst und arbeitet sich dann nach außen.
- Mit logischen Operatoren, zum Beispiel *-And*, *-Or* und *-Not*, können Sie mehrere Vergleichsoperationen miteinander verknüpfen. In diesem Fall muss die Filterabfrage die gesamte Anweisung auswerten.

Ein Beispiel für eine komplexere Abfrage ist:

{*((City -Eq »Berlin«) -And (Department -Eq »Einkauf«)) -Or (Title -Like »*Manager*«)*}

Die Filterabfrage läuft folgendermaßen ab:

1. Die Eigenschaften *City* und *Department* werden ausgewertet. Wenn beide Eigenschaften *True* sind, wertet Exchange die gesamte *And*-Anweisung mit *True*. Hat eine der beiden Eigenschaften den Wert *False*, erhält die gesamte *And*-Anweisung den Wert *False*.
2. Hat die *And*-Anweisung den Wert *True*, hat die gesamte Filterabfrage den Wert *True*, da der *Or*-Operator nur verlangt, dass ein Teil der Abfrage den Wert *True* aufweisen muss.
3. Erhält die *And*-Anweisung den Wert *False*, setzt Exchange die Filterabfrage fort, um die Eigenschaft *Title* auszuwerten.
4. Ist die Eigenschaft *Title* mit *True* gewertet, erhält die gesamte Filterabfrage den Wert *True*, da der Or-Operator nur verlangt, dass ein Teil der Abfrage den Wert *True* aufweisen muss.

Beim Erstellen eines Empfängerfilters können Sie fast jede Eigenschaft des Empfängerobjekts verwenden. Die meisten Eigenschaften funktionieren mit der Option *RecipientRestrictionFilter* des CMDlets *New-ManagementScope.* Erstellen Sie einen Verwaltungsbereich mit der Option *ServerRestrictionFilter* können Sie die folgenden Servereigenschaften verwenden:

- *CurrentServerRole*
- *CustomerFeedbackEnabled*
- *DataPath*
- *DistinguishedName*
- *ExchangeLegacyDN*
- *ExchangeLegacyServerRole*
- *ExchangeVersion*
- *Fqdn*
- *Guid*
- *InternetWebProxy*
- *Name*
- *NetworkAddress*
- *ObjectCategory*
- *ObjectClass*
- *ProductID*
- *ServerRole*
- *WhenChanged*
- *WhenChangedUTC*
- *WhenCreated*
- *WhenCreatedUTC*

16.3.2 Exklusive Verwaltungsbereiche einsetzen

Exklusive Bereiche sind vor allem für Objekte mit hohen Sicherheitsanforderungen, zum Beispiel das Postfach des Geschäftsführers, gedacht und können solche Objekte besonders schützen. Erstellen Sie einen exklusiven Bereich, können nur die Benutzer, die diesem exklusiven Bereich zugewiesen sind, die Objekte in diesem Bereich ändern. Andere Rollenempfänger können keine Objekte in diesem Bereich ändern, auch dann nicht, wenn sich ihre Rollen über Bereiche erstrecken, welche die exklusiven Objekte ansonsten einschließen würden. Exklusive Bereiche überschreiben andere reguläre Bereiche. Exklusive Bereichsfilter erstellen Sie mit dem CMDlet *New-ManagementScope*. Sie können mit dem CMDlet verschiedene Optionen verwenden, um die Bereiche zu unterteilen. Die Bereiche sind in Empfänger und Konfiguration sowie in reguläre und exklusive Bereiche unterteilt. Dazu verwenden Sie folgende Optionen des CMDlets *New-ManagementScope*:

- Exklusiver gefilterter Empfängerbereich – *RecipientRestrictionFilter* und Option *Exclusive*
- Exklusiver gefilterter serverbasierter Konfigurationsbereich – *ServerRestrictionFilter* und Option *Exclusive*

16.3.3 Erstellen und Löschen von regulären und exklusiven Bereichen

Beim Erstellen eines Bereichs verändern Sie den Schreibbereich, der für die Verwaltungsrolle festgelegt ist. Der Administrator darf nur noch Änderungen im festgelegten Verwaltungsbereich, zum Beispiel den Empfängern in einer bestimmten OU, vornehmen. Der für die Verwaltungsrolle konfigurierte Lesebereich ist immer aktiv, das heißt, die Einstellungen anderer Empfänger darf der Administrator anzeigen, aber nicht bearbeiten. Erstellen Sie einen Empfängerfilter für einen Verwaltungsbereich, können Sie zusätzlich noch eine Organisationseinheit angeben.

Syntax:

- *New-ManagementScope -Name <Name des Verwaltungsbereichs> -RecipientRestrictionFilter <Filter> [-RecipientRoot <OU>]*
- *New-ManagementScope -Name <Name des Verwaltungsbereichs> -ServerList <Server 1>, <Server 2...>*

Beispiele:

- *New-ManagementScope -Name »Vertriebsmitarbeiter« -RecipientRestrictionFilter { RecipientType -eq 'UserMailbox' } -RecipientRoot »contoso.com/Vertriebs-OU«*
- *New-ManagementRole -Name »Server am Standort Berlin« -ServerRestrictionFilter { ServerSite -eq 'Berlin' }*
- *New-ManagementScope -Name »Postfachserver« -ServerList MBX1,MBX3,MBX5*

Erstellen Sie exklusive Verwaltungsbereiche, dürfen nur die Rollenempfänger, denen der exklusive Bereich zugewiesen ist, auf enthaltene Objekte zugreifen.

Beispiel:

New-ManagementScope »Leitende Angestellte« -RecipientRestrictionFilter { Department -Eq »Leitende Angestellte« } -Exclusive

Wollen Sie die Warnmeldung bei der Erstellung eines exklusiven Bereichs unterdrücken, verwenden Sie die Option *-Force*.

Um Verwaltungsbereiche zu löschen, verwenden Sie folgende Syntax:

Remove-ManagementScope <Name des Verwaltungsbereichs>

16.3.4 Verwaltungsbereiche anzeigen

Die Details eines Verwaltungsbereichs lassen Sie sich mit dem CMDlet *Get-ManagementScope |fl* anzeigen:

Get-ManagementScope <Name des Verwaltungsbereichs> | fl

Ohne Parameter können Sie sich eine Liste aller angelegten Verwaltungsbereiche anzeigen. Das CMDlet zeigt exklusive und reguläre Bereiche an.

Eine Liste aller Verwaltungsbereiche, die keinen Administratoren zugewiesen sind, erhalten Sie mit *Get-ManagementScope –Orphan*.

Wollen Sie nur reguläre oder exklusive Verwaltungsbereiche anzeigen, verwenden Sie den folgenden Befehl: *Get-ManagementScope -Exclusive $true* zeigt eine Liste der exklusiven Bereiche, *Get-ManagementScope -Exclusive $false* eine Liste der regulären Bereiche.

16.3.5 Verwaltungsbereiche anpassen

Erstellte Verwaltungsbereiche lassen sich nachträglich ändern:

Set-ManagementScope < Name des Verwaltungsbereichs > -Name < Neuer Name des Verwaltungsbereichs >

Neben dem Namen können Sie zum Beispiel auch die Filter ändern, auf deren Basis der Verwaltungsbereich aufgebaut ist:

Set-ManagementScope < Name des Verwaltungsbereichs > -RecipientRestrictionFilter { < Neuer Filer > }

Wollen Sie die oberste Ebene der Organisationseinheiten festlegen, in denen ein Administrator Änderungen vornehmen darf, verwenden Sie folgende Syntax:

Set-ManagementScope < Name des Verwaltungsbereichs > -RecipientRoot < OU >

Generell sind die Möglichkeiten des CMDlets *Set-ManagementScope* identisch mit den Möglichkeiten von *New-ManagementScope*:

Set-ManagementScope < Name des Verwaltungsbereichs > -ServerRestrictionFilter { < Neuer Filter > }

Die Serverliste für einen Verwaltungsbereich lässt sich allerdings nicht einfach ändern. Wollen Sie die Serverliste nachträglich anpassen, müssen Sie den Verwaltungsbereich neu erstellen und zuweisen, indem Sie die neue Serverliste verwenden. Den alten Verwaltungsbereich mit der alten Serverliste können Sie danach löschen.

16.4 Berechtigungen teilen und mehrere Gesamtstrukturen einsetzen

Auch wenn Exchange sehr eng mit dem Active Directory zusammenarbeitet, lassen sich Berechtigungen zwischen Gruppen aufteilen. Auch beim Einsatz mehrerer Exchange-Organisationen oder Active Directory-Gesamtstrukturen lassen sich die Rechte aufteilen. Die Exchange-Verwaltung und die Active Directory-Verwaltung lassen sich mit Exchange Server 2010 effizient trennen. Bei der Verwendung der Exchange-Verwaltungstools ist es unerheblich, über welche Active Directory-Berechtigungen ein Benutzer verfügt. Das RBAC-Berechtigungsmodell gilt nicht

für die Konsole *Active Directory-Benutzer und -Computer*. Sie können in Exchange Server 2010 zwischen einem Freigabeberechtigungsmodell und einem geteilten Berechtigungsmodell unterscheiden.

16.4.1 Freigabeberechtigungsmodell verwenden

Standardmäßig verwendet Exchange Server 2010 ein Freigabeberechtigungsmodell. Bei diesem Modell trennt Exchange die Verwaltung von Exchange- und Active Directory-Objekten nicht. Administratoren können also über die Exchange-Verwaltungstools auch Benutzerkonten erstellen. Dazu berechtigt sind die beiden Rollengruppen *Organisationsverwaltung* und *Empfängerverwaltung* mit den beiden Rollen *Erstellung von E-Mail-Empfängern* und *Sicherheitsgruppenerstellung und -mitgliedschaft*. Die Rollen *Erstellung von E-Mail-Empfängern* und *Sicherheitsgruppenerstellung und -verwaltung* lassen sich auch anderen Rollengruppen, Benutzern oder Gruppen zuweisen.

16.4.2 Getrennte Berechtigungen verwenden

Wollen Sie Exchange-Verwaltung und Active Directory-Verwaltung trennen, müssen Sie Exchange mit einem geteilten Berechtigungsmodell konfigurieren. In diesem Fall darf eine Admingruppe nur Active Directory-Objekte verwalten, zum Beispiel Benutzerkonten anlegen, und eine andere Gruppe darf Exchange-Attribute verwalten. So konfigurieren Sie ein geteiltes Berechtigungsmodell:

1. Erstellen Sie eine neue Rollengruppe mit den Active Directory-Administratoren, die Benutzerkonten erstellen sollen.
2. Erstellen Sie reguläre (erteilt Rechte der Rolle) und delegierende (erteilt die Möglichkeit, selbst Rechte zu erteilen) Rollenzuweisungen mit der Rolle *Erstellung von E-Mail-Empfängern* und der Rolle *Sicherheitsgruppenerstellung und -verwaltung* und der neuen Rollengruppe.
3. Entfernen Sie die regulären und delegierenden Verwaltungsrollenzuweisungen zwischen der Rolle *Erstellung von E-Mail-Empfängern* und den Rollengruppen *Organisationsverwaltung* und *Empfängerverwaltung*.
4. Entfernen Sie die regulären und delegierenden Rollenzuweisungen zwischen der Rolle *Sicherheitsgruppenerstellung und -verwaltung* und der Rollengruppe *Organisationsverwaltung*.

Nach dieser Aktion dürfen nur die Mitglieder der neuen Rollengruppe Postfächer erstellen. Die neue Gruppe kann Objekte aber nur erstellen, die Gruppe kann keine Exchange-Attribute für das neue Objekt konfigurieren. Ein Active Directory-Administrator muss das Objekt daher zuerst erstellen und anschließend muss ein Exchange-Administrator die Exchange-Attribute für das Objekt konfigurieren. Exchange-Administratoren können die folgenden CMDlets nicht verwenden, da diese den Active Directory-Administratoren vorbehalten sind:

- *New-Mailbox*
- *New-MailUser*
- *New-MailContact*
- *New-LinkedUser*
- *Remove-Mailbox*
- *Remove-MailUser*
- *Remove-MailContact*
- *Remove-LinkedUser*
- *Add-MailboxPermission*
- *Add-MailboxFolderPermission*

Soll die neue Rollengruppe auch Exchange-Attribute verwalten, weisen Sie dieser noch die Rolle *E-Mail-Empfänger* zu.

16.4.3 Berechtigungen für mehrere Gesamtstrukturen im Überblick

Exchange Server 2010 unterstützt zwei Arten von Topologien, wenn Sie mehrere Active Directory-Gesamtstrukturen und dabei mehrere Exchange-Organisationen einsetzen:

1. Gesamtstrukturübergreifende Topologien verfügen über mehrere AD-Gesamtstrukturen, mit jeweils einer eigenen Exchange-Organisation.
2. Topologien mit einer Ressourcengesamtstruktur verfügen über eine Exchange-Gesamtstruktur und eine Gesamtstruktur mit Benutzerkonten und Administratoren.

Beim Einsatz von mehreren Gesamtstrukturen verwenden Sie Gesamtstrukturvertrauensstellungen und die *GAL-Synchronisierung* (Global Address List, globale Adressliste) für die Erstellung verknüpfter Postfächer. Mehr zu diesem Thema finden Sie in Kapitel 2. Die Gesamtstruktur mit Exchange Server 2010 muss der Gesamtstruktur vertrauen, welche die universellen Sicherheitsgruppen enthält, die den verknüpften Rollengruppen zugeordnet sind. In dieser Gesamtstruktur befinden sich auch die Benutzer, die den verknüpften Postfächern zugeordnet sind.

INFO

Sie müssen die rollenbasierte Berechtigungen (RBAC) für jede Exchange-Organisation in den eingesetzten Gesamtstrukturen getrennt vornehmen, die Konfiguration lässt sich nicht synchronisieren. Erstellen Sie eine Rollengruppe in einer Gesamtstruktur, ist diese in keiner anderen Gesamtstruktur vorhanden, das gilt auch für die Rechte, die Sie zuweisen. Rollengruppen in verschiedenen Exchange-Organisationen haben keinerlei Verbindung miteinander.

Beim Einsatz von mehreren Exchange-Organisationen können Sie in diesem Fall identische Rollengruppen anlegen und jeweils die gleichen Rechte setzen. Hier

kommen Sie um die doppelte Konfiguration nicht herum. Auch wenn Sie identische Bezeichnungen wählen, ist jede Rollengruppe unabhängig. Auch die Verwaltungsbereiche sind an ihre eigene Gesamtstruktur gebunden. Serverbereiche können nur Server umfassen, die Mitglied der gleichen Gesamtstruktur sind. Sie können aber Benutzern außerhalb einer Gesamtstruktur Berechtigungen zum Anzeigen und Ändern von Exchange-Objekten in einer anderen Gesamtstruktur erteilen. Die Berechtigungen gelten aber nur für diese spezifische Exchange-Gesamtstruktur, auch hier findet keine Synchronisierung statt. Wollen Sie einen Administrator zum Mitglied der verknüpften Rollengruppe *Organisationsverwaltung* machen, die sich in Gesamtstruktur A befindet, kann der Benutzer nur die Exchange-Objekte in Gesamtstruktur A verwalten. Sie müssen den Benutzer zu einem Mitglied der verknüpften Rollengruppen in jeder anderen Exchange-Gesamtstruktur machen, um Berechtigungen zum Verwalten jeder Gesamtstruktur zu erteilen. Grenzübergreifende Berechtigungen ermöglichen es, Rollenzuweisungsrichtlinien auf Postfächer der Benutzer anzuwenden, deren Benutzerkonten in einer anderen Gesamtstruktur gespeichert sind.

Verknüpfte Rollengruppen im Überblick

Administrative Berechtigungen konfigurieren Sie in diesem Fall mit verknüpften Rollengruppen und verknüpften Postfächern über mehrere Gesamtstrukturen hinweg. Sie können eine verknüpfte Rollengruppe in einer Exchange-Organisation erstellen und mit einer universellen Sicherheitsgruppe in einer anderen Gesamtstruktur verknüpfen. Die Gruppe, mit der Sie eine verknüpfte Rollengruppe verbinden, muss sich in einer anderen Gesamtstruktur befinden. Sie können eine verknüpfte Rollengruppe nicht mit einer universellen Sicherheitsgruppe in der gleichen Gesamtstruktur verbinden. Zuweisungen zwischen Rollen und der verknüpften Rollengruppen können sich über mehrere Verwaltungsbereiche erstrecken. Diese Bereiche sind aber auf die Gesamtstruktur beschränkt, in der die verknüpfte Rollengruppe positioniert ist. Die Mitgliedschaft in der verknüpften Rollengruppe verwalten Sie über die Mitgliedschaft in der universellen Gruppe in der anderen Gesamtstruktur. Haben Sie mehrere verknüpfte Rollengruppen mit einer universellen Sicherheitsgruppe verbunden, erhalten die Mitglieder alle Berechtigungen, die jeder verknüpften Rollengruppe in jeder Exchange Server 2010-Gesamtstruktur zugewiesen sind. Sie können die Mitgliedschaft der verknüpften Rollengruppe aber nicht in der Exchange Server 2010-Gesamtstruktur verwalten. Da sich mehrere verknüpfte Rollengruppen aus verschiedenen Exchange Server 2010-Gesamtstrukturen einer einzelnen universellen Sicherheitsgruppe zuordnen lassen, können Unternehmen auch komplexe Strukturen mithilfe einer kleinen Gruppe universeller Sicherheitsgruppen in einer einzelnen Gesamtstruktur verwalten. Herkömmliche Rollengruppen lassen sich nicht in eine verknüpfte Rollengruppe umändern, Sie müssen verknüpfte Rollengruppen manuell erstellen.

Verknüpfte Postfächer im Überblick

Eine weitere Möglichkeit zum Zuweisen von Berechtigungen über Gesamtstrukturen hinweg sind verknüpfte Postfächer (siehe Kapitel 9). Verknüpfte Postfächer lassen sich als Mitglieder zu Rollengruppen innerhalb der Exchange Server 2010-Gesamtstruktur hinzufügen. Konfigurieren Sie ein verknüpftes Postfach als Mitglied einer Rollengruppe, erhält dadurch ein Benutzer in der Gesamtstruktur mit den Benutzerkonten die Berechtigungen der Rollengruppe, da sich das Postfach in der anderen Gesamtstruktur mit Exchange Server 2010 befindet. Verknüpfte Postfächer lassen sich beim Einsatz mehrerer Gesamtstrukturen den vorhandenen Rollengruppen wie normale Postfächer, Sicherheitsgruppen und Benutzer als Mitglieder hinzufügen. Sie müssen die Rollengruppenmitgliedschaft in diesem Fall aber in jeder Exchange Server 2010-Gesamtstruktur ändern, wenn Sie die Rechte eines Benutzers in mehreren Organisationen ändern wollen. Erstellen Sie ein verknüpftes Postfach, ordnet Exchange die standardmäßige Rollenzuweisungsrichtlinie zu, genauso wie bei lokalen Konten.

16.4.4 Verknüpfte Rollengruppen in unterschiedlichen Gesamtstrukturen verwalten

Verknüpfte Rollengruppen benötigen Sie, wenn Sie zwei Gesamtstrukturen miteinander verbinden wollen (siehe Kapitel 22). Sitzen in einer Gesamtstruktur Administratoren und in der anderen Empfänger, können Sie über verknüpfte Rollengruppen einen Link zwischen einer Rollengruppe in der Exchange-Gesamtstruktur und einer universellen Sicherheitsgruppe in einer fremden Gesamtstruktur erstellen. Verknüpfte Rollengruppen können Sie nur einer fremden universellen Sicherheitsgruppe zuordnen. Eine verknüpfte Rollengruppe enthält keine Mitglieder. Alle Mitglieder der Rollengruppe werden über die fremde universelle Sicherheitsgruppe verwaltet. Sie müssen keine bidirektionale Vertrauensstellung zwischen der Exchange-Gesamtstruktur und der fremden Gesamtstruktur erstellen. Die Exchange-Gesamtstruktur muss der fremden Gesamtstruktur vertrauen, aber die fremde Gesamtstruktur muss der Exchange-Gesamtstruktur nicht vertrauen. Eine verknüpfte Rollengruppe besteht aus zwei Teilen:

1. *Verknüpfte Rollengruppe* – Die verknüpfte Rollengruppe ist ein Container, der die fremde universelle Sicherheitsgruppe mit den der Rollengruppe zugewiesenen Verwaltungsrollenzuweisungen verknüpft.
2. *Fremde universelle Sicherheitsgruppe* – Die fremde universelle Sicherheitsgruppe enthält die Mitglieder, denen Sie die von der verknüpften Rollengruppe bereitgestellten Berechtigungen erteilen wollen.

Exchange fügt die Sicherheits-ID (SID) der fremden universellen Sicherheitsgruppe der verknüpften Rollengruppe hinzu. Fügen Sie der fremden universellen Sicherheitsgruppe Mitglieder hinzu, erhalten diese die von der verknüpften Rollengruppe bereitgestellten Berechtigungen.

INFO

Sie können Standardrollengruppen nicht in eine verknüpfte Rollengruppe ändern. Wollen Sie die gesamte Verwaltung einer Exchange-Gesamtstruktur aus einer fremden Gesamtstruktur ausführen, müssen Sie neue verknüpfte Rollengruppen erstellen.

16.4.5 Erstellen einer verknüpften Verwaltungsrollengruppe

Mit einer verknüpften Verwaltungsrollengruppe können Sie Mitglieder einer universellen Sicherheitsgruppe (USG) in einer fremden Active Directory-Gesamtstruktur berechtigen, eine Exchange Server 2010-Organisation in einer anderen Active Directory-Gesamtstruktur zu verwalten. Um Administratoren einer verknüpften Rollengruppe hinzuzufügen, nehmen Sie diese Benutzerkonten in die universelle Sicherheitsgruppe in der fremden Active Directory-Gesamtstruktur auf. Für verknüpfte Rollengruppen benötigen Sie eine unidirektionale Vertrauensstellung zwischen der Gesamtstruktur, in der sich die verknüpfte Rollengruppe befinden soll, und der fremden Active Directory-Gesamtstruktur, in der sich die Benutzer und die universellen Sicherheitsgruppen befinden. Folgende Informationen sind dazu notwendig:

1. Sie müssen über ein Konto verfügen, das Zugriff auf die fremde Active Directory-Gesamtstruktur hat. Die Daten des Benutzerkontos verwenden Sie in der Option *LinkedCredential* des CMDlets *New-RoleGroup*.
2. Sie müssen den vollqualifizierten Domänennamen (FQDN) eines Domänencontrollers in der fremden Active Directory-Gesamtstruktur kennen. Diese Daten übergeben Sie über die Option *LinkedDomainController* des CMDlets *New-RoleGroup*.
3. Sie müssen den Namen der universellen Sicherheitsgruppe in der fremden Active Directory-Gesamtstruktur kennen. In dieser Gruppe sind die Benutzerkonten Mitglied, die Sie der verknüpften Rollengruppe zuweisen wollen. Diese Daten übergeben Sie mit der Option *LinkedForeignGroup* des CMDlets *New-RoleGroup*. Lesen Sie mehr in Kapitel 22.

Wichtige Grundlagen zu Vertrauensstellungen in Active Directory

Durch Domänen, untergeordnete Domänen und Strukturen gibt es die Möglichkeit, fast unbegrenzt Domänen anbinden zu können, die sich automatisch untereinander vertrauen. In einem Active Directory vertraut jede Domäne jeder anderen Domäne, die Bestandteil der gleichen Gesamtstruktur ist. Es ist nicht mehr notwendig, zahlreiche manuelle Vertrauensstellungen einzurichten.

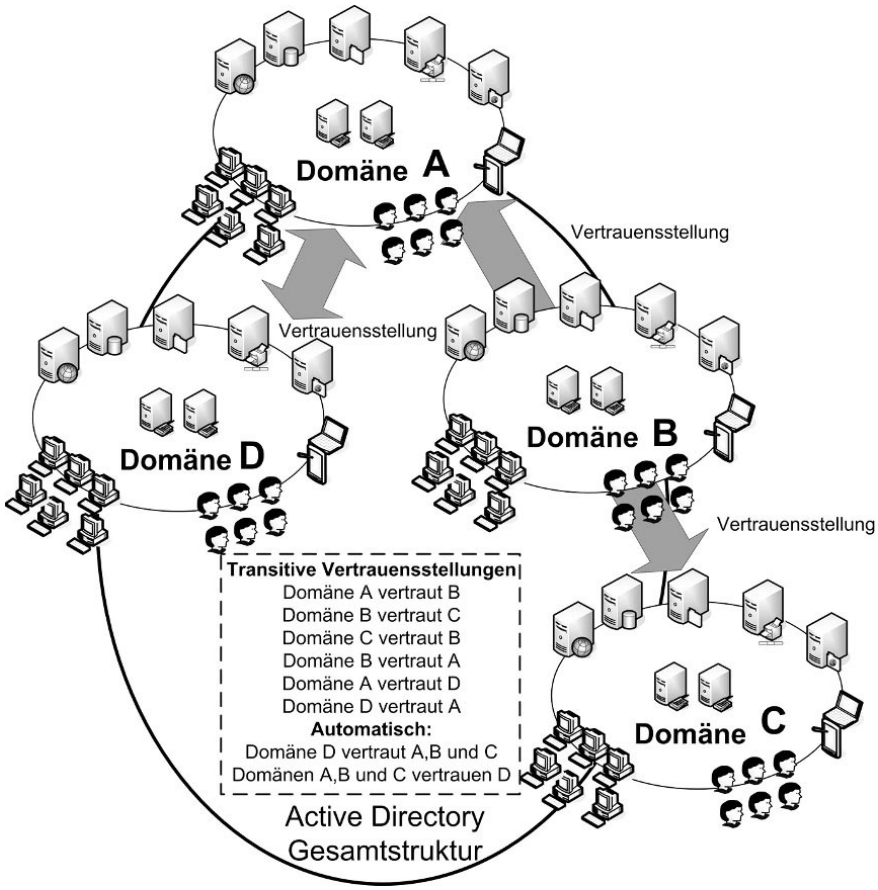


Abbildung 16.33: Transitive Vertrauensstellungen unter Windows Server 2008 (R2) in Active Directory

Auch wenn die Vertrauensstellungen in einer Gesamtstruktur auf den ersten Blick komplex erscheinen, sind sie einfacher als unter Windows NT 4.0, weil diese Vertrauensstellungen automatisch eingerichtet werden. Administratoren müssen keinerlei Maßnahmen vornehmen, damit sich Domänen in einer Gesamtstruktur untereinander vertrauen. Durch diese automatische Verbindung wird die Effizienz von verschiedenen Domänen und Strukturen innerhalb einer Gesamtstruktur deutlich erhöht. In einer Gesamtstruktur werden jedoch nicht automatisch Vertrauensstellungen zwischen allen Domänen eingerichtet, sondern es wird ein gewisses Schema beibehalten:

- Vertrauensstellungen zwischen übergeordneten und untergeordneten Domänen werden immer automatisch eingerichtet. Dieser Typ wird *Untergeordnete Vertrauensstellung* genannt.
- Zusätzlich werden noch Vertrauensstellungen zwischen den Root-Domänen der einzelnen Strukturen eingerichtet. Es gibt jedoch keine Vertrauensstellungen zwischen den Domänen verschiedener Strukturen. Diese vertrauen sich auf

Basis der transitiven Vertrauensstellungen. Der Zugriff auf die Ressourcen wird zwischen Domänen durch transitive Vertrauensstellungen ermöglicht, nicht durch die direkte Verbindung zwischen den Domänen. Die Vertrauensstellungen zwischen den Root-Domänen der verschiedenen Strukturen werden Strukturstamm-Vertrauensstellungen genannt.

Die Verwaltung der Vertrauensstellungen findet mit Hilfe des Snap-Ins *Active Directory-Domänen und -Vertrauensstellungen* statt. Wenn Sie in diesem Snap-In die Eigenschaften einer Domäne aufrufen, finden Sie auf der Registerkarte *Vertrauensstellungen* alle Vertrauensstellungen dieser Domäne und die dazugehörigen Informationen.

Abbildung 16.34: Anzeigen und Verwalten der Vertrauensstellung einer Domäne

Außer den automatisch eingerichteten Vertrauensstellungen können Sie zusätzliche manuelle Vertrauensstellungen einrichten. Für viele Administratoren ist die Richtung der Vertrauensstellungen noch immer gewöhnungsbedürftig, da die einzelnen Begriffe teilweise etwas verwirrend sind. Generell gibt es im Active Directory zunächst zwei verschiedene Arten von Vertrauensstellungen, unidirektionale und bidirektionale. Bei unidirektionalen Vertrauensstellungen vertraut eine Domäne der anderen, aber nicht umgekehrt. Das heißt, die Benutzer der Domäne 1 können zwar auf Ressourcen der Domäne 2 zugreifen, aber die Benutzer in der Domäne 2 nicht auf Ressourcen in der Domäne 1. Dieser Vorgang ist auch umgekehrt denkbar.

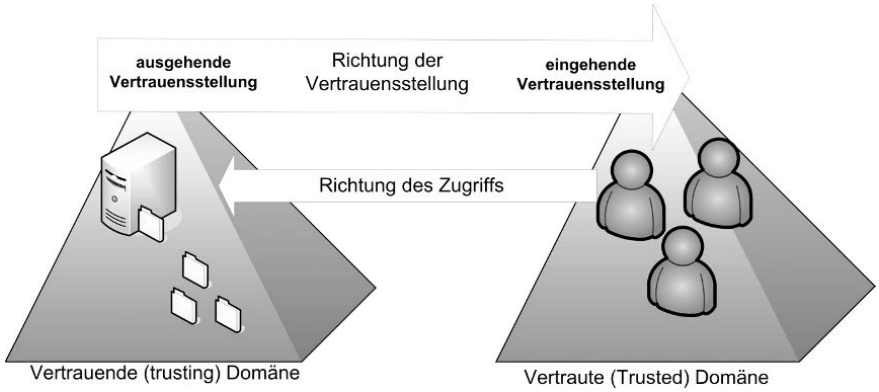


Abbildung 16.35: Vertrauensstellungen in Active Directory verstehen

Weitere Unterscheidungen der Vertrauensstellungen im Active Directory sind ausgehende und eingehende Vertrauensstellungen. Bei ausgehenden Vertrauensstellungen vertraut die Domäne 1 der Domäne 2. Das heißt, Anwender der Domäne 2 dürfen auf Ressourcen der Domäne 1 zugreifen. Bei diesem Vorgang ist die Domäne, von der die Vertrauensstellung ausgeht, die vertrauende (trusting) Domäne. Bei der Domäne mit der eingehenden Vertrauensstellung handelt es sich um die vertraute (trusted) Domäne, in der die Benutzerkonten angelegt sind, die Berechtigungen in der vertrauenden Domäne haben.

Bevor eine Vertrauensstellung erstellt wird, prüft der Server die Eindeutigkeit in folgender Reihenfolge:

- Den NetBIOS-Namen der Domäne
- Den Fully Qualified Domain Name (FQDN) der Domäne
- Die Security Identifier (SID) der Domäne

Diese drei Punkte müssen eindeutig sein, da ansonsten keine Vertrauensstellung erstellt werden kann. Wenn die Domänen-SID identisch ist, muss eine der beiden Domänen erneut installiert werden. Diese Szenarien können eintreffen, wenn eine Domäne von der anderen geklont oder nach dem Installieren des Betriebssystems auf einem Server dieser geklont wurde und anschließend SYSPREP nicht angewendet worden ist. Meistens erhalten Sie in diesem Fall eine Fehlermeldung in der Art »Dieser Vorgang kann nicht auf der aktuellen Domäne ausgeführt werden«.

Varianten der Vertrauensstellungen in Active Directory

Neben den beschriebenen Vertrauensstellungen im Active Directory gibt es verschiedene Möglichkeiten, nachträglich manuelle Vertrauensstellungen einzurichten:

- Externe Vertrauensstellungen, zum Beispiel zu Windows NT 4.0-Domänen oder einzelnen Domänen einer anderen Gesamtstruktur
- Gesamtstrukturübergreifende Vertrauensstellungen (neu seit Windows Server 2003), um die Root-Domänen von zwei unterschiedlichen Gesamt-

strukturen zu verbinden. Alle Domänen der beiden Vertrauensstellungen vertrauen sich anschließend automatisch transitiv.

- Vertrauensstellungen zu einem Nicht-Windows-Kerberos-System
- Vertrauensstellungen zwischen untergeordneten Domänen verschiedener Strukturen, sogenannte Shortcut Trusts oder abkürzende Vertrauensstellungen, sind ebenfalls möglich. Diese Art der Vertrauensstellung wird häufig verwendet, um den Zugriff auf Ressourcen zwischen Domänen zu beschleunigen. In einem Active Directory vertrauen sich alle Domänen innerhalb einer Struktur untereinander. Diese Einrichtung der transitiven Vertrauensstellungen erfolgt automatisch. Es werden allerdings keine Vertrauensstellungen zwischen untergeordneten Domänen verschiedener Strukturen eingerichtet, sondern nur zwischen den Root-Domänen der einzelnen Strukturen. Wenn Anwender auf Daten verschiedener untergeordneter Domänen zugreifen wollen, muss die Authentifizierung daher immer den Weg bis zur Root-Domäne der eigenen Struktur gehen, dann zur Root-Domäne der anderen Struktur und schließlich zur entsprechenden untergeordneten Domäne. Diese Authentifizierung kann durchaus einige Zeit dauern.

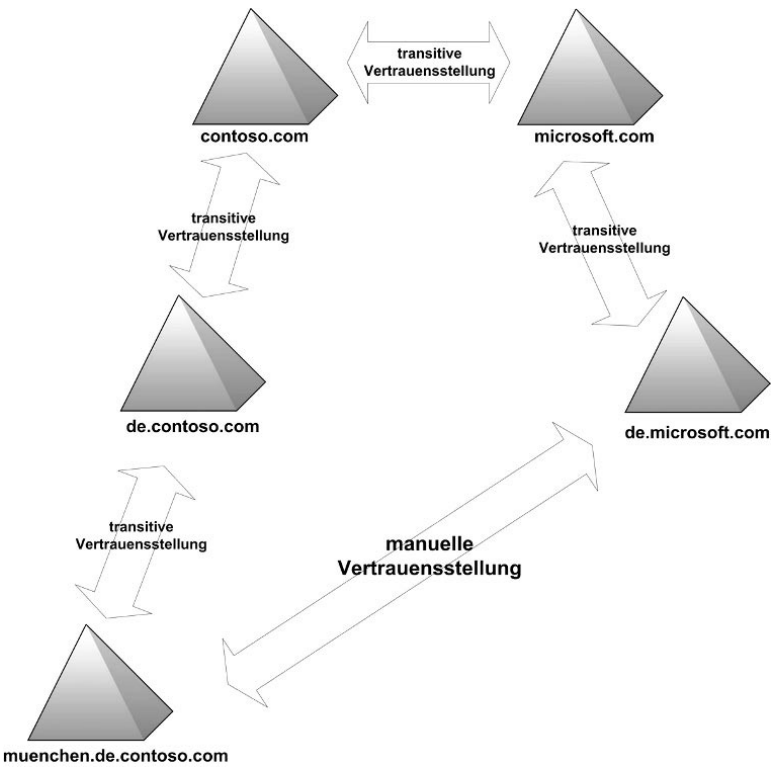


Abbildung 16.36: Pfad der Vertrauensstellungen mit mehreren Domänenstrukturen in einer Gesamtstruktur

Einrichtung einer Vertrauensstellung

Wenn Sie eine Vertrauensstellung zu einer externen Domäne erstellen wollen, sollten Sie zunächst sicherstellen, dass die Namensauflösung zwischen den Domänen fehlerfrei funktioniert. Erst wenn die Namensauflösung stabil und zuverlässig funktioniert, sollten Sie die Vertrauensstellung einrichten. Hilfreich ist auch hier eine WINS-Server-Infrastruktur, wenn Sie außerhalb von Active Directory-Domänen arbeiten.

TIPP

Um eine externe bidirektionale Vertrauensstellung über die Befehlszeile einzurichten, können Sie auch den Befehl *Netdom Trust <vertrauende Domäne> /d:<vertraute Domäne> /Add /Twoway* verwenden.

1. Um eine Vertrauensstellung einzurichten, rufen Sie im Snap-In *Active Directory-Domänen und Vertrauensstellungen* die Eigenschaften der Domäne auf, von der die Vertrauensstellung ausgehen soll.
2. Wechseln Sie in den Eigenschaften auf die Registerkarte *Vertrauensstellungen*.
3. Klicken Sie auf die Schaltfläche *Neue Vertrauensstellung*. Es erscheint der Assistent zur Einrichtung neuer Vertrauensstellungen. Bestätigen Sie das Fenster und geben Sie auf der zweiten Seite den Namen der Domäne an, zu der Sie eine Vertrauensstellung einrichten wollen.

Abbildung 16.37: Aufruf des Assistenten zum Erstellen einer neuen Gesamtstruktur

4. Wenn Sie eine Vertrauensstellung zu einer Active Directory-Domäne aufbauen wollen, verwenden Sie am besten den DNS-Namen, beim Verbindungsaufbau zu einer Windows NT 4.0-Domäne den NetBIOS-Namen.

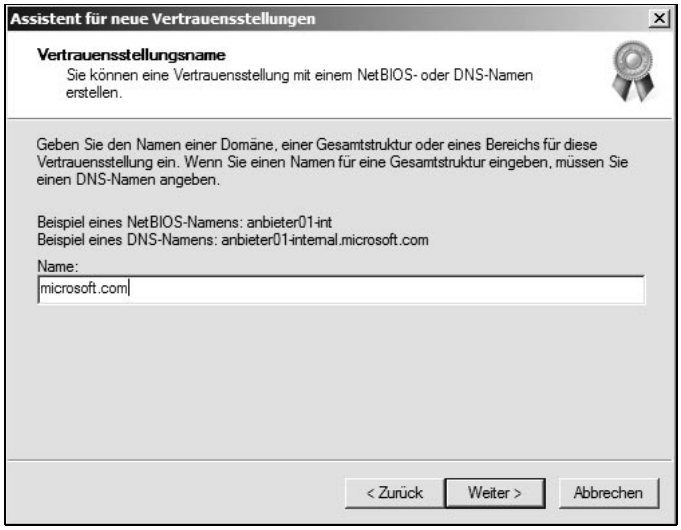


Abbildung 16.38: Festlegen des Namens der Domäne, zu der Sie eine Vertrauensstellung aufbauen wollen

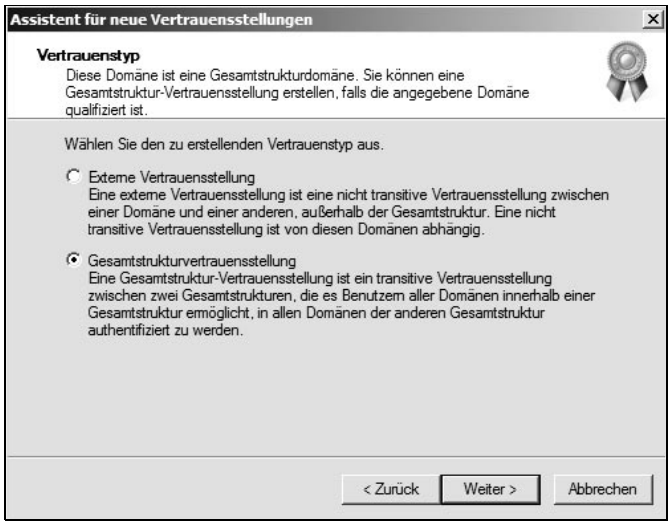


Abbildung 16.39: Erstellen einer neuen Gesamtstrukturvertrauensstellung

5. Nach einem Klick auf *Weiter* überprüft der Assistent, ob er eine Verbindung zur Domäne aufbauen kann. Wollen Sie eine Vertrauensstellung mit einer anderen Gesamtstruktur aufbauen, können Sie im nächsten Fenster diese Option auswählen. Bei einer externen Vertrauensstellung kann eine uni- oder bidirektionale Vertrauensstellung zu einer einzelnen Domäne (in einer separaten Gesamtstruktur) eingerichtet werden. Diese Art einer Vertrauensstellung ist nie transitiv. Eine externe Vertrauensstellung kann notwendig sein, wenn Benutzer Zugriff auf Ressourcen einer anderen Domäne in einer anderen Gesamtstruktur brauchen und keine Gesamtstrukturvertrauensstellung besteht. Dadurch wird eine explizite Vertrauensstellung nur zu dieser einen

Domäne erstellt. Wenn diese Domäne weiteren Domänen vertraut, bleibt der Zugriff auf die weiteren Domänen verwehrt. Gesamtstrukturvertrauensstellungen haben den Vorteil, dass diese eine vollständige Kerberos-Integration zwischen Gesamtstrukturen bieten, und zwar bidirektional und transitiv.

Für die gesamtstrukturübergreifende Vertrauensstellung müssen einige Voraussetzungen geschaffen werden:

- Gesamtstrukturübergreifende Vertrauensstellungen werden nur in Windows Server 2003/2008/2008 R2-Gesamtstrukturen unterstützt.
- Stellen Sie sicher, dass sich die Domänenfunktionsebene und die Gesamtstrukturfunktionsebene im Windows Server 2003-Modus, besser im Windows Server 2008 (R2)-Modus befinden.
- Stellen Sie sicher, dass die Namensauflösung zwischen den Gesamtstrukturen funktioniert. Stellen Sie domänenspezifische Weiterleitungen her und überprüfen Sie, ob sich die Domänencontroller der beiden Gesamtstrukturen untereinander per DNS auflösen können. Alternativ können Sie einen DNS-Server erstellen, der für die Zonen beider Gesamtstrukturen zuständig ist.
- Bei gesamtstrukturübergreifenden Vertrauensstellungen müssen Sie nur die beiden Root-Domänen der Gesamtstrukturen durch eine Vertrauensstellung verbinden. Dann vertrauen sich die Domänen der beiden Gesamtstrukturen transitiv, so dass Sie durch eine Vertrauensstellung mehrere Domänen miteinander verbinden können.

Nach der Auswahl der Art der Vertrauensstellung können Sie festlegen, ob Sie eine unidirektionale oder bidirektionale Vertrauensstellung aufbauen wollen.

- *Bidirektional* – In diesem Fall können sich die Anwender beider Domänen in der jeweils anderen Domäne authentifizieren.
- *Unidirektional:eingehend* – Bei dieser Variante legen Sie fest, dass es sich bei dieser Domäne um die vertraute Domäne der Vertrauensstellung handelt. In diesem Fall können sich die Benutzer dieser Domäne bei der anderen Domäne authentifizieren.
- *Unidirektional:ausgehend* – Bei dieser Vertrauensstellung konfigurieren Sie, dass sich ausschließlich die Anwender der anderen Domäne bei dieser Domäne anmelden dürfen. Die Benutzer dieser Domäne können sich hingegen nicht bei der anderen Domäne anmelden.

Im nächsten Fenster können Sie bei Gesamtstrukturvertrauensstellungen auswählen, ob Sie auch gleich die Vertrauensstellung in der anderen Domäne der anderen Gesamtstruktur erstellen wollen. Diese Option ist selten sinnvoll. Erstellen Sie am besten erst die Vertrauensstellung in der Stammdomäne der einen, dann in der anderen Gesamtstruktur.

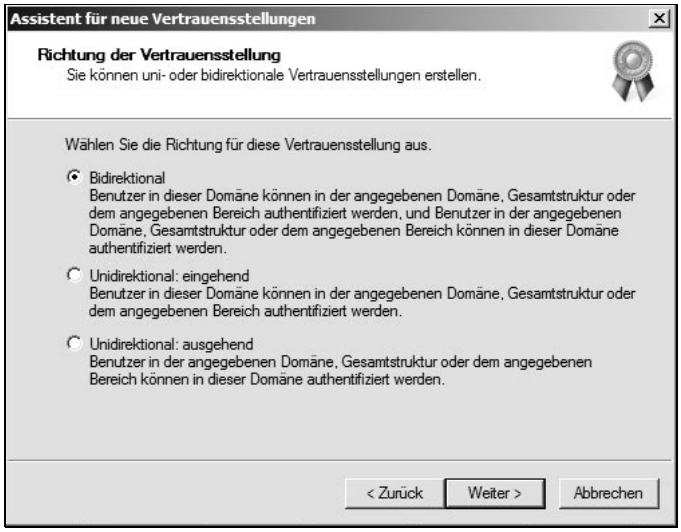


Abbildung 16.40: Festlegen der Richtung von Vertrauensstellungen

Im nächsten Fenster legen Sie den Bereich der Authentifizierung der Vertrauensstellung fest. Die meisten Administratoren verwenden hier die Option *Ausgewählte Authentifizierung* bzw. bei einer Gesamtstrukturvertrauensstellung die Option *Gesamtstrukturweite Authentifizierung*. Dabei können die Anwender der anderen Domäne durch Gruppenmitgliedschaften oder direkte Berechtigungen Zugriff auf die Ressourcen dieser Domäne nehmen. Wenn Sie die Variante *Ausgewählte Authentifizierung* auswählen, müssen Sie für jeden Server, auf den die Anwender der anderen Domäne zugreifen dürfen, in den Sicherheitseinstellungen die Option *Darf authentifizieren* aktivieren. Durch diese Einstellung erhöhen Sie zwar die Sicherheit auf der anderen Seite, aber auch den Verwaltungsaufwand für die Berechtigungsstruktur. Wenn Sie diese Option aktivieren, wird der Zugriff auf die einzelnen Server im Unternehmen für die Benutzer der anderen Domäne verweigert. Erst muss diese Verweigerung für jeden Server mit Aktivierung der Option *Darf authentifizieren* einzeln zurückgenommen werden. Im nächsten Fenster müssen Sie ein Kennwort für die Vertrauensstellung festlegen. Merken Sie sich dieses Kennwort, da Sie es unter Umständen später wieder für die Verifizierung verwenden müssen.

Verbinden Sie zwei Gesamtstrukturen durch eine gesamtstrukturübergreifende Vertrauensstellung, sollten Sie sicherstellen, dass möglichst alle Domänennamen eindeutig sind. Sobald in den Gesamtstrukturen doppelte DNS- oder NetBIOS-Namen auftreten, können diese Domänen nicht auf Ressourcen der jeweils anderen Gesamtstruktur zugreifen.

Wählen Sie im nächsten Fenster aus, ob Sie die Vertrauensstellung überprüfen wollen. Wenn Sie eine Vertrauensstellung zu einer Windows NT 4.0-Domäne einrichten, sollten Sie zunächst die Vertrauensstellung auf der Seite der Windows NT

4.0-Domäne einrichten, bevor Sie in den Eigenschaften der Vertrauensstellung in der Active Directory-Domäne die Überprüfung starten. Erst wenn eine Vertrauensstellung als aktiv verifiziert wurde, können Sie auch sicher sein, dass Anwender auf die Ressourcen zugreifen können. Wenn die Erstellung einer Vertrauensstellung nicht funktioniert, liegt es fast immer an Problemen mit der Namensauflösung oder entsprechenden Berechtigungen. Unter Umständen müssen Sie sich bei der Überprüfung der Vertrauensstellung erneut in der anderen Domäne authentifizieren. Nach der erfolgreichen Überprüfung erhalten Sie eine Meldung, dass die Vertrauensstellung aktiv ist. Wenn in Ihrer Gesamtstruktur mehrere Strukturen eingesetzt werden, können Sie in der gesamtstrukturübergreifenden Vertrauensstellung festlegen, welche Namensräume bzw. Strukturen diese Vertrauensstellung nutzen kann. Sie können einzelne Namensräume aus dem Routing entfernen oder später über die Eigenschaften der Vertrauensstellung hinzufügen. Für die Verwaltung dieser verschiedenen Strukturen verwenden Sie in den Eigenschaften der Vertrauensstellung die Registerkarte *Namensuffixrouting*.

Erstellen einer verknüpften Verwaltungsrollengruppe in der Exchange-Verwaltungsshell

Gehen Sie zum Erstellen einer verknüpften Verwaltungsrollengruppe und zum Zuordnen von Verwaltungsrollen folgendermaßen vor:

1. Speichern Sie die Anmeldeinformationen für die fremde Active Directory-Gesamtstruktur in einer Variablen, indem Sie den folgenden Befehl in der Exchange-Verwaltungshell eingeben: *$ForeignCredential = Get-Credential*
2. Erstellen Sie die verknüpfte Verwaltungsrollengruppe mit folgender Syntax: *New-RoleGroup <Verwaltungsrollengruppe> -LinkedForeignGroup <Name der universellen Gruppe> -LinkedDomainController <FQDN eines Domänencontrollers in der fremdem Gesamtstruktur> -LinkedCredential $ForeignCredential -Roles <Verwaltungsrollen, die Sie zuweisen wollen, durch Komma getrennt>*
3. Fügen Sie mit der Konsole *Active Directory-Benutzer und -Computer* in der fremden AD-Gesamtstruktur die Mitglieder der universellen Sicherheitsgruppe hinzu.

Ändern der universellen Sicherheitsgruppe einer verknüpften Verwaltungsrollengruppe

Sie können die universelle Sicherheitsgruppe ändern, die der verknüpften Verwaltungsrollengruppe zugeordnet ist. Sie verwenden dazu das CMDlet *Set-RoleGroup*. Gehen Sie zum Ändern folgendermaßen vor:

1. Speichern Sie die Anmeldeinformationen für die fremde Active Directory-Gesamtstruktur in einer Variablen, indem Sie den folgenden Befehl in der Exchange-Verwaltungshell eingeben: *$ForeignCredential = Get-Credential*

2. Ändern Sie die verknüpfte Verwaltungsrollengruppe mit folgender Syntax ab: *Set-RoleGroup < Verwaltungsrollengruppe > -LinkedForeignGroup < Name der neuen universellen Gruppe > -LinkedDomainController < FQDN eines Domänencontrollers in der fremdem Gesamtstruktur > -LinkedCredential $ForeignCredential -Roles < Verwaltungsrollen, die Sie zuweisen wollen, durch Komma getrennt >*
3. Fügen Sie mit der Konsole *Active Directory-Benutzer und -Computer* die Mitglieder der fremden universellen Sicherheitsgruppe hinzu.

Standard-Verwaltungsrollengruppen in verknüpfte Verwaltungsrollengruppen kopieren

Sie können die standardmäßig angelegten Verwaltungsrollengruppen in Exchange Server 2010 über Kopien als verknüpfte Verwaltungsrollengruppen neu erstellen. Exchange übernimmt bei diesem Vorgang alle Verwaltungsrollen und Verwaltungsbereiche:

1. Erstellen Sie in der fremden Gesamtstruktur eine universelle Sicherheitsgruppe für jede Verwaltungsrollengruppe, die Sie mit den einzelnen neuen Verwaltungsrollengruppen verknüpfen wollen.
2. Speichern Sie die Anmeldeinformationen für die fremde Active Directory-Gesamtstruktur in einer Variablen. Diesen Schritt müssen Sie nur einmal durchführen, da Sie die Variable auch für die anderen Gruppen verwenden können*: $ForeignCredential = Get-Credential*.
3. Zeigen Sie alle Verwaltungsrollengruppen an: *Get-RoleGroup*.
4. Gehen Sie für jede Verwaltungsrollengruppe, mit Ausnahme der Verwaltungsrollengruppe *Organisationsverwaltung*, folgendermaßen vor. Wie Sie die Verwaltungsrollengruppe *Organisationsverwaltung* als verknüpfte Verwaltungsrollengruppe erstellen, zeigen wir Ihnen im Anschluss an diesen Abschnitt.
   - *$RoleGroup = Get-RoleGroup < Name der Verwaltungsrollengruppe >*
   - *New-RoleGroup »< Verwaltungsrollengruppe > – Verknüpft« -LinkedForeignGroup < Name der universellen Gruppe > -LinkedDomainController < FQDN eines Domänencontrollers in der fremden Gesamtstruktur > -LinkedCredential $ForeignCredential -Roles $RoleGroup.Roles*
5. Wiederholen Sie Schritt 4 für jede Verwaltungsrollengruppe, die Sie als verknüpfte Verwaltungsrollengruppe erstellen wollen.

Um die Verwaltungsrollengruppe *Organisationsverwaltung* als verknüpfte Rollengruppe zu erstellen, müssen Sie etwas anders vorgehen, da diese Verwaltungsrollengruppe über die höchsten Rechte in der Exchange-Organisation verfügt:

1. Erstellen Sie in der fremden Gesamtstruktur eine universelle Sicherheitsgruppe, die Sie mit der Verwaltungsrollengruppe *Organisationsverwaltung* verknüpfen wollen.

2. Speichern Sie die Anmeldeinformationen für die fremde Active Directory-Gesamtstruktur in einer Variablen: *$ForeignCredential = Get-Credential*
3. Speichern Sie alle Rollenzuweisungen der Verwaltungsrollengruppe *Organisationsverwaltung* in einer Variablen: *$OrgMgmt = Get-RoleGroup »Organization Management«*
4. Erstellen Sie die verknüpfte Rollengruppe *Organisationsverwaltung* und fügen Sie die entsprechenden Verwaltungsrollen hinzu: *New-RoleGroup »Organization Management – Verknüpft« -LinkedForeignGroup <Name der universellen Sicherheitsgruppe> -LinkedDomainController <Name eines DCs in der fremden Gesamtstruktur> -LinkedCredential $ForeignCredential -Roles $OrgMgmt.Roles*
5. Entfernen Sie alle regulären Zuweisungen zwischen der verknüpften Rollengruppe *Organisationsverwaltung* und den *My**-Endbenutzerrollen: *Get-ManagementRoleAssignment -RoleAssignee »Organization Management – Verknüpft« -Role My* | Remove-ManagementRoleAssignment*
6. Fügen Sie delegierende Rollenzuweisungen zwischen der verknüpften Rollengruppe *Organisationsverwaltung* und allen Verwaltungsrollen hinzu: *Get-ManagementRole | New-ManagementRoleAssignment -SecurityGroup »Organization Management – Verknüpft« -Delegating*

16.5 Zuweisungsrichtlinien für Verwaltungsrollen

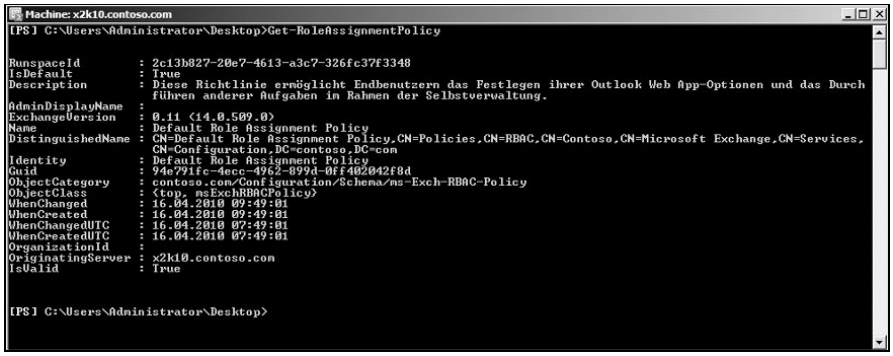
Eine Richtlinie für die Verwaltungsrollenzuweisung ist eine Sammlung aus einer oder mehreren Verwaltungsrollen, mit denen Endbenutzer ihre eigene Postfach- und Verteilergruppenkonfiguration verwalten können. Mit Rollenzuweisungsrichtlinien können Sie steuern, welche Konfigurationseinstellungen Benutzer für Postfächer und Verteilergruppen ändern können. Die Richtlinie für die Verwaltungsrollenzuweisung ist ein spezielles Objekt in Exchange Server 2010. Die Kombination aller Rollen in einer Rollenzuweisungsrichtlinie definiert, was der Benutzer in seinem Postfach oder in der Verteilergruppe verwalten darf. Eine Verwaltungsrollenzuweisung ist eine Verknüpfung zwischen einer Verwaltungsrolle und einer Rollenzuweisungsrichtlinie. Bei Verwaltungsrollen handelt es sich um eine Gruppe von Verwaltungsrolleneinträgen. Ein Verwaltungsrolleneintrag ist ein CMDlet, Skript oder eine spezielle Berechtigung.

INFO

Sie können nur Endbenutzerverwaltungsrollen mit Rollenzuweisungsrichtlinien verwenden.

Verwaltungsrolleneinträge sind die einzelnen Einträge in einer Verwaltungsrolle, die festlegen, welche CMDlets für die Verwaltungsrolle und die Rollengruppe zur Verfügung stehen. Jeder Rolleneintrag besteht aus einem CMDlet. Mit dem CMDlet *Get-RoleAssignmentPolicy* lassen Sie sich alle vorhandenen Zuweisungsrichtlinien anzeigen.

Abbildung 16.41: Anzeigen der Zuweisungsrichtlinien einer Exchange-Organisation

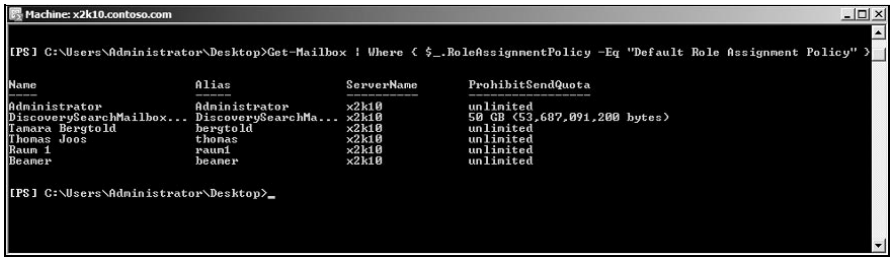


Wollen Sie eine Liste bestimmter Eigenschaften für alle Zuweisungsrichtlinien anzeigen, verwenden Sie die Option |*ft*. Wie immer bei dieser Option, können Sie durch Eingabe von *Get-RoleAssignmentPolicy | ft <Eigenschaft 1>, <Eigenschaft 2>,…* weitere Optionen detaillierter anzeigen. Mit dem Befehl *Get-RoleAssignmentPolicy | Format-Table Name, IsDefault* lassen Sie den Namen der Zuweisungsrichtlinien festlegen, die als Standard festgelegt sind.

Wollen Sie alle Postfächer anzeigen, denen eine bestimmte Zuweisungsrichtlinie zugeordnet ist, verwenden Sie das CMDlet *Get-Mailbox* und geben Sie das Ergebnis an das CMDlet *Where* weiter. Filtern Sie die Daten mit dem CMDlet *Where*, damit die Exchange-Verwaltungsshell nur die Postfächer anzeigt, bei denen die Eigenschaft *RoleAssignmentPolicy* den Wert der Zuweisungsrichtlinie enthält, nach der Sie filtern wollen. Verwenden Sie die folgende Syntax:

Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq »<Name der Zuweisungsrichtlinie>« }

Abbildung 16.42: Anzeigen aller Postfächer, denen eine bestimmte Zuweisungsrichtlinie zugeordnet ist



Sie können sich die Zulassungsrichtlinie, die einem Benutzerkonto angepasst ist, nach der Installation von Service Pack 1 für Exchange Server 2010 auch in den Eigenschaften des Benutzerkontos in der Exchange-Verwaltungskonsole anzeigen lassen und die Zuweisung ändern. Rufen Sie dazu die Registerkarte *Postfacheinstellungen* auf.

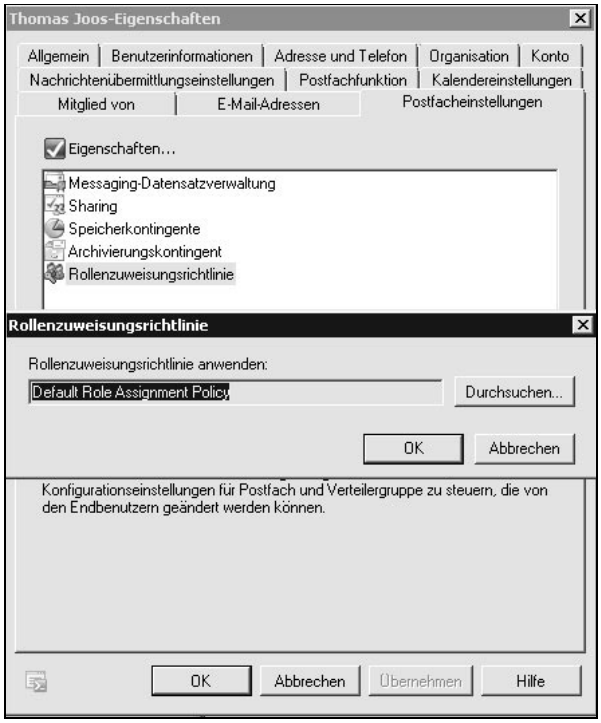


Abbildung 16.43: Ändern der Rollenzuweisungsrichtlinie für Empfänger

16.5.1 Standard-Rollenzuweisungsrichtlinie

Eine Standard-Rollenzuweisungsrichtlinie ist eine Rollenzuweisungsrichtlinie, die Exchange neuen Postfächern zuweist. Exchange Server 2010 verfügt über eine Standard-Rollenzuweisungsrichtlinie, die den Empfängern häufig verwendete Berechtigungen zuteilt. Sie können die Standardberechtigungen in der Standard-Rollenzuweisungsrichtlinie ändern, indem Sie Verwaltungsrollen hinzufügen oder entfernen. Wollen Sie die Standard-Rollenzuweisungsrichtlinie durch eine eigene Rollenzuweisungsrichtlinie ersetzen, verwenden Sie das CMDlet *Set-RoleAssignmentPolicy*, um einen neuen Standard auswählen.

INFO

Ändern Sie die Standard-Rollenzuweisungsrichtlinie, weist Exchange den Postfächern, denen die Standard-Rollenzuweisungsrichtlinie zugewiesen wurde, nicht automatisch die neue Standard-Rollenzuweisungsrichtlinie zu. Wollen Sie Postfächer aktualisieren, müssen Sie das CMDlet *Set-Mailbox* mit der Option *RoleAssignmentPolicy* verwenden. Eine explizite Rollenzuweisungsrichtlinie ist eine Richtlinie, die Sie einem Postfach mit der Option *RoleAssignmentPolicy* den CMDlets *New-Mailbox*, *Set-Mailbox* oder *Enable-Mailbox* manuell zuweisen. Weisen Sie eine explizite Rollenzuweisungsrichtlinie zu, wird die neue Richtlinie sofort wirksam und ersetzt die vorher zugewiesene explizite Rollenzuweisungsrichtlinie.

Sie können die Standard-Zuweisungsrichtlinie ändern, die Exchange neuen Postfächern automatisch zuordnet. Dazu verwenden Sie den Befehl:

Set-RoleAssignmentPolicy < Zuweisungsrichtlinie > -IsDefault

Neuen Postfächern weist Exchange immer die standardmäßige Zuweisungsrichtlinie zu, auch dann, wenn dieser keine Verwaltungsrollen zugewiesen sind.

16.5.2 Hinzufügen, Entfernen und Verwalten von Rollenzuweisungsrichtlinien

Ein Postfach kann nur eine Rollenzuweisungsrichtlinie gleichzeitig verwenden. Wollen Sie bestimmten Benutzern andere Rechte zuweisen, müssen Sie für diese Postfächer eine eigene Rollenzuweisungsrichtlinie erstellen und diese zuweisen. Nachdem Sie eine neue Rollenzuweisungsrichtlinie erstellt haben, weisen Sie der Rollenzuweisungsrichtlinie die gewünschten Verwaltungsrollen zu. Anschließend weisen Sie die Rollenzuweisungsrichtlinie den gewünschten Postfächern zu. Sie können Verwaltungsrollen auch nachträglich noch hinzufügen und entfernen oder eine andere Rollenzuweisungsrichtlinie als Standard auswählen.

Hinzufügen einer Zuweisungsrichtlinie

Wollen Sie die Berechtigungen anpassen, die einer Gruppe von Endbenutzern zugewiesen sind, erstellen Sie eine neue benutzerdefinierte Zuweisungsrichtlinie für Verwaltungsrollen. Nachdem Sie eine neue Zuweisungsrichtlinie erstellt haben, weisen Sie dieser die Verwaltungsrollen zu und ordnen die Zuweisungsrichtlinie anschließend Benutzern zu. Um eine neue Zuweisungsrichtlinie zu erstellen, verwenden Sie den Befehl:

New-RoleAssignmentPolicy < Name der neuen Zuweisungsrichtlinie >

Erstellen Sie eine neue Zuweisungsrichtlinie und wollen Sie diese neuen Postfächern als Standardrichtlinie zuweisen, verwenden Sie den Befehl:

New-RoleAssignmentPolicy < Name der neuen Zuweisungsrichtlinie > -IsDefault

Allerdings übernehmen nur neue Postfächer diese Zuweisungsrichtlinie als Standard, bereits vorhandene Postfächer übernehmen diese nicht. Nach der Installation von Service Pack 1 für Exchange Server 2010 können Sie Rollenzuweisungsrichtlinien auch in der Exchange-Systemsteuerung anpassen. Sie finden diese Einstellungen über Benutzerrollen. Sie können neue Richtlinien erstellen und Einstellungen bestehender Richtlinien ändern.

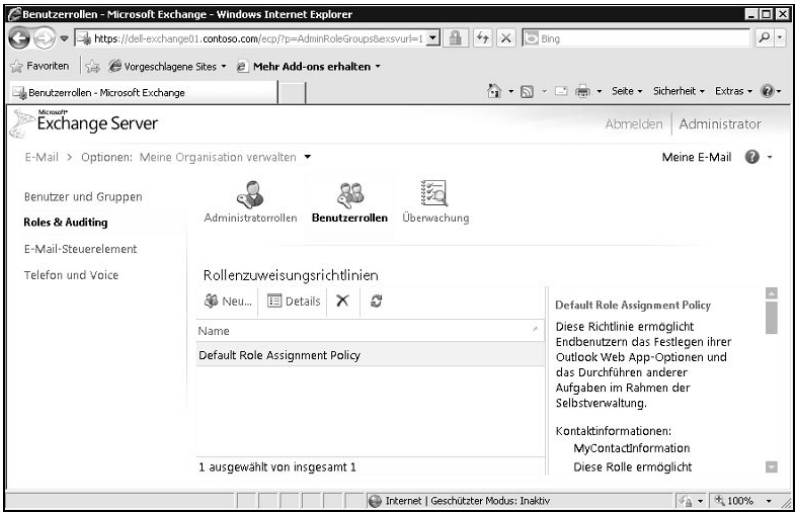


Abbildung 16.44: Verwalten von Zuweisungsrichtlinien

Entfernen einer Zuweisungsrichtlinie

Sie müssen vor dem Entfernen allen Benutzern eine andere Zuweisungsrichtlinie zuordnen. Außerdem müssen Sie alle Verwaltungsrollenzuweisungen der Zuweisungsrichtlinie entfernen. Zum Entfernen verwenden Sie den Befehl:

Remove-RoleAssignmentPolicy <Zuweisungsrichtlinie>

Über die Exchange-Systemsteuerung können Sie Zuweisungsrichtlinien löschen.

Ändern der Zuweisungsrichtlinie für Postfächer

Die Zuweisungsrichtlinien, die Postfächern zugeordnet sind, lassen sich nachträglich ändern. Zum Ändern verwenden Sie das CMDlet *Set-Mailbox* mit der Syntax:

Set-Mailbox <Postfach oder Name> -RoleAssignmentPolicy <Zuweisungsrichtlinie>

Wollen Sie die Zuweisungsrichtlinie für alle Postfächer ändern, denen eine bestimmte Zuweisungsrichtlinie zugewiesen ist, verwenden Sie folgenden Befehl:

Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq »<Alte Zuweisungsrichtlinie>« } | Set-Mailbox -RoleAssignmentPolicy <Neue Zuweisungsrichtlinie>

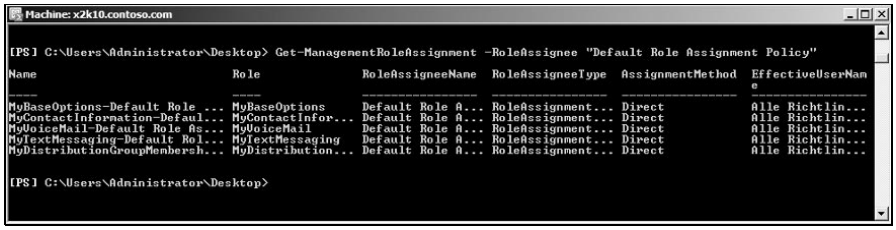
Verwenden Sie am Ende des Befehls die Option *WhatIf*, können Sie sich anzeigen lassen, was der Befehl durchführen würde, ohne die Änderungen tatsächlich auszuführen.

16.5.3 Hinzufügen, Entfernen und Anzeigen von Verwaltungsrollen zu einer Zuweisungsrichtlinie

Eine Zuweisungsrichtlinie hat erst dann eine richtige Auswirkung, wenn Sie dieser auch Verwaltungsrollen zuweisen. Dazu verwenden Sie folgenden Befehl:

New-ManagementRoleAssignment -Name <Name der Zuweisung> -Role <Verwaltungsrolle> -Policy <zuweisungsrichtlinie>

Abbildung 16.45: Anzeigen der Verwaltungsrollen einer Zuweisungsrichtlinie



Zum Entfernen der Rollenzuweisung aus der Zuweisungsrichtlinie verwenden Sie folgende Syntax.

Remove-ManagementRoleAssignment <Name der Rollenzuweisung>

Nach der Installation von Service Pack 1 für Exchange Server 2010 können Sie die Exchange-Systemsteuerung zum Entfernen von Rollenzuweisungen aus einer Zuweisungsrichtlinie verwenden. Klicken Sie dazu auf *Benutzerrollen* und öffnen Sie die Details der Richtlinie. Anschließend können Sie festlegen, welche Rechte die Anwender haben sollen.

Mit dem CMDlet *Get-ManagementRoleAssignment* lassen Sie sich alle zugewiesenen Verwaltungsrollen einer Zuweisungsrichtlinie anzeigen. Mit *Get-RoleAssignmentPolicy* lassen Sie sich wiederum die Zuweisungsrichtlinien in der Organisation anzeigen. Um die Verwaltungsrollen für eine Zuweisungsrichtlinie anzuzeigen, verwenden Sie den Befehl:

Get-ManagementRoleAssignment -RoleAssignee <Zuweisungsrichtlinie>

Um alle Verwaltungsrollen anzuzeigen, die der Standard-Rollenzuweisungsrichtlinie zugewiesen sind, verwenden Sie den Befehl

Get-ManagementRoleAssignment -RoleAssignee »Default Role Assignment Policy«

Die folgende Tabelle zeigt benutzerspezifische Verwaltungsrollen in Exchange Server 2010.

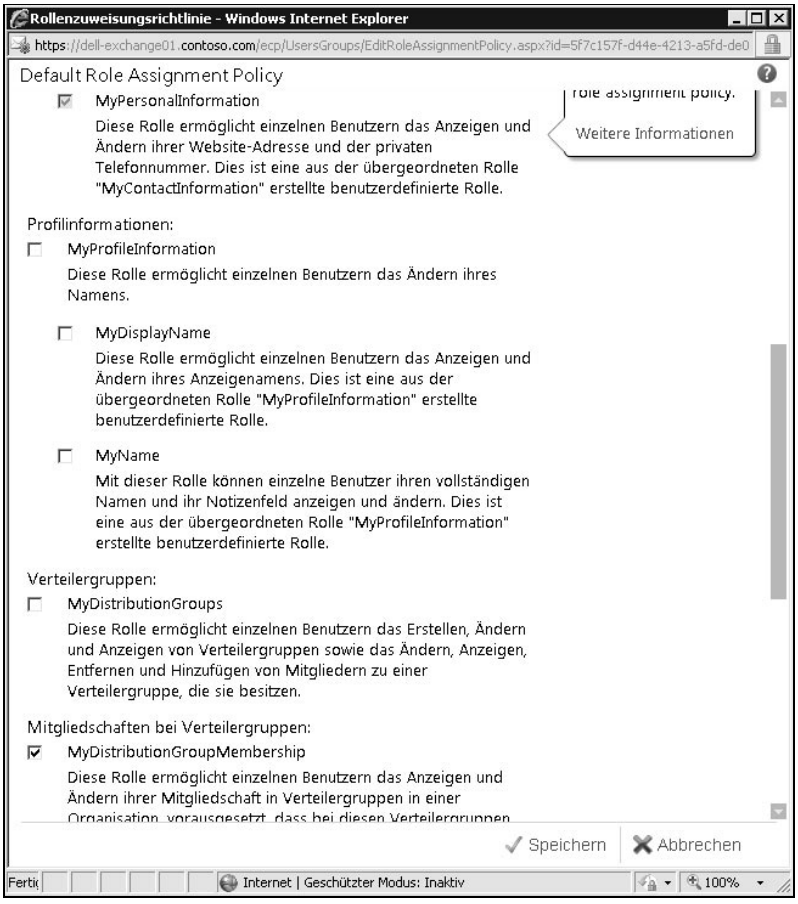


Abbildung 16.46: Entfernen oder Hinzufügen von Rechten zu einer Zuweisungsrichtlinie

Rollentyp	Beschreibung	Gültigkeitsbereich
MyBaseOptions	Basiskonfiguration des eigenen Postfachs und die Einstellungen anzeigen und ändern können	Postfach
MyContactInformation	Eigene Kontaktinformationen ändern, zum Beispiel Adresse und Telefonnummern	Postfach
MyDistributionGroupMembership	Mitgliedschaft in Verteilergruppen in einer Organisation anzeigen und ändern, sofern die Bearbeitung der Mitgliedschaft für diese Verteilergruppen gestattet ist	Postfach
MyDistributionGroups	Verteilergruppen erstellen, ändern und anzeigen	Postfach
MyMailSubscriptions	Einstellungen der E-Mail-Abonnements und Standardeinstellungen für Nachrichtenformate und Protokollfunktion anzeigen und ändern	Postfach
MyProfileInformation	Ändern des eigenen Namens	Postfachs

Tabelle 16.4: Verwalten von benutzerdefinierten Rollentypen

Tabelle 16.4: Verwalten von benutzerdefinierten Rollentypen (Forts.)

Rollentyp	Beschreibung	Gültigkeitsbereich
MyRetentionPolicies	Eigene Aufbewahrungstags anzeigen und ändern	Postfach
MyTextMessaging	Textnachrichteneinstellungen erstellen, anzeigen und ändern	Postfach
MyVoiceMail	Voicemail-Einstellungen anzeigen und ändern	Postfach

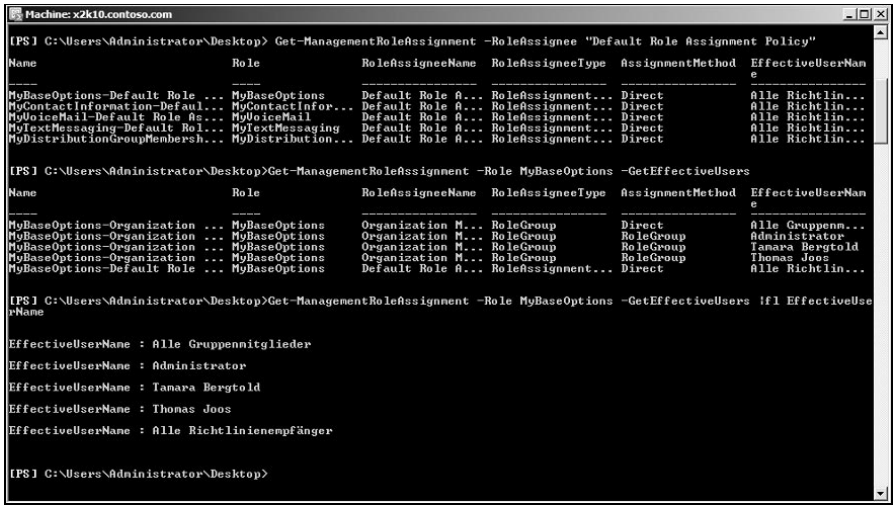
16.6 Anzeigen der gesetzten Berechtigungen

Die meisten Berechtigungen vergeben Unternehmen sicherlich auf Basis der Mitgliedschaft in Verwaltungsrollengruppen oder durch das Zuordnen von Zuweisungsrichtlinien zu Endbenutzern. Mit der Option *GetEffectiveUsers* des CMDlets *Get-ManagementRoleAssignment* können Sie anzeigen, welchen Benutzern die Berechtigungen einer Verwaltungsrolle gewährt sind. Dabei ist es unerheblich, ob diese Rechte über Rollengruppen, Verwaltungsrichtlinien oder universelle Sicherheitsgruppen zugeordnet sind. Die Option *GetEffectiveUser* zeigt allerdings keine Benutzer auf, die Mitglieder einer verknüpften fremden Rollengruppe sind. Hier zeigt die Shell alle verknüpften Gruppenmitglieder an. Zur Anzeige verwenden Sie den Befehl

Get-ManagementRoleAssignment -Role <Verwaltungsrolle> -GetEffectiveUsers

Mit dem Befehl *Get-ManagementRoleAssignment -Role <Verwaltungsrolle> -GetEffectiveUsers |fl EffectiveUserName* lassen Sie sich nur die Benutzernamen anzeigen.

Abbildung 16.47: Anzeigen der effektiven Benutzer, denen eine bestimmte Verwaltungsrolle zugewiesen ist



Wollen Sie einen bestimmten Benutzer anzeigen, dem Sie über eine Verwaltungsrolle Berechtigungen zugeteilt haben, verwenden Sie das CMDlet *Get-ManagementRoleAssignment* zum Abrufen einer Liste aller effektiven Benutzer und geben Sie die Liste an das CMDlet *Where* weiter. Das CMDlet *Where* filtert die Ausgabe und zeigt nur die gewünschten Benutzer an. Verwenden Sie die folgende Syntax:

Get-ManagementRoleAssignment -Role <Verwaltungsrolle> -GetEffectiveUsers | Where { $_.EffectiveUserName -Eq »<Name des Benutzers>« }

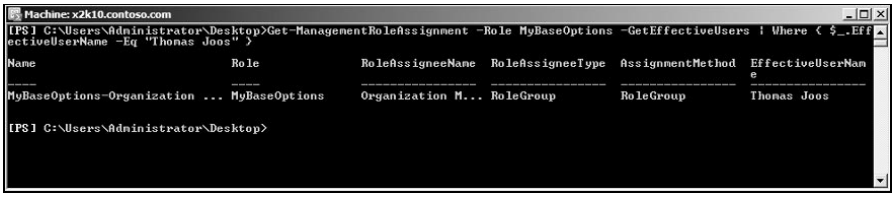


Abbildung 16.48: Anzeigen bestimmter Benutzer, denen eine bestimmte Verwaltungsrolle zugewiesen ist

Wollen Sie alle Verwaltungsrollen anzeigen, die Sie einem Benutzer zugewiesen haben, verwenden Sie ebenfalls das CMDlet *Get-ManagementRoleAssignment* zum Anzeigen aller effektiven Benutzer und filtern mit dem CMDlet *Where* die Anzeige:

Get-ManagementRoleAssignment -GetEffectiveUsers | Where { $_.EffectiveUserName -Eq »<Name des Benutzers>« }

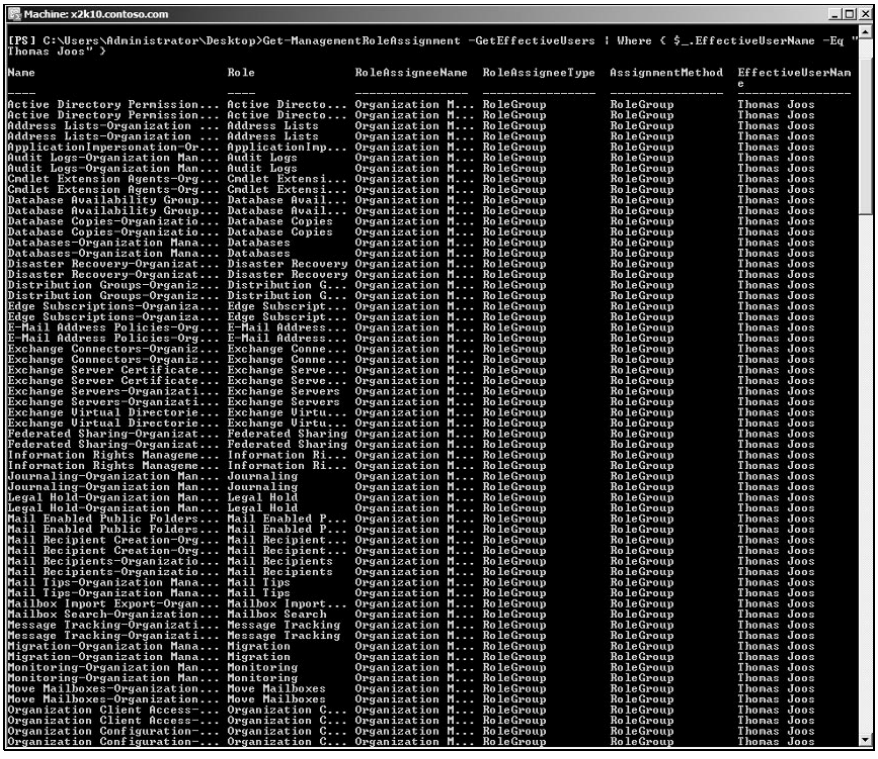
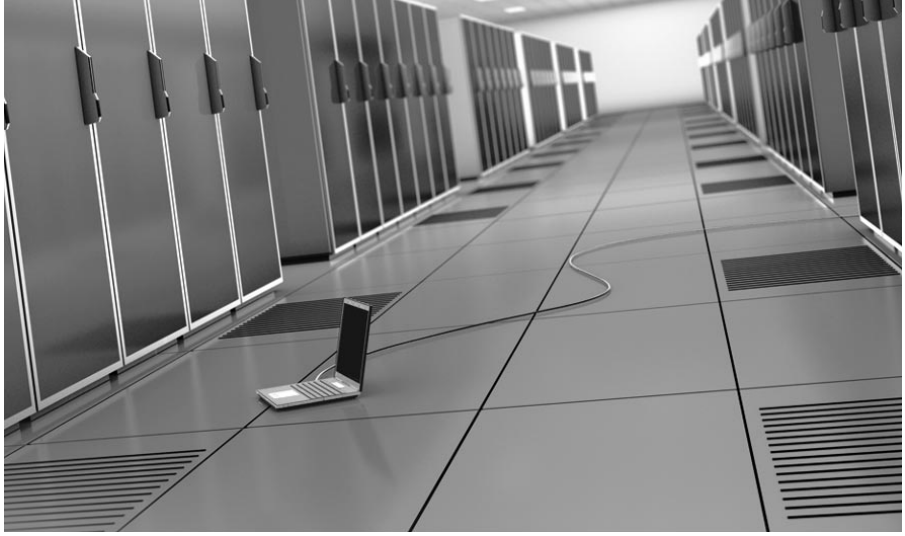


Abbildung 16.49: Anzeigen aller Verwaltungsrollen, die einem Benutzer zugewiesen sind

Die Ausgabe des CMDlets *Get-ManagementRoleAssignment* lässt sich mit der Option *|fl* oder *|ft <Eigenschaft 1>, <Eigenschaft 2>,…* noch weiter filtern. Dazu stehen vor allem folgende Eigenschaften zur Filterung zur Verfügung:

- *EffectiveUserName* – Name des Benutzers
- *Role* – Zeigt die Rolle an, über welche die Berechtigungen zugeteilt sind.
- *RoleAssigneeName* – Bezeichnung der Rollengruppe, Zuweisungsrichtlinie oder universellen Sicherheitsgruppe, die der Rolle zugewiesen ist und den Benutzer in der Eigenschaft *EffectiveUserName* enthält
- *RoleAssigneeType* – Zeigt an, ob die Rollenzuweisung einer Rollengruppe, einer Zuweisungsrichtlinie, einer universellen Sicherheitsgruppe oder einem Benutzer zugeordnet ist.
- *AssignmentMethod* – Zeigt an, ob es sich um eine direkte oder indirekte Zuweisung zwischen der Rolle und dem Rollenempfänger handelt.
- *CustomRecipientWriteScope* – Zeigt den benutzerdefinierten Empfängerschreibbereich an.
- *CustomConfigWriteScope* – Zeigt den benutzerdefinierten Konfigurationsschreibbereich an.



Kapitel 17
Datensicherung

Die Datensicherung eines Exchange Servers gehört sicherlich zu den wichtigsten Aufgaben eines Exchange-Administrators. Da die Kommunikation mithilfe von E-Mails in Unternehmen eine immer größere Rolle spielt, verlassen sich Ihre Benutzer immer mehr auf das System. Schon vor dem Ausfall eines Servers oder einer Exchange-Datenbank sollten Sie rechtzeitig einen Plan ausgearbeitet haben und testen, was bei einer Wiederherstellung zu tun ist. Auch das Zurücksichern einzelner E-Mails wird von vielen Benutzern inzwischen vorausgesetzt. Bei der Sicherung eines Exchange Servers müssen Sie immer Murphys Gesetz beachten: *»Was schiefgehen kann, geht schief«*, und zwar zum ungünstigsten Zeitpunkt. Exchange Server 2010 setzt bei der Sicherung vollständig auf den *Schattenkopiedienst* (*VSS*). Auch das Datensicherungsprogramm in Windows Server 2008 und Windows Server 2008 (R2) lässt eine Sicherung von Exchange-Datenbanken zu und überprüft dabei auch die Konsistenz der Datenbank.

17.1 Einführung in die Datensicherung von Exchange Server 2010

Es gibt zwei verschiedene Varianten der Datensicherung: die *Online-Sicherung* und die *Offline-Sicherung*. Da auch Exchange Server 2010 auf einer ESE-Datenbank aufbaut (siehe Kapitel 7), die ständig online ist, benötigen Sie zur Sicherung der Datenbank spezielle Exchange-Agenten, da Sie keinen Zugriff auf die Datendateien erhalten. Durch die verschiedenen neuen Serverrollen in Exchange Server 2010 besteht die Notwendigkeit, dass Sie auf verschiedenen Exchange-Servern, abhängig von den installierten Rollen, unterschiedliche Daten sichern soll-

ten, die für die Funktion der Exchange-Organisation eine wesentliche Rolle spielen. Natürlich sind auch weiterhin die Exchange-Datenbanken und die damit verbundenen **.edb*-Dateien auf Mailbox-Servern die wichtigsten Daten, die Sie sichern sollten.

Die wichtigsten Daten befinden sich auf den Mailbox-Servern. Hier liegen die Inhalte der Postfächer und öffentlichen Ordner, die Exchange-Datenbanken. Diese Daten sind in einzelnen *.edb-Dateien gespeichert, für jede Postfachdatenbank gibt es eine solche Datei. Jeder Datenbank ist eine *.edb-Datei zugeordnet. Alle Änderungen an der Datenbank speichert Exchange zunächst in Transaktionsprotokolldateien (siehe auch *Kapitel 7*). Die Transaktionsprotokolldateien sind jeweils 1 MB groß (unter Exchange 2003 waren es noch 5 MB). Verwenden Sie eine Exchange-kompatible Sicherungsanwendung, um regelmäßige Sicherungen der Exchange-Datenbank durchzuführen.

Folgende Daten und Dateien sollten Sie auf Postfachservern sichern:

- *Exchange-Datenbankdateien*, einschließlich Postfach- und Öffentliche-Ordner-Datenbanken, durch eine Exchange-kompatible Datensicherung (wird in Kapitel 17.2 ausführlich besprochen)
- *Exchange-Transaktionsprotokolldateien*, die für jede Postfachdatenbank spezifisch sind, durch eine Exchange-kompatible Datensicherung
- *Windows-Registrierung* – Sie sollten die Pfade *HKLM\SOFTWARE\Microsoft\Exchange* und *HKLM\SYSTEM\CurrentControlset\Services* regelmäßig exportieren. Alternativ sichern Sie den ganzen Serverstatus des Servers über ein passendes Sicherungsprogramm oder die interne Sicherung in Windows Server 2008 oder Windows Server 2008 (R2).

Exchange speichert in einer speziellen Datei, der Checkpoint-Datei, welche Transaktionsprotokolle bereits in die Datenbank geschrieben wurden (siehe hierzu auch Kapitel 7). Um den Pfad zu erfahren, rufen Sie in der Exchange-Verwaltungskonsole den Punkt *Organisationskonfiguration/Postfach* auf. Klicken Sie im Ergebnisbereich auf die Datenbank, deren Checkpoint-Datei Sie suchen. In der Spalte Protokollordnerpfad sehen Sie den aktuellen Speicherort. Fahren Sie mit der Maus über die Spalte, zeigt die Konsole den Pfad an. Über das Kontextmenü der Datenbank können Sie mit Datenbankpfad verschieben ebenfalls den Pfad zu den Datenbankdateien und zu den Protokolldateien anzeigen.

Den Umgang mit der Checkpoint-Datei (*.chk) zeigen wir Ihnen in Kapitel 7. Löschen Sie diese Datei, schreibt Exchange alle Transaktionsprotokolle, die zur Verfügung stehen, noch einmal in die Datenbank. Standardmäßig liegt die Checkpoint-Datei im selben Verzeichnis wie die Transaktionsprotokolle. Die Checkpoint-Datei hat die Syntax *E0n.chk*. Bei jedem Beenden oder Starten des Exchange Servers überprüft Exchange anhand der Checkpoint-Datei, welche Transaktionsprotokolle noch nicht in die Datenbank geschrieben sind, und schreibt die restlichen Transaktionsprotokolle in die Datenbank. Das Herunterfahren eines Exchange Servers kann etwas dauern, wenn viele Transaktionsprotokolle zu ver-

arbeiten sind. Wird ein Exchange Server beim Herunterfahren und Schreiben in die Datenbank unterbrochen, führt er diesen Vorgang beim Starten durch.

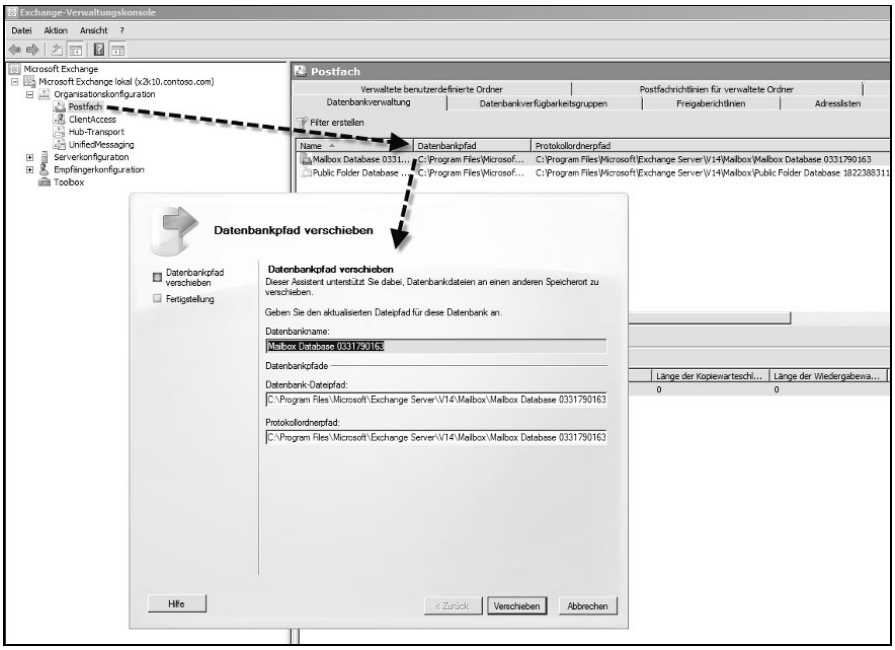


Abbildung 17.1: Anzeige des Pfads zu den Protokolldateien

Prinzipiell können Sie mit einer leeren Datenbank und einem vollständigen Satz Transaktionsprotokollen Ihre Exchange-Datenbank wieder vollkommen herstellen. Dieser Vorgang wird *Soft-Recovery* genannt. Der Exchange-Server führt diese Aufgabe vollkommen selbstständig, ohne Eingreifen eines Administrators durch. Beenden Sie den Dienst *Microsoft Exchange-Informationsspeicher* und löschen Sie anschließend die Checkpoint-Datei, beginnt der Exchange-Server beim Starten des Dienstes damit, die Datenbank wiederherzustellen, indem er alle vorhandenen Transaktionsprotokolle in die Datenbank schreiben will. Die Checkpoint-Datei wird in diesem Schritt automatisch neu angelegt. Starten Sie den Dienst, erkennt er, dass die Checkpoint-Datei fehlt, und meldet dies über die Ereignisanzeige im Anwendungsprotokoll. Im Anschluss meldet der Server die einzelnen Transaktionsprotokolle in der Ereignisanzeige, die vom Informationsspeicher-Dienst abgearbeitet und in die Datenbank geschrieben werden. Für jedes Transaktionsprotokoll, das der Server abarbeitet, sehen Sie einen Eintrag in der Ereignisanzeige. Sind alle Transaktionsprotokolle erfolgreich in die Datenbank geschrieben, erhalten Sie eine abschließende Meldung, die Sie darüber informiert, dass die Wiederherstellung der Exchange-Datenbank erfolgreich durchgeführt werden konnte.

Deaktivieren Sie die Umlaufprotokollierung (siehe Kapitel 7), legt Exchange immer neue Transaktionsprotokolle an. Dadurch benötigt der Server zwar mehr Plattenplatz, der Vorteil besteht jedoch darin, dass die Daten, die in diesen Trans-

aktionsprotokolldateien stehen, kaum verloren gehen können. Wird Exchange während des Speicherns der Daten aus den Transaktionsdateien unterbrochen, wenn zum Beispiel der Server einfach ausgeschaltet wird, überprüft der Server beim Starten der Dienste diese Vorgänge und schreibt noch nicht geschriebene Transaktionsprotokolldateien in die Datenbank. Dieser Prozess kann natürlich fehlschlagen, wenn durch die Umlaufprotokollierung ältere Transaktionsprotokolle inzwischen überschrieben wurden.

17.2 Online-Sicherung einer Exchange-Datenbank

Die Online-Sicherung ist eigentlich der einzige richtige und professionelle Weg der Datensicherung von Exchange-Datenbanken. Dabei speichert das entsprechende Datensicherungsprogramm den Inhalt der Datenbanken, während die Exchange-Dienste weiterlaufen. Abhängig von der Sicherungsvariante löscht das Sicherungsprogramm anschließend die Transaktionsprotokolle, die in die Datenbank geschrieben und gesichert wurden. Diese Aufgabe übernimmt nicht Exchange selbst, sondern das entsprechende Sicherungsprogramm.

17.2.1 Ablauf einer Online-Sicherung

Bei einer Online-Sicherung liest das Sicherungsprogramm jede einzelne Datenbanktabelle aus den Datenbankdateien (*.edb) Stück für Stück aus. Dabei belastet das Sicherungsprogramm den Server entsprechend. Die Datensicherung sollten Sie daher immer außerhalb der üblichen Nutzungszeiten durchführen. Da aber Änderungen in der Datenbank auch stattfinden können, wenn kein Benutzer angemeldet ist, muss ein weiterer Mechanismus der Datensicherung diese Daten erfassen, wenn die Tabellen von der Sicherung bereits auf Band geschrieben sind. Exchange schreibt solche Änderungen in sogenannten Patch-Dateien auf Festplatte. Hat das Sicherungsprogramm alle Tabellen gesichert, speichert es zum Schluss die Patch-Dateien, damit auch wirklich alle Änderungen in der Datensicherung berücksichtigt sind. Zum Abschluss sichert das Datensicherungsprogramm standardmäßig außerdem die Transaktionsprotokolle und löscht sie anschließend. Die Dateien sollten Sie unter keinen Umständen manuell löschen, sondern lieber ein richtiges Sicherungsprogramm verwenden.

17.2.2 Verschiedene Varianten der Online-Sicherung: normal, inkrementell und differenziell

Um Ihre Exchange-Datenbanken zu sichern, stehen Ihnen für die verschiedenen Datensicherungsprogramme verschiedene Möglichkeiten zur Verfügung. Die vollständige oder normale Sicherung ist die geläufigste Art der Sicherung und wird am häufigsten verwendet. Sie dauert sehr lange, da sie alle ausgewählten Daten enthält und deshalb auch am meisten Platz belegt. Da durch diese Sicherung alle Daten des

Systems in einem Sicherungssatz vorliegen, kann eine Wiederherstellung damit sehr schnell erfolgen. Alle gesicherten Daten markiert das Sicherungsprogramm als gesichert, so dass diese Sicherung auch aufbauende Datensicherungstypen, wie differenziell oder inkrementell, unterstützt. Die Transaktionsprotokolldateien löscht das Programm nach der Sicherung.

Inkrementelle Sicherung von Transaktionsprotokollen

Die inkrementelle Sicherung eines Exchange-Servers sichert keine Exchange-Datenbanken, sondern nur die Transaktionsprotokolldateien. Nach der Sicherung der Transaktionsprotokolldateien löscht das Sicherungsprogramm die Transaktionsprotokolle. Die Dauer und der Plattenverbrauch dieser Sicherung sind daher sehr gering, da dabei nur die geänderten Inhalte seit der letzten Sicherung erfasst werden. Da dadurch aber auch die Exchange-Daten auf verschiedene Sicherungssätze verteilt sind, dauert eine eventuell notwendige Rücksicherung viel länger als bei der normalen Sicherung, welche auch die kompletten Datenbanken enthält. Die Wiederherstellung mit der inkrementellen Sicherung dauert am längsten, denn außer der letzten vollständigen Sicherung müssen Sie auch alle seitdem erfolgten inkrementellen Sicherungen wiederherstellen.

Viele Unternehmen kombinieren inkrementelle Sicherungen mit normalen Sicherungen. In regelmäßigen Abständen, zum Beispiel einmal pro Woche oder Monat, sichern sie die Exchange-Datenbanken vollständig mit der normalen Sicherung. In dem Zeitraum zwischen diesen vollständigen Sicherungen sichern sie die Transaktionsprotokolle inkrementell. Das ist ein guter Kompromiss zwischen Dauer und Platzverbrauch der Datensicherung und einer schnellen Wiederherstellung der Daten. Aktivieren Sie für eine Datenbank die Umlaufprotokollierung, können Sie diese nicht mehr inkrementell sichern. Bei der Umlaufprotokollierung verwendet Exchange immer denselben Satz Transaktionsprotokolle. Da die inkrementelle Sicherung die Transaktionsprotokolle löscht, kann sie bei aktivierter Umlaufprotokollierung natürlich nicht verwendet werden.

Differenzielle Sicherung der Transaktionsprotokolle

Bei der differenziellen Sicherung sichert das Datensicherungsprogramm, wie bei der inkrementellen Sicherung, keine Datenbanken, sondern nur die Transaktionsprotokolldateien. Im Gegensatz zur inkrementellen Sicherung löscht das Programm die Transaktionsprotokolle aber nach der Sicherung nicht. Sie können beispielsweise Ihre Datenbanken wöchentlich mit der normalen Sicherung vollständig sichern und an den Wochentagen differenziell die Transaktionsprotokolle. Dadurch werden einmal in der Woche die Transaktionsprotokolle gelöscht und unter der Woche geht die Sicherung sehr schnell, da lediglich die Transaktionsprotokolle gesichert werden. Der Plattenverbrauch von Exchange und die Dauer der Sicherung steigen zwar unter der Woche an, da bei der differentiellen Sicherung

die Transaktionsprotokolle nicht entfernt werden, aber am Wochenende wird während der normalen Sicherung wieder Plattenplatz freigegeben. Mit der differenziellen Sicherung lässt sich eine Wiederherstellung viel schneller durchführen als mit der inkrementellen, da Sie nur den letzten vollständigen Sicherungssatz sowie den letzten differenziellen Sicherungssatz wiederherstellen müssen. Da die differenzielle Sicherung auf den Transaktionsprotokollen aufbaut, kann diese Sicherungsmethode nicht verwendet werden, wenn Sie für eine Postfachdatenbank die Umlaufprotokollierung aktiviert haben.

Für die vollständige Wiederherstellung anhand von differenziellen und inkrementellen Sicherungen sind mehrere Sicherungssätze erforderlich. Fehlt ein Sicherungssatz oder kann er nicht wiederhergestellt werden, erfolgt die Wiederherstellung nur bis zu dem nicht mehr vorhandenen Sicherungssatz. Wie der Kategorietyp besagt, werden in differenziellen und inkrementellen Sicherungen nur die Änderungen gespeichert. Daher sind die Sicherungsdateien kleiner als die Dateien einer Gesamtsicherung und der Sicherungsvorgang nimmt weniger Zeit in Anspruch.

17.3 Die Windows-Server-Sicherung im Überblick

Die einzelnen Server im Netzwerk können auch die interne Datensicherung von Windows Server 2008 nutzen. Das Programm sichert die Daten über den *Schattenkopiedienst* (*Volume Shadow Service*, *VSS*) mithilfe einer Block-Level-Backup-Technologie in VHD-Dateien. Nach einem vollständigen Backup können Sie so einfach inkrementelle Sicherungen auf Blockebene erstellen. Übergangsweise oder zu Testzwecken können Sie Exchange Server 2010 auch mit dem Datensicherungsprogramm von Windows Server 2008 oder Windows Server 2008 (R2) sichern. Das Sicherungsprogramm unterstützt auch die Online-Sicherung der Exchange-Datenbanken. Während der Sicherung führt das Sicherungsprogramm eine Konsistenzprüfung der Exchange-Datendateien durch. Microsoft hat die Datensicherung im Vergleich zu Windows Server 2008 noch mal überarbeitet. Sie können bei der Sicherung jetzt wieder einzelne Ordner und Dateien gezielt auswählen. In Windows Server 2008 konnten Sie nur komplette Laufwerke sichern. Einzelne Dateien lassen sich integrieren oder explizit ausschließen. Die Steuerung der Sicherung können Sie in der PowerShell vornehmen. Der Systemstatus lässt sich jetzt auch inkrementell sichern, bisher war das immer nur vollständig möglich. Auch die möglichen Ziellaufwerke zur Sicherung lasen sich jetzt wesentlich flexibler auswählen, Sie benötigen nicht gezwungenermaßen eine komplette physikalische Festplatte, sondern einzelne Partitionen können Sie auch als Ziel auswählen. Außerdem passt sich die Sicherung besser an SAN-Systeme an und unterstützt SnapShots von LUNs.

17.3.1 Windows-Server-Sicherung installieren und konfigurieren

Damit Sie die neue Windows-Server-Sicherung verwenden können, installieren Sie diese über den Server-Manager als neues Feature. Die Sicherungsfunktionen von Windows Server 2008 sind in die beiden Unterkomponenten *Windows Server-Sicherung* und *Befehlszeilentools* unterteilt.

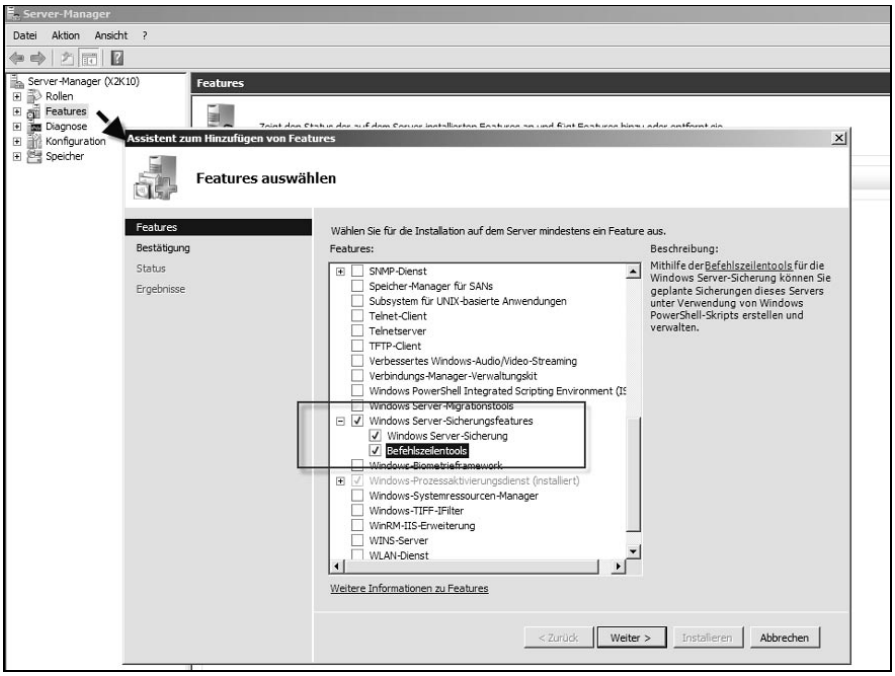


Abbildung 17.2: Die Windows-Server-Sicherung installieren Sie als Feature.

Nach der Installation verwalten Sie die Windows-Server-Sicherung über *Start/Verwaltung/Windows-Server-Sicherung*. Alternativ können Sie im Suchfeld des Startmenüs auch *wbadmin.msc* eingeben.

INFO

Die Windows-Server-Sicherung ist für alle 32- und 64-Bit-Editionen von Windows Server 2008 und Windows Server 2008 (R2) verfügbar, nicht jedoch bei Core-Server-Installationen. Hier kann die Sicherung dann entweder mit *Wbadmin.exe* über die Befehlszeile verwaltet oder von einem anderen Server aus mit dem Snap-In durchgeführt werden. Auch die CMDlets für die PowerShell sind auf Core-Servern nicht verfügbar.

Diese Konsole können Sie in jeder MMC laden. Über Assistenten lassen sich Sicherungs- und Wiederherstellungsvorgänge sehr leicht durchführen. Die neue Datensicherung sichert die Daten blockbasiert von den Datenträgern, nicht mehr pro Datei. Standardmäßig führt die Sicherung immer vollständige Sicherungen durch. Über den Menübefehl *Aktion/Leistungseinstellungen konfigurieren* können Sie inkrementelle Sicherungen aktivieren.

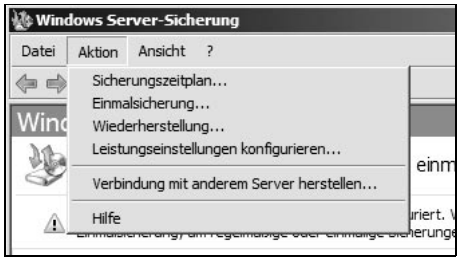


Abbildung 17.3: Über den Menüpunkt Aktion stellen Sie die Sicherung ein.

Zu einem gewissen Zeitpunkt benötigen Sie eine Vollsicherung, zum Beispiel freitags. Am Montag sichern Sie alle Daten, die sich seit Freitag verändert haben. Am Dienstag werden alle Daten gesichert, die sich seit Montag verändert haben.

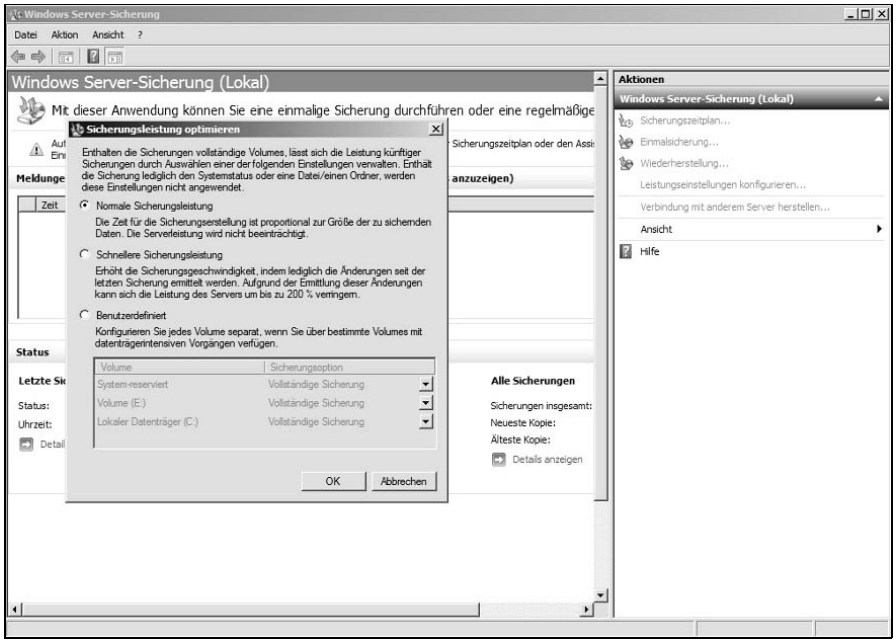


Abbildung 17.4: Konfigurieren der Leistungsoptionen der Sicherung

Sicherungsvorgänge konfigurieren Sie über den Aktionsbereich der Konsole. Sie können einzelne Sicherungen erstellen oder einen *Sicherungszeitplan* definieren. Durch die Einrichtung führt ein Assistent.

Nachdem die Sicherung und Verwaltungsprogramme installiert wurden, können Sie eine Datensicherung einrichten. Microsoft empfiehlt zur Sicherung einen externen Datenträger, den Sie über USB oder Firewire mit dem Computer verbinden. Auch eine Freigabe im Netzwerk funktioniert.

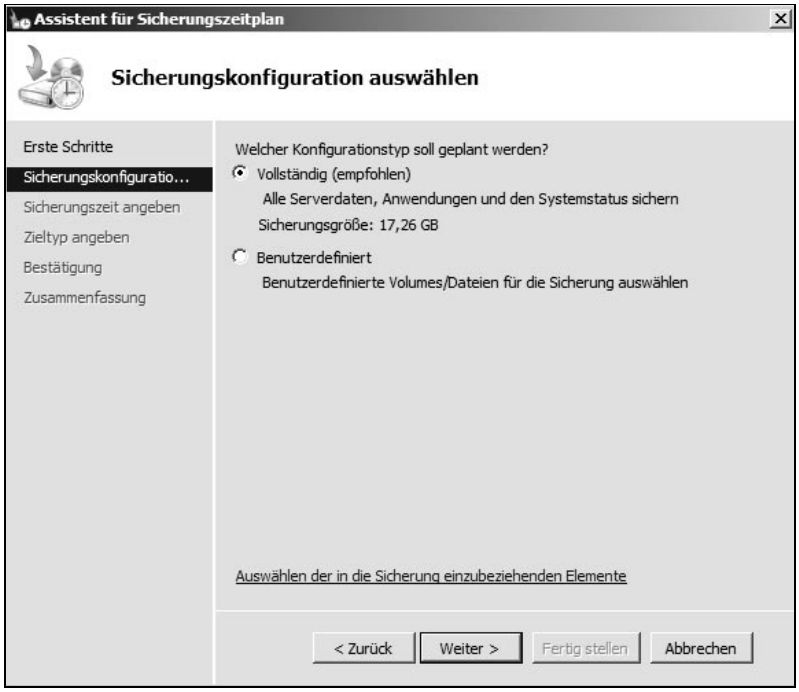


Abbildung 17.5: Die Windows-Server-Sicherung bietet eine neue Oberfläche zur Verwaltung.

Achten Sie darauf, dass die zur Sicherung verwendete externe Festplatte keine Daten enthält. Vor der Sicherung formatiert der Sicherungsassistent den Datenträger, so dass alle gespeicherten Daten verloren gehen.

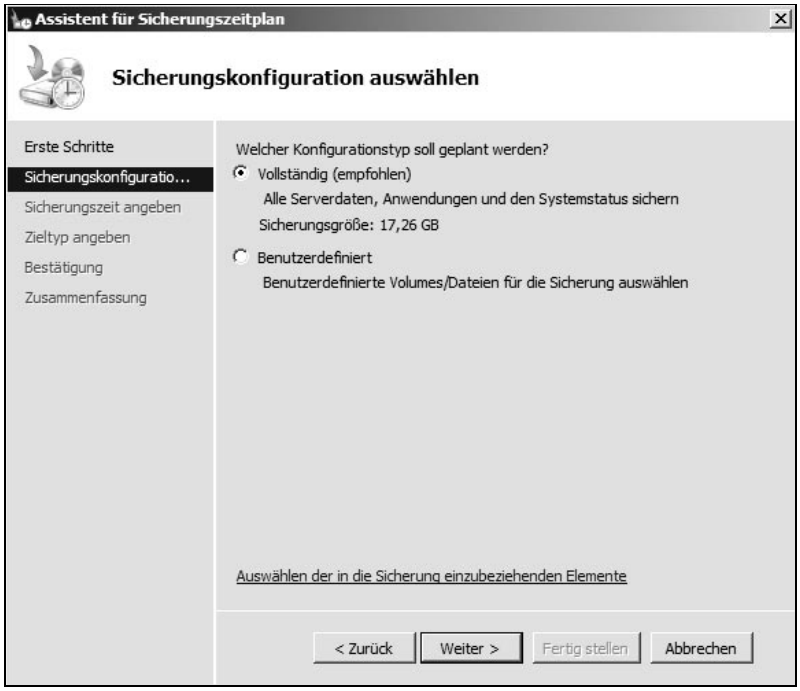
STOP

Um einen neuen Sicherungsauftrag zu erstellen, rufen Sie entweder über die Verwaltung die Konsole des Sicherungsprogramms auf oder geben Sie im Suchfeld des Startmenüs den Befehl *wbadmin.msc* ein. Der Befehl *wbadmin.exe* startet das Befehlszeilen-Tool der Sicherung. Einen neuen Auftrag erstellen Sie über *Aktion/Sicherungszeitplan*. Sie können nach der Erstellung eines Zeitplans auch eine Einmalsicherung durchführen mit den Einstellungen des Sicherungszeitplans. Auf der nächsten Seite des Assistenten wählen Sie aus, ob Sie den kompletten Server sichern wollen oder ob Sie die Partitionen und Daten selbst auswählen wollen. Wählen Sie zur Sicherung eines Servers mit Exchange Server 2010 am besten die Option *Vollständig* aus. Bei dieser Sicherung sind auch das Betriebssystem und der Systemstatus des Servers enthalten. Auf Domänencontrollern sichert das Tool auch die Active Directory-Datenbank mit.

Auf der nächsten Seite wählen Sie aus, welche Partitionen Sie sichern wollen, wenn Sie die benutzerdefinierte Sicherung ausgewählt haben. Standardmäßig sind alle Partitionen aktiviert. Das Sicherungsprogramm zeigt nicht mehr die Exchange-Datenbanken an, sondern bindet diese automatisch ein, wenn Sie den kompletten Server und den Serverstatus sichern lassen. Erst bei einer eventuellen

Wiederherstellung können Sie explizit Datenbanken auswählen. Wie das geht, zeigen wir Ihnen in Kapitel 17.7. Zur Sicherung müssen Sie immer alle Partitionen sichern und auch alle Datenbanken auf dem Server. Die Sicherung einzelner Datenbanken ist auch über Umwege nicht möglich.

Abbildung 17.6: Auswählen der zu sichernden Daten



INFO

Das Sicherungsprogramm kann bis zu 512 Kopien einer Partition in der Sicherung speichern. Da die Sicherung den Schattenkopiedienst nutzt, ist damit das Limit der Schattenkopien erreicht. Alle Partitionen, die Daten, Dateien und Programme des Betriebssystems enthalten, wählt der Assistent immer automatisch aus.

Auf der nächsten Seite konfigurieren Sie den Zeitplan, über den Sie den Server sichern wollen. Hier legen Sie fest, ob Sie mehrmals oder nur einmal pro Tag sichern wollen.

Als Nächstes legen Sie fest, wo Sie die Sicherungen speichern wollen, also auf einer eigenen Partition, einer externen Festplatte oder auf einer Freigabe im Netzwerk. Auf der nächsten Seite wählen Sie das Sicherungsmedium aus, auf das Sie die Daten sichern wollen. Zeigt der Assistent die Festplatte nicht an, hilft ein Klick auf die Schaltfläche *Alle verfügbaren Datenträger anzeigen*. Datenträger, auf denen Daten des Betriebssystems gespeichert sind, können Sie nicht als Sicherungsmedium auswählen. Nach der Auswahl des Datenträgers erscheint eine Meldung, die Sie darauf hinweist, dass der Datenträger formatiert wird. Der Assistent

führt die Formatierung aber nicht sofort durch, sondern erst nach der Einrichtung. Es ist nicht möglich, dass auf einen Datenträger gesichert wird, der mit FAT32 formatiert wurde.

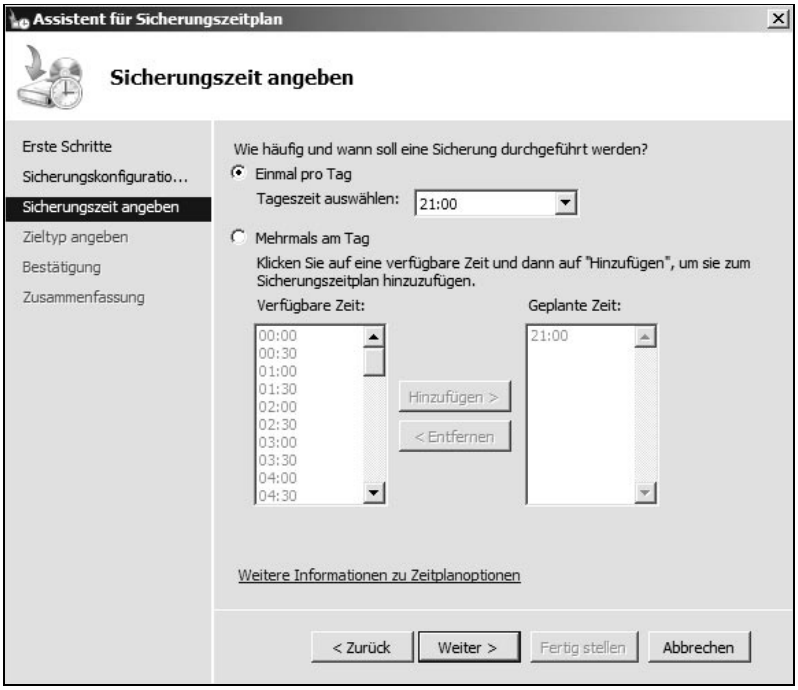


Abbildung 17.7: Konfigurieren der Sicherungszeit

INFO

Die Sicherung überwacht automatisch den Speicherplatz auf den Datenträgern, auf denen die Sicherungen liegen. Steht nicht mehr genügend Plattenplatz zur Verfügung, informiert die Sicherung darüber und führt keine Sicherung mehr durch. Außerdem zeigt Windows den Datenträger nicht mehr im Explorer des Servers an, dieser steht ausschließlich für die Datensicherung zur Verfügung. Auf einer Netzwerkfreigabe können Sie jeweils nur eine Sicherung ablegen, eine frühere Sicherung wird automatisch überschrieben.

Die Einrichtung des Sicherungszeitplans ist damit abgeschlossen. Wollen Sie eine sofortige Einmalsicherung durchführen, können Sie den Assistenten über das Menü *Aktion* starten. Der Assistent übernimmt die Einstellungen der vorhandenen, geplanten Sicherung. Natürlich können Sie für Einmalsicherungen auch unterschiedliche Optionen wählen.

Sobald die Sicherung durchgelaufen ist, erhalten Sie eine entsprechende Information. Zusätzlich zeigt die Exchange-Verwaltungskonsole den Zeitpunkt der letzten erfolgreichen Sicherung in den Eigenschaften der Datenbank an. Sie können nach einer manuellen Sicherung auch überprüfen, ob das Sicherungsprogramm die Transaktionsprotokolle gelöscht hat wie vorgesehen.

Abbildung 17.8: Anzeigen des Sicherungsprozesses

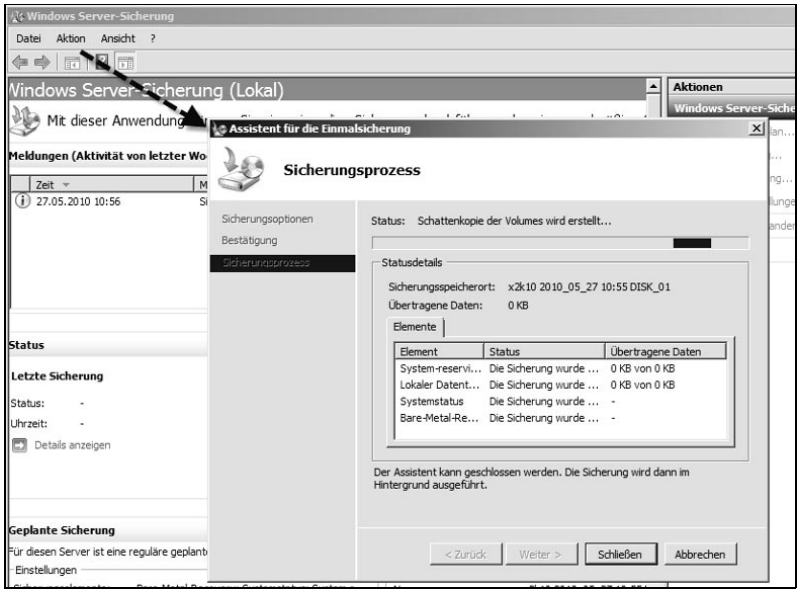


Abbildung 17.9: Anzeigen des Sicherungszeitpunkts der letzten Datensicherung

17.3.2 Sicherung in der Befehlszeile durchführen

Für Skripts steht das Befehlszeilen-Tool *wbadmin.exe* für die Verwaltung der Sicherungen zur Verfügung. Über */?* blendet der Befehl für jeden der unten aufgelisteten Befehle eine entsprechende Hilfe ein. Die wichtigsten Befehle für das Tool sind:

- *Wbadmin enable backup* – erstellt oder ändert eine eingerichtete Sicherung.
- *Wbadmin disable backup* – deaktiviert die eingerichteten Sicherung.
- *Wbadmin start backup* – startet einen Sicherungsauftrag.
- *Wbadmin stop job* – unterbricht eine laufende Sicherung oder Wiederherstellung.
- *Wbadmin get disks* – zeigt die IDs der Disk an, die gesichert und auf denen Sicherungen abgelegt sind.
- *Wbadmin get versions* – zeigt Informationen über die verfügbaren Sicherungen an.
- *Wbadmin get items* – zeigt die enthaltenen Daten einer Sicherung an.
- *Wbadmin start recovery* – startet eine Wiederherstellung.
- *Wbadmin get status* – zeigt den Status einer laufenden Sicherung oder Wiederherstellung an.
- *Wbadmin start sysstaterecovery* – stellt den Systemstatus wieder her.
- *Wbadmin start sysrecovery* – startet eine vollständige Systemwiederherstellung, die später in den Computerreparaturoptionen über die Windows Server 2008-DVD wiederhergestellt werden kann.

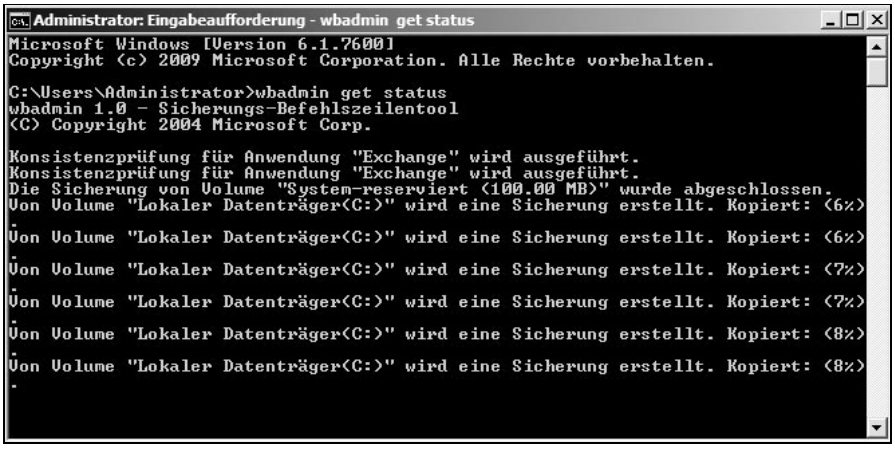


Abbildung 17.10: Anzeigen des Sicherungsstatus einer laufenden Sicherung in der Befehlszeile

- *wbadmin delete systemstatebackup –keepversions:N* – löscht alle System-State-Sicherungen bis auf die letzten N Versionen.
- *wbadmin delete systemstatebackup –deleteoldest* – löscht die jeweils älteste System-State-Sicherung.

- *vssadmin list shadows /for=x:* – zeigt die vorhandenen Sicherungen für das Laufwerk x: an.
- *vssadmin delete shadows /for=x: /oldest* – löscht die jeweils älteste Sicherung des Laufwerks x:.

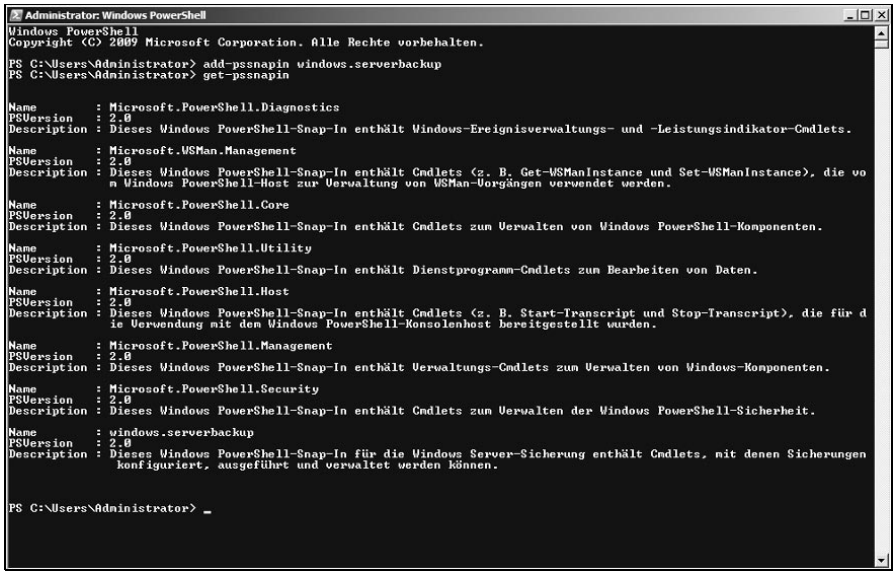
Das Sicherungsprogramm ermöglicht es, die Datensicherung über die Befehlszeile zu starten. Mit dem Befehl *wbadmin start backup –allCritical –backuptarget:<Zielfestplatte> –quiet* wird die Sicherung der notwendigen Partitionen auf die Zielfestplatte durchgeführt. Durch Eingabe von *–quiet* muss die Eingabe nicht bestätigt werden, sondern die Sicherung beginnt sofort.

Mit dem Befehl *wbadmin start backup –include:<Partition1>:,<Partition2>:, <PartitionN> –backuptarget:<Zielfestplatte>: –quiet* werden alle hinterlegten Partitionen in die Sicherung eingeschlossen. Die Partitionen werden durch Komma ohne Leerzeichen voneinander getrennt.

17.3.3 Sicherung mit der PowerShell steuern

Neben *wbadmin.exe* können Sie in Windows Server 2008 (R2) die Datensicherung auch über die PowerShell steuern. Dazu müssen Sie in der PowerShell oder der PowerShell ISE zunächst die Befehle für die Datensicherung laden. Verwenden Sie dazu den Befehl *add-pssnapin windows.serverbackup*. Mit dem Befehl *get-pssnapin* überprüfen Sie, ob das SnapIn erfolgreich geladen ist.

Abbildung 17.11: Anzeigen der geladenen SnapIns der PowerShell



Mit dem Befehl *Get-Command -module windows.serverbackup* lassen Sie sich die CMDlets der PowerShell anzeigen.

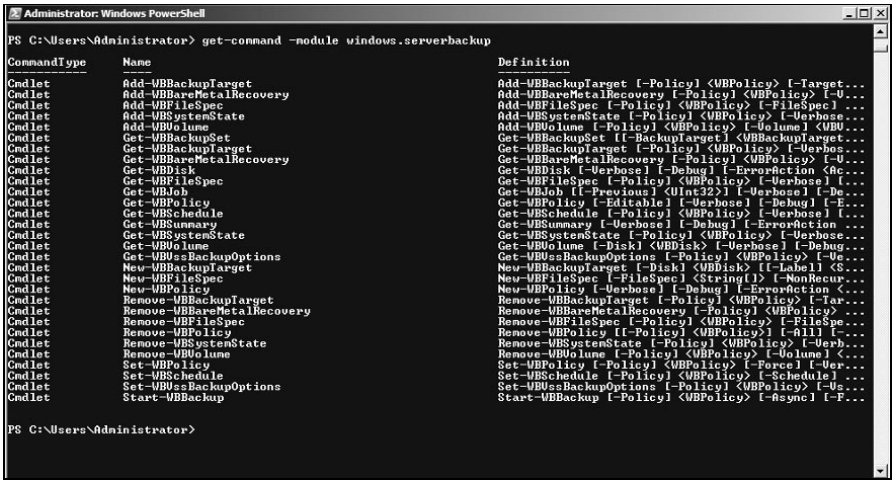


Abbildung 17.12: Anzeigen der CMDlets für die PowerShell

Um eine neue Sicherung über die PowerShell zu erstellen, müssen Sie zunächst einen Sicherungssatz anlegen, also eine Richtlinie, die steuert, welche Daten der Server sichern soll. Am besten setzen Sie dazu eine Variable:

$policy = New-WBPolicy

Als Nächstes legen Sie fest, wo der Server seine Daten sichern soll, zum Beispiel auf dem Laufwerk E:

$BackupTargetVolume = New-WBbackupTarget –VolumePath E:

Wollen Sie in der Sicherung festlegen, dass auch ein Bare-Metal-Restore möglich sein soll, fügen Sie die Sicherung wichtiger Systemdaten der Variablen für die neue Sicherungsrichtlinie hinzu:

Add-WBBareMetalRecovery –Policy $policy

Sie starten die erstellte Sicherung mit dem Befehl:

Start-WBBackup –Policy $policy

Wollen Sie der Sicherung einen Zeitplan hinzufügen, zum Beispiel ein Start um 11:00 und 17:30 Uhr, verwenden Sie den Befehl:

Set-WBSchedule –Policy $policy –Schedule 11:00, 17:30

17.4 Offline-Sicherung von Exchange Servern

Die Offline-Sicherung ist im Gegensatz zur Online-Sicherung kein Sicherungssystem, bei dem Transaktionsprotokolle gelöscht und Dateien als gesichert markiert werden. Eine Offline-Sicherung beinhaltet nur das manuelle Kopieren des Exchange-Verzeichnisses in ein anderes Verzeichnis oder auf Band, ohne dass dabei eine Überprüfung der Datenbank oder ein Löschen der Transaktionsproto-

kolle stattfindet. Damit Sie die Exchange-Datenbank kopieren können, müssen Sie notwendige, am besten alle, Exchange-Dienste beenden. Nach dem Beenden der Dienste können Sie die Exchange-Daten kopieren und danach die Dienste wieder starten. Sie sollten diese Sicherung nur in Ausnahmefällen einsetzen und keinesfalls in Ihre Sicherungsstrategie einbauen. In manchen Fällen, zum Beispiel beim Durchführen von Optimierungsarbeiten, Hardware-Änderungen am Server oder Fehlerbehebungen, kann eine zusätzliche Offline-Sicherung sinnvoll sein, aber auf keinen Fall als einzige Sicherungsstrategie.

17.4.1 Vorbereitung für eine Offline-Sicherung

Überprüfen Sie, ob für die Datenbank die Umlaufprotokollierung aktiviert ist. Dies spielt zwar für die Offline-Sicherung direkt keine Rolle, wenn Sie aber eine Datenbank sichern, bei der die Umlaufprotokollierung aktiviert ist, können Sie später keine Transaktionsprotokolle nachträglich in das Offline-Backup einspielen. Das ist nur möglich, wenn die Umlaufprotokollierung deaktiviert ist. Standardmäßig ist bei Exchange Server 2010 die Umlaufprotokollierung immer deaktiviert. Die Konfiguration für die Umlaufprotokollierung finden Sie in den Eigenschaften der Datenbank. Als Nächstes sollten Sie überprüfen, auf welchem Datenträger und Pfad die einzelnen Datenbanken und deren Dateien liegen. Auch der Speicherort der Transaktionsprotokolle und der Checkpoint-Datei ist wichtig. Diese Informationen finden Sie, wie die Umlaufprotokollierung, in den Eigenschaften der Postfachspeicher. Um später Transaktionsprotokolle in ein Offline-Backup einzuspielen, müssen Sie die Dateien der Datenbanken in dasselbe Verzeichnis kopieren, aus dem Sie diese gesichert haben. Ändern Sie den Pfad der Datenbank nach einem Offline-Backup, müssen Sie zum Einspielen der Transaktionsprotokolle in die Datenbankdateien den alten Pfad wiederherstellen. Sie können in einem solchen Fall nur die Transaktionsprotokolle zurückspielen, die vor dem Ändern des Datenbankpfads erstellt wurden. Die Transaktionsprotokolle können hingegen auf einem beliebigen Pfad zurückgespielt werden. Das liegt daran, dass die Transaktionsprotokolle zwar den Pfad zu den Datenbankdateien fest enthalten, die Datenbankdateien jedoch den Pfad zu den Transaktionsprotokollen nicht kennen. Sie sollten sich den Pfad zur Checkpoint-Datei ebenfalls merken. In dieser Datei speichert Exchange ab, welche Transaktionsprotokolle bereits in die Datenbank geschrieben wurden. Wollen Sie nach einem Offline-Backup die Transaktionsprotokolle in die Datenbank spielen, müssen Sie diese Datei eventuell löschen.

Um einen Postfachspeicher oder Informationsspeicher für öffentliche Ordner offline zu sichern, müssen Sie zunächst dessen Bereitstellung aufheben. Sie brauchen nicht die Bereitstellung aller Datenbanken aufzuheben oder den Informationsspeicherdienst beenden, wenn Sie nur einzelne Postfachspeicher sichern wollen. Sie können die Bereitstellung einzelner Informationsspeicher aufheben, wenn Sie in der Exchange-Verwaltungskonsole mit der rechten Maustaste auf den

Informationsspeicher klicken und die Option *Bereitstellung der Datenbank aufheben* auswählen. Haben Sie den Informationsspeicherdienst bereits beendet, müssen Sie die Bereitstellung nicht auch noch aufheben.

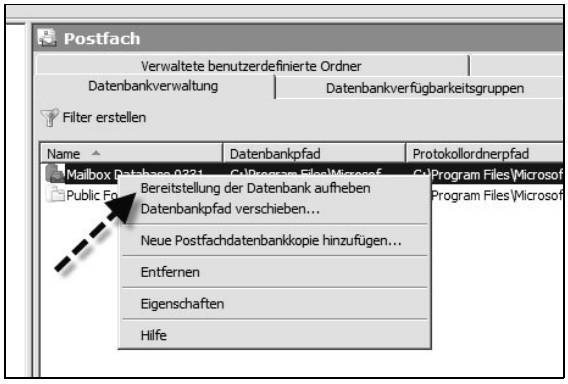


Abbildung 17.13: Aufheben der Bereitstellung eine Datenbank vor dem Kopieren

Als Nächstes sollten Sie mit *Eseutil* die Datenbank auf Konsistenz prüfen. Verwenden Sie dazu den Befehl *Eseutil /mh <Pfad zur Datenbankdatei>*, zum Beispiel *Eseutil /mh »C:\Program Files\Microsoft\Exchange Server\V14\Mailbox\Mailbox Database 0331790163\Mailbox Database 0331790163.edb«*. Nach der Eingabe des Befehls erscheint auf dem Bildschirm die Ausgabe der Abfrage. Mehr zur Konsistenzprüfung lesen Sie in Kapitel 7.

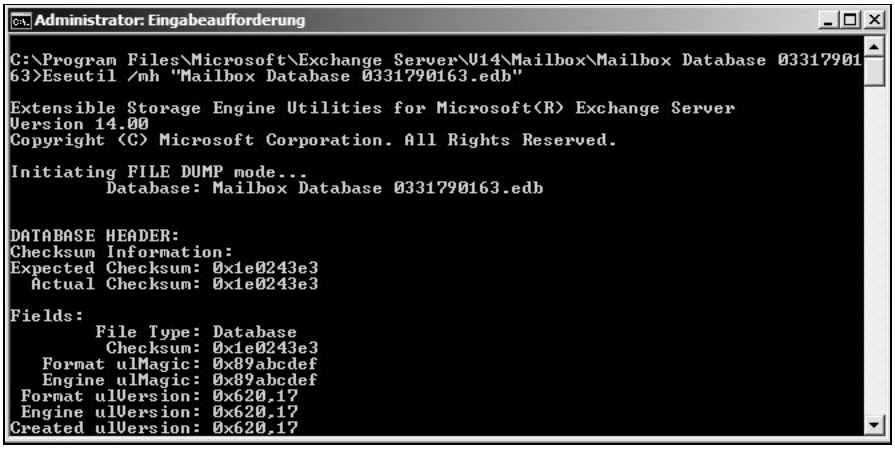


Abbildung 17.14: Überprüfen des konsistenten Beendens der Datenbank

Hat die Datenbank einen inkonsistenten Wert oder wird die Meldung ausgegeben, dass die Datenbank nicht sauber heruntergefahren worden ist, sollten Sie die Datenbank wieder bereitstellen und die Bereitstellung nochmals aufheben. Dann sollte die Datenbank allerdings konsistent sein. Wenn nicht, haben Sie wahrscheinlich ein größeres Problem mit Ihrer Datenbank und sollten diese reparieren. Im folgenden Listing sehen Sie den Status einer Datenbank an einem Beispiel.

```
Extensible Storage Engine Utilities for Microsoft(R) Exchange Server
Version 14.00
Copyright (C) Microsoft Corporation. All Rights Reserved.
Initiating FILE DUMP mode...
         Database: Mailbox Database 0331790163.edb
DATABASE HEADER:
Checksum Information:
Expected Checksum: 0x1e0243e3
  Actual Checksum: 0x1e0243e3
Fields:
        File Type: Database
         Checksum: 0x1e0243e3
   Format ulMagic: 0x89abcdef
   Engine ulMagic: 0x89abcdef
 Format ulVersion: 0x620,17
 Engine ulVersion: 0x620,17
Created ulVersion: 0x620,17
     DB Signature: Create time:04/16/2010 10:17:30 Rand:2753968 Computer:
         cbDbPage: 32768
           dbtime: 279000 (0x441d8)
            State: Clean Shutdown
       Last Consistent: (0x1EB,8,13F)  05/27/2010 11:50:02
      Last Attach: (0x192,9,86)  05/04/2010 14:53:50
      Last Detach: (0x1EB,8,13F)  05/27/2010 11:50:02
             Dbid: 1
    Log Signature: Create time:04/16/2010 10:17:28 Rand:2724548 Computer:
       OS Version: (6.1.7600 SP 0 NLS 60101.60101)
Previous Full Backup:
        Log Gen: 486-489 (0x1e6-0x1e9) - OSSnapshot
           Mark: (0x1EA,8,16)
           Mark: 05/27/2010 10:56:56
```

Nach den notwendigen Vorarbeiten können Sie die Datenbankdateien in ein Backup-Verzeichnis kopieren. Sichern Sie auch die restlichen Transaktionsprotokolle vorsichtshalber mit. Haben Sie die Dateien gesichert, können Sie den Postfachspeicher oder Informationsspeicher für öffentliche Ordner wieder bereitstellen.

17.5 Exchange-Daten mit dem Sicherungsprogramm wiederherstellen

Wenn auf dem Server Sicherungen zur Verfügung stehen, besteht auch die Möglichkeit, einzelne Dateien und Ordner wiederherzustellen beziehungsweise auch einzelne Datenbanken von Exchange. Eine Wiederherstellung starten Sie im Sicherungsprogramm über das Menü *Aktion*. Auch hier führt ein Assistent durch die einzelnen Schritte der Wiederherstellung. Wählen Sie den lokalen Server für die Wiederherstellung aus. Sie müssen vor der Wiederherstellung keine Anpassungen an der Datenbank vornehmen. Während der Wiederstellung hebt der Sicherungsassistent die Bereitstellung der Datenbanken, die Sie wiederherstellen, selbstständig auf und stellt diese nach der Sicherung wieder bereit.

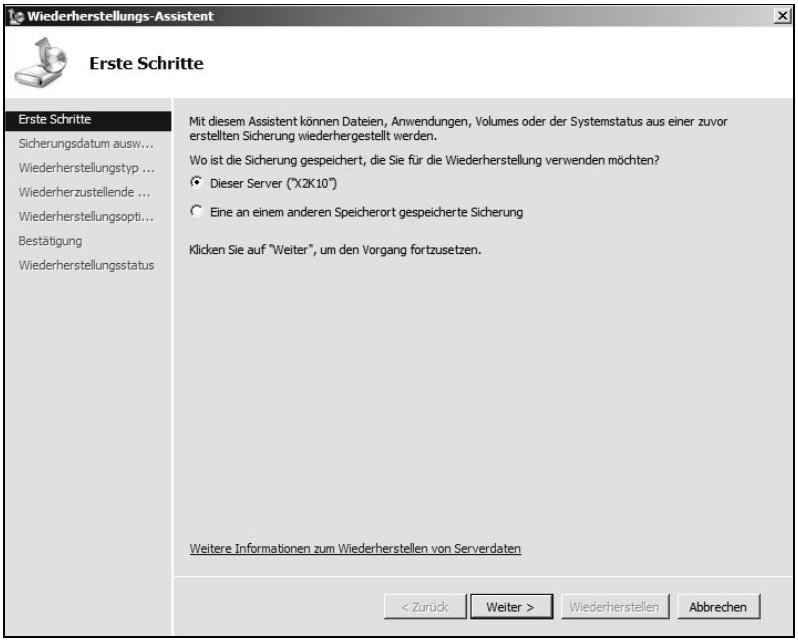


Abbildung 17.15: Auswählen des Servers für die Wiederherstellung

17

Wählen Sie auf der Seite *Sicherungsdatum auswählen* das Datum und die Uhrzeit der Sicherung aus, die Sie wiederherstellen wollen.

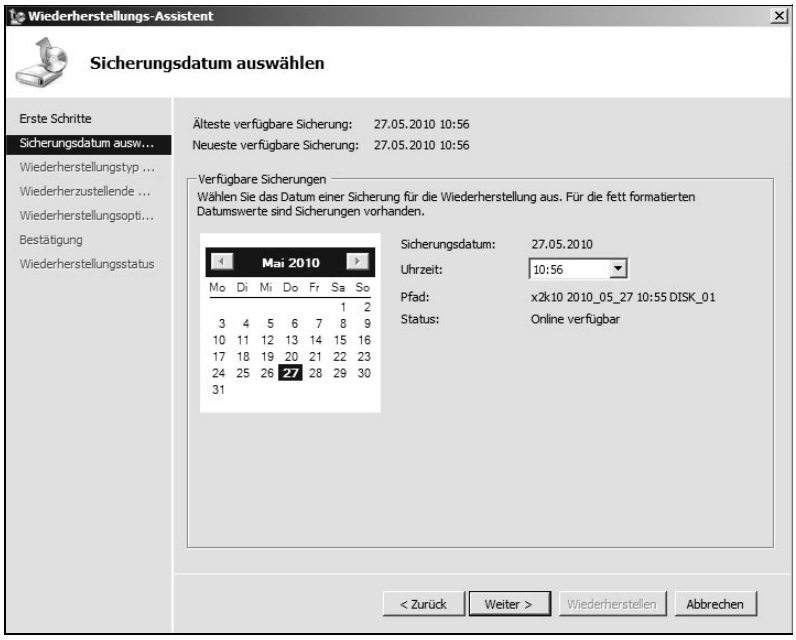
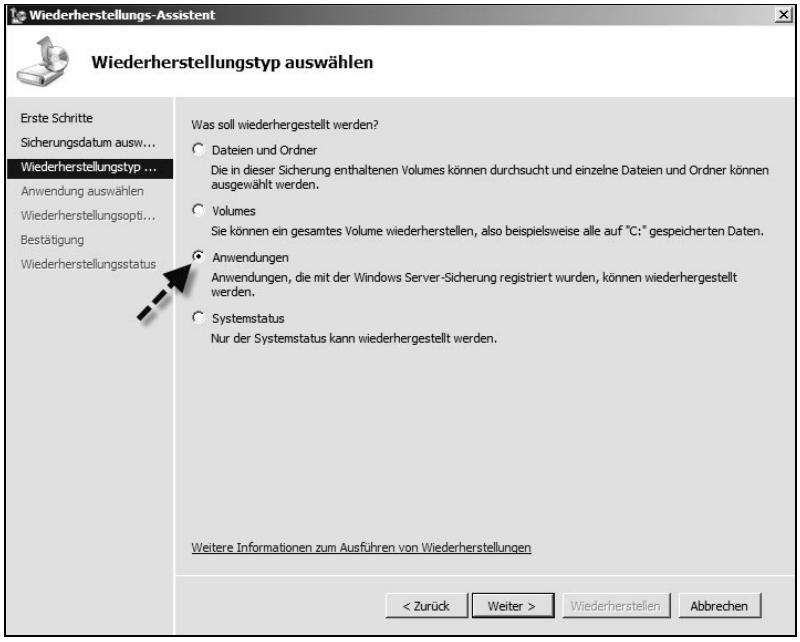


Abbildung 17.16: Auswählen des Datums der Sicherung

Wählen Sie auf der nächsten Seite *Wiederherstellungstyp auswählen* die Option *Anwendungen* aus und klicken Sie dann auf *Weiter*.

Abbildung 17.17: Auswählen des Wiederherstellungstyps Anwendungen



Auf der nächsten Seite muss bei *Anwendungen* Exchange aufgelistet sein. Dann ist sichergestellt, dass eine Exchange-taugliche Sicherung vorhanden ist. Klicken Sie auf *Details anzeigen*, um sich die gesicherten Exchange-Datenbanken anzeigen zu lassen.

Handelt es sich bei der Sicherung um die aktuellste Version der Sicherung, erscheint noch die Option *Keine Rollforward-Wiederherstellung der Anwendungsdatenbanken ausführen*. Für eine Rollforward-Wiederherstellung benötigen Sie Transaktionsprotokolle, die nach der Sicherung erstellt wurden. Sind die Transaktionsprotokolle nicht vollständig vorhanden, erzeugt die Wiederherstellung einen Fehler in der Ereignisanzeige, der Sie darauf hinweist, dass Daten verloren gehen.

Wählen Sie auf der nächsten Seite *Wiederherstellungsoptionen auswählen* aus, wo Sie die Daten wiederherstellen wollen. Aktivieren Sie die Option *Am ursprünglichen Speicherort wiederherstellen*, stellt das Sicherungsprogramm alle gesicherten Datenbanken am ursprünglichen Speicherort wieder her. Der Vorgang dabei entspricht der Wiederherstellung einer normalen Datei. Bei der Option *An einem anderen Speicherort wiederherstellen* können Sie die Datenbanken in einem anderen Verzeichnis wiederherstellen. Nach der Wiederherstellung können Sie die Datendateien in eine Wiederherstellungsdatenbank integrieren und danach manuell wieder an ihren ursprünglichen Speicherort verschieben. Auf der nächsten Seite klicken Sie dann

auf *Wiederherstellen*. Sie sehen den Status der Wiederherstellung auf dieser Seite. Klicken Sie auf *Schließen*, wenn die Wiederherstellung abgeschlossen ist.

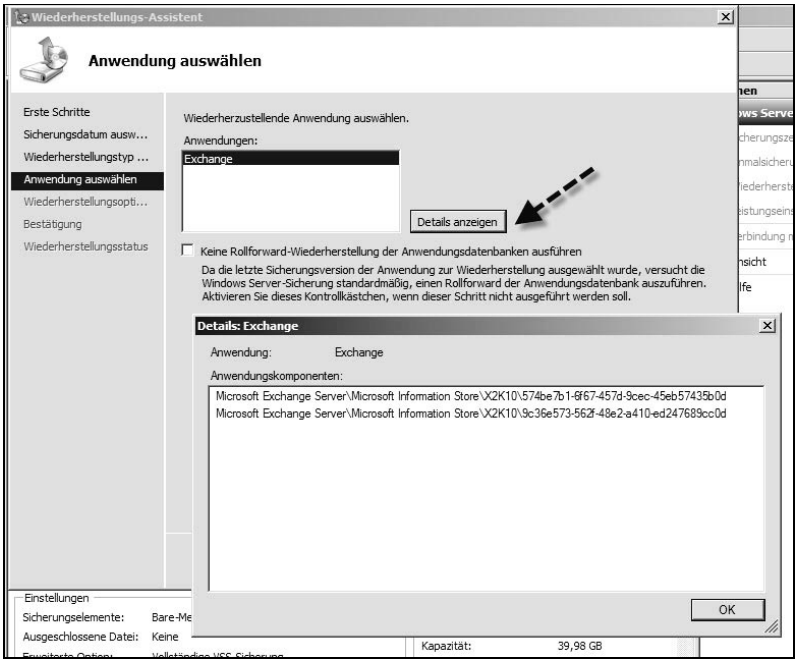


Abbildung 17.18: Anzeigen der gesicherten Exchange-Datenbanken in der Windows-Server-Sicherung

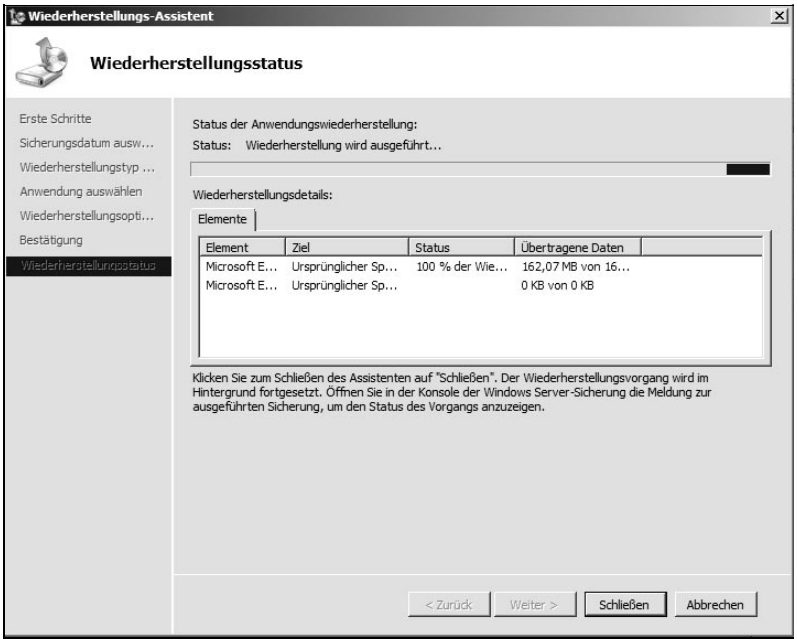


Abbildung 17.19: Anzeigen des Wiederherstellungsstatus der Datenbank

17.6 Kompletten Server mit dem Sicherungsprogramm wiederherstellen

Haben Sie auf dem Server eine vollständige Datensicherung erstellt, können Sie mit dieser den kompletten Server wiederherstellen, wenn dieser zum Beispiel nicht mehr starten kann.

17.6.1 Wiederherstellen über die Computerreparaturoptionen

Dazu muss der Datenträger mit der Sicherung mit dem Server verbunden und der Server mit der Windows Server 2008 (R2)-DVD gebootet werden. Auf der Startseite des Installationsassistenten klicken Sie auf *Weiter*. Auf der nächsten Seite wird aber statt der Installation der Menüpunkt *Computerreparaturoptionen* ausgewählt. Der Vorgang ist übrigens identisch mit Windows Vista und Windows 7, nur das Sicherungsprogramm sieht am Client etwas anders aus. In den Systemwiederherstellungsoptionen können Sie die Option *Stellen Sie den Computer mithilfe eines zuvor erstellten Systemabbilds wieder her* wählen.

INFO

Windows Server 2008 (R2) unterstützt die Wiederherstellung einer Systemsicherung auch auf anderer Hardware. Es muss keine Rücksicht mehr auf den *Hardware Abstraction Layer* (*HAL*) genommen werden. Die neue Hardware muss lediglich zertifiziert für Windows Server 2008 (R2) sein.

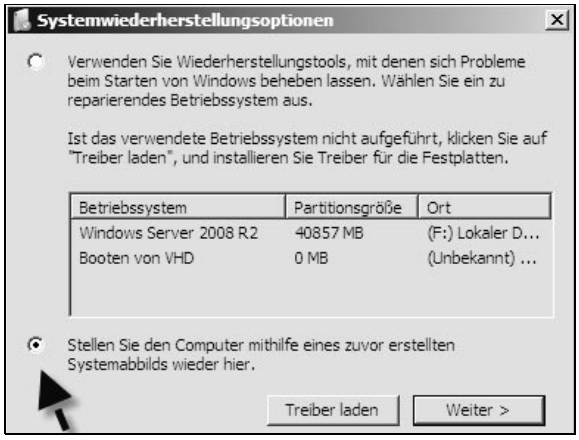


Abbildung 17.20: Komplette Wiederherstellung von Windows Server 2008 (R2)

Als Nächstes durchsucht der Assistent alle verfügbaren Datenträger und der Zeitpunkt, zu dem der Server zurückgesetzt werden soll, kann ausgewählt werden.

Abbildung 17.21: Auswählen der Sicherung, die wiederhergestellt werden soll

Als Nächstes wählen Sie aus, ob Windows den Datenträger formatieren und partitionieren soll oder ob Sie die Daten auf die alte Partition zurücksichern wollen. Über die Schaltfläche *Datenträger ausschließen* wählen Sie die Datenträger aus, die nicht wiederhergestellt werden sollen, weil diese zum Beispiel noch Daten enthalten. Über *Treiber installieren* lassen sich wichtige Treiber integrieren, die für die Wiederherstellung unter Umständen benötigt werden. In den Optionen unter *Erweitert* wird festgelegt, dass der Server automatisch nach der Wiederherstellung neu starten soll und Datenträger auf Defekte überprüft werden.

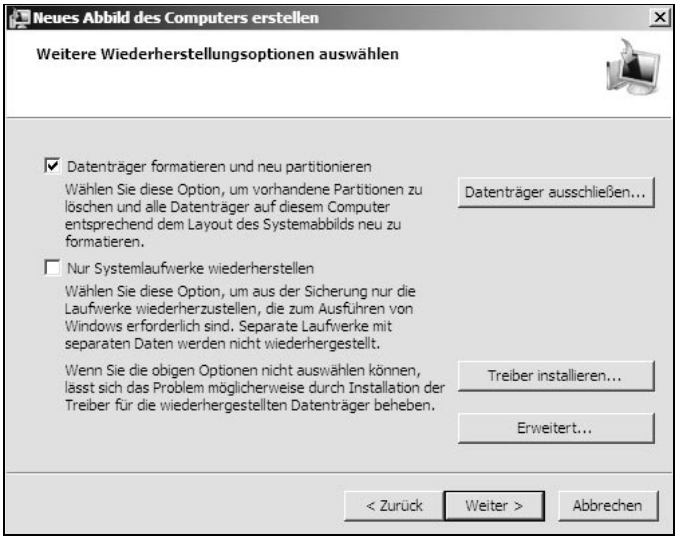


Abbildung 17.22: Auswählen der Wiederherstellungsoptionen des Servers

Als Nächstes wird eine Zusammenfassung angezeigt und Sie können die Eingaben noch mal überprüfen. Als Abschluss erscheint eine Meldung, die darüber informiert, dass die Datenträger, die wiederhergestellt werden, neu formatiert werden müssen. Diese Meldung muss bestätigt werden, bevor die Wiederherstellung beginnt. Anschließend startet der Assistent die Wiederherstellung des Servers. Nach der Wiederherstellung steht der Server wieder zur Verfügung.

17.6.2 Wiederherstellen der Exchange-Komponenten auf einem Server

In manchen Fällen, zum Beispiel bei einem Hardware-Ausfall, kann es notwendig sein, einen kompletten Exchange Server wiederherzustellen, auch wenn keine Sicherung des Systemstatus zur Verfügung steht. Hierzu müssen Sie einige besondere Punkte beachten. Nach einem solchen Vorfall sollten Sie zunächst Ruhe bewahren. Überprüfen Sie genau, wo Sie stehen:

- Welche Daten des Exchange Servers sind mit welchem Stand wo gesichert?
- Gibt es Offline-Backups und wenn ja, von wann?
- Können die Festplatten des Servers gerettet werden oder handelt es sich um einen Totalausfall?
- Haben Sie ausreichend Ersatzhardware vorrätig, um den Server wiederherzustellen?
- Wie groß ist die Datenbank auf der Datensicherung? Danach richtet sich die Dauer der Wiederherstellung.

Steht Ihnen eine Offline-Sicherung der Datenbanken zur Verfügung oder – besser noch – eine Online-Sicherung, sollten Sie diese überprüfen und bereithalten. Besorgen Sie sich die Datenträger und die aktuellen Service Packs für Betriebssystem, Exchange und die Drittherstellersoftware, die auf dem Server installiert waren. Sie sollten alle notwendigen Datenträger zur Verfügung haben, damit Sie den Server nach und nach wiederherstellen können. Installieren Sie auf dem Ersatzserver beziehungsweise auf dem reparierten Server das Betriebssystem. Hier hilft es natürlich ungemein, wenn diese Informationen möglichst genau dokumentiert wurden. Integrieren Sie nach der Installation des Betriebssystems den Server unter seinem alten Namen in Ihrem Active Directory.

Folgende Voraussetzungen sind wichtig für eine solche Wiederherstellung:

- Auf dem Server muss das gleiche Betriebssystem installiert sein. Es ist nicht möglich, auf einen Server mit Windows Server 2008 eine Wiederherstellung auf Basis von Windows Server 2008 (R2) durchzuführen.
- Der Server muss die gleiche Hardwarekonfiguration wie der ausgefallene Server haben. Die Größe des Arbeitsspeichers und der Festplatten kann natürlich variieren.

Verwenden von setup /m:RecoverServer

Nach der Installation des Betriebssystems können Sie mit der Installation von Exchange beginnen. Mit *Setup /m:RecoverServer* werden Server wiederhergestellt, die nicht zu einem Cluster gehören und auch keine Edge-Transport-Server sind. *Setup /m:RecoverServer* kann nur für die Server-Wiederherstellung verwendet werden. Die Verwendung als Reparaturtool zur Wiederherstellung einer fehlerhaften Installation oder Deinstallation sowie zur Neukonfiguration eines Servers ist nicht möglich. *Setup /m:RecoverServer* migriert nur die Einstellungsinformationen, die in Active Directory gespeichert sind. Alle lokalen Anpassungen werden mit dieser Methode nicht migriert.

Gehen Sie dazu folgendermaßen vor:

1. Setzen Sie das Computerkonto des Servers in der Domäne zurück und stellen Sie sicher, dass der Server sich ordnungsgemäß mit dem Active Directory verbunden hat. Hilfreich ist dazu oft der Befehl *dsmod computer <Servername> -reset*. Notfalls löschen Sie das Konto einfach.
2. Installieren Sie das Betriebssystem und geben Sie dem neuen Server den gleichen Namen wie dem ausgefallenen Server.
3. Nehmen Sie den Server in der gleichen Domäne auf, in welcher der ausgefallene Server Mitglied war.
4. Installieren Sie die erforderlichen Voraussetzungen und Betriebssystemkomponenten für Exchange Server 2010 (siehe Kapitel 2).
5. Melden Sie sich am Server an und öffnen Sie eine Eingabeaufforderung.
6. Navigieren Sie zu den Installationsdateien von Exchange Server 2010 und geben Sie den Befehl *Setup /m:RecoverServer* ein.
7. Nach der Installation müssen Sie alle benutzerdefinierten Einstellungen vornehmen, die auf dem Server konfiguriert waren.

Die Option geht von einer konsistenten Konfiguration in Active Directory für den Server aus. Ist ein Installationsfehler aufgetreten, wurden die Informationen in Active Directory möglicherweise nicht vollständig geschrieben. Starten Sie das Exchange-Setup mit dieser Option, liest sich das Setup möglichst viele Daten aus dem Active Directory, die den ursprünglichen Server betreffen. Exchange Server 2010 speichert seine Konfiguration normalerweise in der Metabase des lokalen IIS. In regelmäßigen Abständen werden die wichtigsten Daten durch diese in das Active Directory repliziert. Das Disaster Recovery-Setup versucht anhand der zur Verfügung stehenden Optionen, den Server so gut wie möglich wiederherzustellen. Die Pfade der Datenbank werden auf alle Fälle übernommen. Es ist daher sehr wichtig, dass der neue Server dieselbe Plattenkonfiguration besitzt wie der ursprüngliche Server. Installieren Sie die gleichen Komponenten wie bereits bei der ursprünglichen Installation. Überprüfen Sie nach der Installation die Funktionsfähigkeit des Servers. Nach der erfolgreichen Installation von Exchange müssen Sie die Daten

aktualisieren. Dazu benötigen Sie Ihre Datensicherung. Gehen Sie bei der Wiederherstellung der Daten so vor, wie bereits weiter vorne im Kapitel besprochen.

Nacharbeiten zur Server-Wiederherstellung

Setup /m:RecoverServer stellt die Exchange-Server-Konfigurationsdaten aus Active Directory wieder her, kopiert die Exchange-Dateien auf den Server und legt Standardeinstellungen fest, wenn keine Alternativeinstellungen in Active Directory gefunden wurden. Der Befehl stellt keine angepassten Einstellungen wieder her, die auf dem Server gespeichert waren. Auch in den Exchange-Datenbanken auf dem Server gespeicherte Endbenutzerdaten werden nicht wiederhergestellt. Für jede Serverfunktion sind unterschiedliche Schritte und Wiederherstellungen notwendig, damit die Funktion den Status besitzt, den sie vor der Wiederherstellung hatte:

- Die Postfach- und Öffentliche-Ordner-Datenbanken auf einem Mailbox-Server müssen wiederhergestellt werden. Werden die öffentlichen Ordner auf dem Server alle auf einen anderen Server repliziert, könnten Sie eine neue leere Öffentliche-Ordner-Datenbank erstellen und diese aus anderen Replikaten abgleichen.
- Unified-Messaging-Telefonansagen und benutzerdefinierte Audiodateien auf einem Unified-Messaging-Server müssen wiederhergestellt werden, wenn der Server die Dateifreigabe für Telefonansagen für einen Wählplan war. Andernfalls werden die Daten vom Server für die Dateifreigabe für Telefonansagen wiederhergestellt.
- Alle benutzerdefinierten Outlook Web Access-Dateien oder virtuelle Verzeichnisse auf einem Clientzugriffsserver müssen erneut erstellt werden.
- Alle benutzerdefinierten Einstellungen, die auf den Servern konfiguriert waren, müssen erneut konfiguriert werden.

17.7 Wiederherstellen von Postfachdatenbanken im Detail

Haben Sie Ihre Postfachdatenbank mit einer Online-Datensicherung gesichert, können Sie diese bei Datenverlust oder Defekt relativ leicht wiederherstellen. Wir erklären Ihnen in diesem Abschnitt detaillierter, wie Sie eine Postfachdatenbank aus einer Sicherung wiederherstellen können. Bevor Sie eine defekte Datenbank wiederherstellen, sollten Sie zunächst den Informationsspeicherdienst beenden oder die Bereitstellung der defekten Datenbank aufheben. Sichern Sie dann die *.edb-Datei auf einen anderen Datenträger. Sollte die Datensicherung nicht alle notwendigen Daten enthalten, dann können Sie unter Umständen auch von einer defekten Datenbank noch E-Mails exportieren. Haben Sie eine defekte Postfachdatenbank oder hegen Sie den Verdacht, dass eine Ihrer Postfachdatenbanken nicht mehr funktioniert, hat sich folgende Vorgehensweise bewährt:

1. Sichern Sie zunächst die Datenbankdatei (*.edb) und eventuell auch die anderen Dateien der Postfachdatenbank auf einen anderen Datenträger, bevor Sie irgendwelche Aktionen durchführen.
2. Versuchen Sie, mit *Eseutil* die Datenbank zu reparieren (siehe Kapitel 7).
3. Lässt sich die produktive Datenbank nicht mehr reparieren und haben Sie auch keine Database Availability Group (DAG), spielen Sie die letzte Datensicherung zurück, die Ihnen zur Verfügung steht.

17.7.1 Postfachdatenbank wiederherstellen

Sie sollten zunächst die Dateien der Datenbank sichern, bevor Sie Wiederherstellungsvorgänge durchführen. Um die Dateien offline zu sichern, müssen Sie zuvor den Informationsspeicherdienst beenden oder die Bereitstellung aller Datenbanken aufheben, die sich unterhalb der Postfachdatenbank befinden. Um eine Postfachdatenbank aus der Datensicherung auf dem produktiven Server zurückzusichern, gehen Sie folgendermaßen vor:

1. Rufen Sie in der Exchange-Verwaltungskonsole die Eigenschaften der Postfachdatenbank auf, die Sie zurücksichern wollen.
2. Aktivieren Sie die Option *Diese Datenbank kann bei einer Wiederherstellung überschrieben werden*.
3. Als Nächstes sollten Sie die Bereitstellung der Datenbank aufheben, die Sie wiederherstellen wollen. Klicken Sie diese dazu mit der rechten Maustaste an und wählen Sie die Option *Bereitstellung der Datenbank aufheben*.

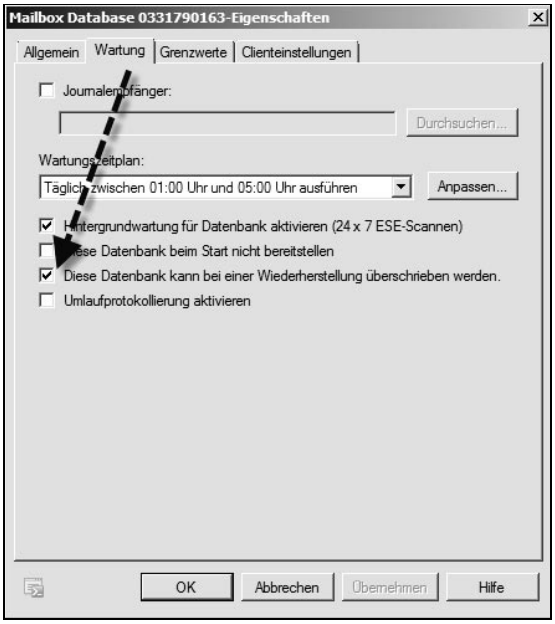


Abbildung 17.23: Vorbereiten einer Datenbank zur Wiederherstellung aus einer Sicherung

4. Starten Sie anschließend das Datensicherungsprogramm und wählen Sie die Option zur Wiederherstellung von Daten.
5. Als Nächstes müssen Sie den Sicherungssatz öffnen, aus dem Sie Daten wiederherstellen wollen. Wurde der Sicherungssatz geöffnet, müssen Sie die Datenbank aktivieren, aus der Sie Daten wiederherstellen wollen.
6. Aktivieren Sie bei der Wiederherstellung der Datenbank im Datensicherungsprogramm immer die Option *Letzter Wiederherstellungssatz (Protokolldateiwiederholung folgt darauf)*. Sollte in Ihrem Datensicherungsprogramm diese Option nicht zur Verfügung stehen oder sollten Sie vergessen haben, sie zu aktivieren, können Sie nach der Wiederherstellung der Datenbank mit dem Tool *Eseutil* die Wiederherstellung nachträglich beeinflussen. Die Aktivierung der Option *Letzter Wiederherstellungssatz* dient zum nachträglichen Abarbeiten der Transaktionsprotokolle durch den Server. Bei der Windows-Server-Sicherung erfolgt diese Wiederherstellung, indem Sie die Rollforward-Wiederherstellung nicht deaktivieren. Diese Option steht zur Verfügung, wenn Sie eine Wiederherstellung durchführen. Dieser Vorgang wird Hard-Recovery genannt (im Gegensatz zum beschriebenen Soft-Recovery zu Beginn dieses Kapitels).

17.7.2 Wiederherstellen einer Offline-Sicherung

Um eine Exchange-Datenbank mit einer Offline-Sicherung wiederherzustellen, stehen Ihnen zwei verschiedene Möglichkeiten zur Verfügung:

1. Sind die aktuellen Transaktionsprotokolle verfügbar, können diese Protokolle in die Offline-Sicherung eingespielt und diese dadurch auf den aktuellsten Stand gebracht werden. Diese Sicherung wird *Roll forward* genannt.
2. Ist Ihr Server ausgefallen und stehen keine Transaktionsprotokolle zur Verfügung, müssen Sie die Offline-Sicherung ohne Transaktionsprotokolle zurückspielen. Alle weiteren Daten nach dieser Sicherung sind unwiederbringlich verloren. Diese Wiederherstellung wird *Point in Time* genannt.

Point-in-Time-Wiederherstellung aus einer Offline-Sicherung

Um eine Point-in-Time-Wiederherstellung durchzuführen, müssen Sie zunächst die Bereitstellung für alle Datenbanken der Postfachdatenbank aufheben. Für die Wiederherstellung müssen Sie auf die *.chk-Datei der Transaktionsprotokolle zurückgreifen. Alle Datenbanken einer Postfachdatenbank verwenden denselben Satz Transaktionsprotokolle und daher auch dieselbe *.chk-Datei. Als Nächstes sollten Sie die Checkpoint-Datei überprüfen. Diese Datei befindet sich in dem Verzeichnis, das Sie in den Eigenschaften als Systempfad angegeben haben. Damit Sie auf diese Checkpoint-Datei zugreifen können, müssen alle Datenbanken deaktiviert sein. Ist eine Datenbank noch aktiv, greift sie auf die Checkpoint-Datei zu. Um die Checkpoint-Datei zu überprüfen, verwenden Sie *Eseutil*. Geben Sie in der

Befehlszeile einfach folgende Befehle ein. Sie müssen sich dazu aber im Verzeichnis mit der Datenbank befinden.

Eseutil /mk E00.chk

Eseutil /ml E00.log

In der Ausgabe der beiden Befehle können Sie vergleichen, ob die Daten übereinstimmen. Trifft dies zu, kann die *.chk-Datei der Datenbank zugeordnet werden. Als Nächstes können Sie die *.edb-Datei der Datenbank wiederherstellen. Kopieren Sie die Datei auf dem zugeordneten Pfad auf dem Datenträger. Überprüfen Sie, ob die Datei konsistent ist. Verwenden Sie dazu das Tool *Eseutil.exe*. Sollte sich im Pfad bereits eine *.edb-Datei befinden, kopieren Sie diese vorher. Auch wenn die Datenbank defekt ist, lässt sie sich eventuell wiederherstellen. Haben Sie die Datenbanken kopiert, können Sie diese in der Exchange-Verwaltungskonsole bereitstellen.

Rollforward-Wiederherstellung einer Offline-Sicherung

Ist eine Datenbank defekt, haben Sie aber alle Transaktionsprotokolle seit der letzten Offline-Sicherung zur Verfügung, können Sie eine Rollforward-Wiederherstellung durchführen. Für eine Rollforward-Wiederherstellung aus einer Offline-Sicherung werden alle Transaktionsprotokolle benötigt, die nach dem Offline-Backup erstellt wurden, auch die Datei *E0n.log*. Diese Datei enthält alle Transaktionen, die aktuell von der Datenbank verwendet wurden und noch nicht in einem Transaktionsprotokoll gespeichert sind. Sind die Transaktionsprotokolle nicht vollständig vorhanden, wird bei der Wiederherstellung ein Fehler in der Ereignisanzeige erzeugt, der Sie darauf hinweist, dass Daten verloren gehen. Die Checkpoint-Datei kann gelöscht werden, da diese falsche Informationen darüber enthält, welche Transaktionsprotokolle bereits in die Datenbank geschrieben sind. Die aktuelle Checkpoint-Datei enthält nur die Informationen, welche Transaktionsprotokolle in die Datenbank geschrieben wurden, die durch die Wiederherstellung überschrieben wird. Da Sie eine Datenbank aus einer Offline-Sicherung wiederherstellen wollen, müssen alle Transaktionsprotokolle erneut in die Datenbank geschrieben werden und zwar in die wiederhergestellte Datenbank aus der Offline-Sicherung. Heben Sie die Bereitstellung der Datenbank auf, die Sie wiederherstellen wollen. Heben Sie auch die Bereitstellung aller anderen Datenbanken dieser Postfachdatenbank auf. Während der Wiederherstellung aus einer Offline-Sicherung darf die Datenbank nicht bereitgestellt werden und es dürfen keine Benutzer verbunden sein. Als Nächstes sollten Sie mit *Eseutil* alle Datenbankdateien auf Konsistenz überprüfen. Verwenden Sie zum Überprüfen der Konsistenz folgenden Eseutil-Befehl:

Eseutil /mh < *Pfad zur Datenbankdatei* >

Hat die Datenbank einen inkonsistenten Wert, wurde sie wahrscheinlich von Exchange nicht sauber heruntergefahren. In einem solchen Fall sollten Sie die

Datenbank wieder bereitstellen und die Bereitstellung nochmals aufheben. Dann sollte die Datenbank allerdings konsistent sein.

Um eine Datenbank zu aktualisieren, ist der Stand der Offline-Sicherung vollkommen egal. Es ist allerdings sehr wichtig, dass Sie alle Transaktionsprotokolle seit dieser Offline-Sicherung lückenlos zur Verfügung stellen können. Sie können eine vollständige Rollforward-Wiederherstellung nur dann ausführen, wenn sich nach dem Erstellen der Offline-Sicherung die Datenbank immer noch am selben Speicherort befindet und nicht verschoben wurde.

Haben Sie die Datenbank nach dem Erstellen einer Offline-Sicherung verschoben, können Sie lediglich die Transaktionsprotokolle wiederherstellen, die vor dem Verschieben erstellt wurden. Die Transaktionsprotokolle enthalten unter anderem den Pfad zur Datenbank. Dieser Pfad wurde auch in die *.edb-Datei der Datenbank geschrieben. Diese Datei muss daher an ihrem ursprünglichen Ort wiederhergestellt werden. Überprüfen Sie, ob im Pfad der Transaktionsprotokolle alle Protokolle seit der Offline-Sicherung enthalten sind. Ist das nicht der Fall, kopieren Sie alle Transaktionsprotokolle aus der Datensicherung auf den Pfad.

Falls noch nicht geschehen, löschen Sie die Checkpoint-Datei (*E0n.chk*). Kopieren Sie die Offline-Sicherung in das entsprechende Verzeichnis und stellen Sie die Postfachdatenbank wieder bereit. Haben Sie den Informationsspeicherdienst beendet, starten Sie ihn wieder. Es werden alle Transaktionsprotokolle in die Datenbanken geschrieben. Dieser Vorgang kann je nach Größe der Datenbank und Anzahl der Protokolle etwas dauern. Nach diesen Schritten sollte Ihnen Ihr Informationsspeicher wieder zur Verfügung stehen.

17.7.3 Probleme beim Offline-Backup

Wollen Sie ein Offline-Backup auf einem getrennten Wiederherstellungsserver und nicht auf dem Produktivserver wiederherstellen, kann es vorkommen, dass bei einem Roll forward keine Transaktionsprotokolle in die Offline-Datenbank eingelesen werden. Dieses Problem kann auftreten, wenn Sie einen dedizierten Wiederherstellungsserver installiert haben und dieser Server keinen Zugriff auf das Active Directory hat. Bei einem Soft-Recovery überprüft Exchange während des Wiederherstellungsvorgangs und des selbstständigen Schreibens von Transaktionsprotokollen in die Datenbank in regelmäßigen Abständen die GUID der Datenbank in Active Directory. Hat Exchange während der Wiederherstellung keinen Zugriff auf das Active Directory, geht Exchange davon aus, dass die Transaktionsprotokolle nicht zu der Datenbank gehören, und schreibt diese dann nicht in den Informationsspeicher. Um dieses Problem zu lösen, installieren Sie am besten eine Kopie des produktiven Active Directory, auf das der Wiederherstellungsserver Zugriff hat.

17.8 Wiederherstellungsdatenbanken verwenden

Exchange Server 2010 unterstützt die Möglichkeit, Daten direkt in einer Wiederherstellungsdatenbank wiederherzustellen. Eine Wiederherstellungsdatenbank ist eine spezielle Art von Postfachdatenbank. Mit dieser können Sie eine wiederhergestellte Postfachdatenbank verbinden und anschließend mit dem CMDlet *Restore-Mailbox* Daten extrahieren. Die Daten lassen sich in einen Ordner exportieren oder in ein Postfach importieren. Mit Wiederherstellungsdatenbanken können Sie Daten aus einer Sicherung wiederherstellen, ohne Benutzer zu beeinträchtigen. Wiederherstellungsdatenbanken erstellen Sie in der Exchange-Verwaltungsshell, die Erstellung in der Exchange-Verwaltungskonsole ist nicht möglich.

17.8.1 Grundlagen von Wiederherstellungsdatenbanken

Wiederherstellungsdatenbanken unterstützen nur die Wiederherstellung von Postfachdatenbankdaten. Daten in Öffentlichen Ordnern können nicht mit einer Wiederherstellungsdatenbank wiederhergestellt werden. Sie können nur eine Wiederherstellungsdatenbank auf einem Postfachserver erstellen. Die Datenbanken zur Wiederherstellung können keine E-Mails empfangen oder Benutzer anbinden, zählen dafür aber auch nicht zur Begrenzung der Datenbanken auf einem Server dazu. Der gesamte Clientprotokollzugriff auf eine Wiederherstellungsdatenbank ist blockiert. Wiederherstellungsdatenbanken unterstützen MAPI aber nur über Wiederherstellungstools. Postfächer in einer Wiederherstellungsdatenbank lassen sich nicht mit Benutzerkonten verbinden. System- und Postfachverwaltungsrichtlinien unterstützen diese Datenbanken ebenfalls nicht. Auch die Online-Wartung wird für Wiederherstellungsdatenbanken nicht durchgeführt. Sie können für Wiederherstellungsdatenbanken keine Umlaufprotokollierung aktivieren (siehe auch Kapitel 7). Postfachdatenbankkopien (siehe Kapitel 21) lassen sich nicht mit Wiederherstellungsdatenbanken verbinden. Wiederherstellungsdatenbanken können Sie nur für Exchange Server 2010-Postfachdatenbanken verwenden.

17.8.2 Erstellen einer Wiederherstellungsdatenbank

Nachdem Sie eine Wiederherstellungsdatenbank erstellt haben, können Sie eine wiederhergestellte Postfachdatenbank in die Wiederherstellungsdatenbank verschieben und mit dem CMDlet *Restore-Mailbox* exportieren. Der Befehl zum Erstellen einer Wiederherstellungsdatenbank ist folgender:

New-MailboxDatabase -Recovery -Name <Name der Datenbank -Server <Servername>

Der Parameter *–Server* muss auch angegeben werden, wenn die Datenbank auf dem lokalen Server angelegt werden soll, zum Beispiel:

New-MailboxDatabase -Recovery -Name recovery -Server x2k10

Abbildung 17.24: Erstellen einer Wiederherstellungsdatenbank

Sie können eine Datenbank auch in einem eigenen Pfad erstellen, der auch die Protokolldateien enthält. Die Syntax dazu ist:

New-MailboxDatabase -Recovery -Name < Name der Datenbank > -Server < Server > -EdbFilePath » < Pfad zur Datenbankdatei > « -LogFolderPath » < Pfad zu den Protokolldateien«

Der Parameter *–EdbFilePath* muss dabei ein Dateiname sein, dessen Erweiterung auf .edb endet.

17.8.3 Wiederherstellen von Daten mit einer Wiederherstellungsdatenbank

Wollen Sie Daten einer Postfachdatenbank, zum Beispiel einzelne Postfächer, über eine Wiederherstellungsdatenbank wiederherstellen, müssen Sie zunächst auf dem Server eine solche Wiederherstellungsdatenbank erstellen. Als Nächstes stellen Sie die Datenbank, aus der Sie Daten wiederherstellen wollen, wieder her und verwenden dazu den Pfad der Wiederherstellungsdatenbank.

Die wiederhergestellte Datenbank muss den Status *Clean Shutdown* aufweisen. Als Nächstes sollten Sie mit *Eseutil* die Datenbank auf Konsistenz prüfen. Nach der Eingabe des Befehls erscheint auf dem Bildschirm die Ausgabe der Abfrage. Suchen Sie hier die Zeile mit dem Status der Datenbank. Da die Wiederherstellungsdatenbank einen alternativen Wiederherstellungsort darstellt, weisen wiederhergestellte Datenbanken den Status *Dirty Shutdown* auf. Mit *Eseutil /R* können Sie die wiederhergestellte Datenbank in den Status *Clean Shutdown* versetzen. Mit *Restore-Mailbox -Identity < Name des Postfachs > -RecoveryDatabase < Name der Recovery-Datenbank >* können Sie dann Daten auslesen.

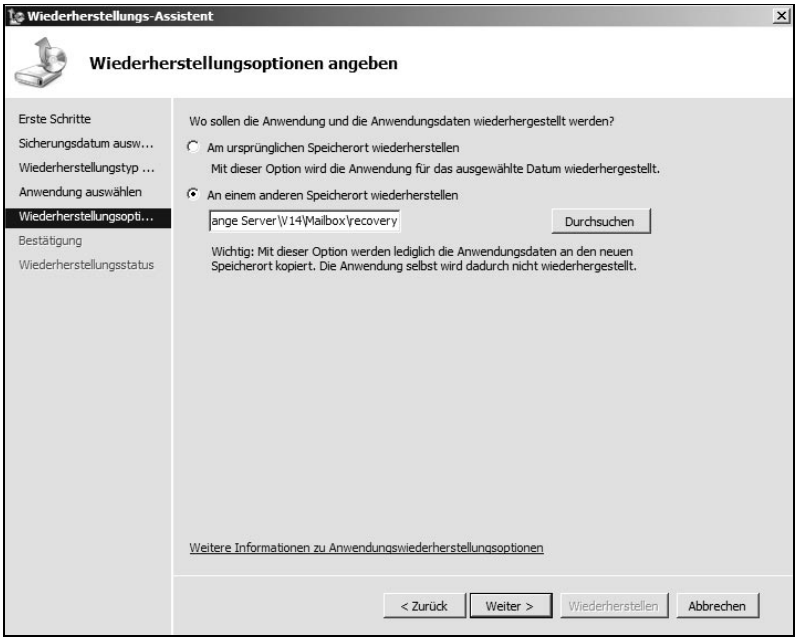


Abbildung 17.25: Wiederherstellen einer Postfachdatenbank im Pfad der Wiederherstellungsdatenbank

17.9 Verwenden der Datenbankportabilität

In Exchange Server 2007/2010 können Sie durch die *Datenbankportabilität* eine Postfachdatenbank auf jedem Server innerhalb der Organisation bereitstellen. In Exchange Server 2003 und Exchange 2000 Server mussten Sie beim Verschieben einer Datenbank auf einen anderen Server innerhalb derselben administrativen Gruppe verschiedene Punkte berücksichtigen. Die Datenbankportabilität können Sie nur für Exchange Server 2010-Postfachdatenbanken verwenden, Sie können keine Versionen miteinander mischen. Datenbankportabilität steht nur für die Postfachdatenbanken zur Verfügung. Öffentliche Ordnerdatenbanken sind nicht portierbar. Die beste Methode, öffentliche Ordner zwischen Servern zu verschieben, besteht darin, sie zu replizieren, anstatt die Datenbankdateien auf einen anderen Server zu kopieren. Kopieren Sie eine Öffentliche-Ordner-Datenbank auf einen anderen Server, wird sie nicht mehr zusammen mit den anderen Datenbanken repliziert. Gehen Sie zum Verschieben einer Postfachdatenbank auf einen anderen Server in der Organisation folgendermaßen vor:

1. Um eine Datenbank mithilfe der Datenbankportabilität auf einem anderen Server in der Organisation zu starten, verwenden Sie eine Offline-Sicherung dieser Datenbank. Heben Sie dazu zunächst die Bereitstellung der Datenbank auf.

2. Als Nächstes sollten Sie mit *Eseutil* die Datenbank auf Konsistenz prüfen und sicherstellen, dass diese sauber heruntergefahren worden ist. Verwenden Sie dazu den Befehl *Eseutil /mh <Pfad zur Datenbankdatei>*.
3. Im nächsten Schritt erstellen Sie auf dem Zielserver eine neue, leere Datenbank. Geben Sie dieser Datenbank exakt die gleiche Bezeichnung wie auf dem Quellserver.
4. Rufen Sie anschließend die Eigenschaften der neuen Datenbank auf dem Zielserver auf und setzen Sie auf der Registerkarte *Wartung* die Option *Diese Datenbank kann bei einer Wiederherstellung überschrieben werden*.
5. Verschieben Sie die Datenbankdateien (*.edb-Dateien, Protokolldateien und den Inhaltsindizierungskatalog) an den entsprechenden Speicherort. Die Datenbankdateien müssen auf dem neuen Server vorhanden sein und am richtigen Speicherort vorliegen.
6. Stellen Sie die Datenbank bereit.
7. Haben Sie die Datenbank bereitgestellt, müssen Sie die Benutzerkonteneinstellungen ändern, damit Konten auf das Postfach auf dem neuen Mailbox-Server verweisen. Führen Sie den folgenden Befehl aus: *Get-Mailbox -Database <Quell-Datenbank> |where {$_.ObjectClass -NotMatch '(SystemAttendantMailbox|ExOleDbSystemMailbox)'}| Set-Mailbox -Database <Ziel-Datenbank>*. Der Befehl liest die entsprechenden Postfächer aus und ändert deren Datenbank auf die neue Bezeichnung ab.
8. War ein neues Postfach vorhanden, das keine E-Mail empfangen hat oder dessen E-Mails nicht geöffnet wurden, verschiebt dieser Befehl dieses Postfach nicht, weil es im Informationsspeicher nicht vorhanden ist. Wurde die Replikation des Active Directory abgeschlossen, können alle Benutzer auf ihre Postfächer auf dem neuen Exchange-Server zugreifen. Outlook 2007/2010-Clients werden mithilfe von Autodiscovery umgeleitet (siehe Kapitel 11). Outlook Web Access-Benutzer werden automatisch auf den neuen Server umgeleitet.

17.10 Dial-Tone-Wiederherstellung

Durch die *Dial-Tone-Portabilität* können Sie das Postfach eines Benutzers verschieben, ohne dass Zugriff auf die Inhalte des Postfachs erforderlich ist. Auf diese Weise können Server die Postfächer von Benutzern speichern, die sich zuvor auf einem anderen Server befunden haben, der nicht mehr verfügbar ist. Mit dem automatischen Erkennungsdienst (Autodiscover, siehe Kapitel 11) von Outlook 2007/2010 und Exchange Server 2010 werden Clients auf den neuen Server umgeleitet, wenn sie versuchen, eine Verbindung herzustellen. Es ermöglicht Benutzern während des Wiederherstellungsvorgangs ihres ursprünglichen Postfachs das Senden und Empfangen von E-Mails ohne Zugriff auf die auf dem Server gespeicherten Daten. Das

temporäre Postfach kann sich auf demselben Exchange-Server-2010-Postfachserver oder auf einem anderen Exchange-2010-Postfachserver in der Organisation befinden:

1. Eine Dial-Tone-Datenbank erstellen Sie mit dem CMDlet *New-MailboxDatabase*, zum Beispiel mit *New-MailboxDatabase -Name DTDB1 -EdbFilePath C:\DialTone\DTDB1.EDB.*
2. Mit dem CMDlet *Set-Mailbox* ändern Sie die Konfiguration der Benutzerpostfächer, damit diese auf die neue Datenbank verweisen: *Get-Mailbox -Database <Quell-Datenbank> | Set-Mailbox -Database DTDB1.*
3. Mit dem CMDlet *Mount-Database* stellen Sie die Dial-Tone-Datenbank bereit: *Mount-Database -Identity DTDB1.*
4. Erstellen Sie eine Wiederherstellungsdatenbank und stellen Sie die Quelldatenbank wieder her oder kopieren Sie die Daten.
5. Nachdem Sie die Daten in die Wiederherstellungsdatenbank kopiert haben, kopieren Sie noch die Transaktionsprotokolle aus der fehlerhaften Datenbank in den Protokollordner der Wiederherstellungsdatenbank.
6. Stellen Sie die Wiederherstellungsdatenbank bereit und heben Sie dann die Bereitstellung wieder auf. Verwenden Sie dazu hintereinander die Befehle *Mount-Database -Identity <Wiederherstellungsdatenbank>* und dann *Dismount-Database -Identity <Wiederherstellungsdatenbank>*.
7. Nachdem Sie die Bereitstellung aufgehoben haben, verschieben Sie die aktuelle Datenbank und die Protokolldateien aus dem Ordner *Wiederherstellungsdatenbank* in ein anderes Verzeichnis.
8. Heben Sie die Bereitstellung der Dial-Tone-Datenbank auf.
9. Verschieben Sie die Dial-Tone-Datenbank und die Protokolldateien aus dem Ordner der Dial-Tone-Datenbank in den Ordner der Wiederherstellungsdatenbank.
10. Verschieben Sie die Datenbank und die Protokolldateien aus dem Verzeichnis, in dem sich die wiederhergestellte Datenbank befindet, in den Ordner der Dial-Tone-Datenbank und stellen Sie dann die Datenbank bereit.
11. Verwenden Sie die CMDlets *Get-Mailbox* und *Restore-Mailbox*, um Daten aus der Wiederherstellungsdatenbank zu exportieren und in die wiederhergestellte Datenbank zu importieren. Alle E-Mails, die Empfänger über die Dial-Tone-Datenbank senden, werden dabei in die Produktionsdatenbank importiert.
12. Sobald der Wiederherstellungsvorgang abgeschlossen ist, können Sie die Bereitstellung der Wiederherstellungsdatenbank aufheben und die Datenbank entfernen: *Remove-MailboxDatabase -Identity <Wiederherstellungsdatenbank>*.

17.11 Konfiguration der Aufbewahrungszeit für gelöschte Elemente und Postfächer

Das erneute Verbinden einzelner Postfächer kann notwendig sein, wenn Sie versehentlich einen Benutzer mit Postfach gelöscht haben. Bei Exchange Server 2010 sind die Postfächer von Benutzern mit dem Benutzerobjekt in Active Directory verbunden. Wird das Konto des Benutzers von Active Directory gelöscht, wird auch das entsprechende Postfach des Benutzers aus der Exchange-Datenbank gelöscht. Damit durch diese enge Verbindung von Postfach und Benutzer nicht versehentlich Daten gelöscht werden, hat Exchange einen Mechanismus eingebaut, der Postfächer vor einem Löschvorgang schützt. Wird ein Benutzer mit Postfach gelöscht, bewahrt Exchange das Postfach des Benutzers standardmäßig weitere 30 Tage auf, bevor es endgültig aus dem System gelöscht wird. In diesem Zeitraum kann das Postfach jederzeit wieder mit einem neuen Benutzer verbunden werden. Sie können diesen Grenzwert in den Eigenschaften der Postfachdatenbank auf der Registerkarte *Grenzwerte* im Bereich *Löscheinstellungen* festlegen. Verwenden Sie dazu die Option *Gelöschte Postfächer aufbewahren für (Tage)*. Ihnen stehen zur Konfiguration der Aufbewahrungszeit von gelöschten Objekten zwei Optionen zur Verfügung:

- *Gelöschte Objekte aufbewahren für (Tage)* – Löschen Benutzer Objekte, werden diese in den gelöschten Objekten des Postfachs aufbewahrt. Exchange Server 2010 markiert diese Objekte nur als gelöscht. Sie können jedoch während des definierten Zeitraums wiederhergestellt werden. Zu diesem Zweck gibt es die Option *Gelöschte Elemente wiederherstellen* in Outlook.
- *Gelöschte Postfächer aufbewahren für (Tage)* – Hier legen Sie fest, wie lange ein gelöschtes Postfach wieder mit einem neuen Benutzer in Active Directory verbunden werden kann, bevor es endgültig gelöscht wird.

TIPP

Geben Sie den *Befehl Set-Mailbox –Identity <Postfach> –LitigationHoldEnabled $true* in der Exchange-Verwaltungsshell für ein Postfach ein (siehe auch Kapitel 10), löscht Exchange E-Mails in diesem Postfach niemals. Auf diesem Weg lassen sich gelöschte E-Mails aus dem Exchange-Papierkorb jederzeit wiederherstellen. Wie das geht, zeigen wir Ihnen in den nächsten Abschnitten.

Standardmäßig sind für Datenbanken Grenzwerte definiert die festlegen, wie viele Daten wiederhergestellt werden können. Ab 20 GB erhalten Administratoren eine Warnung, ab 30 GB lassen sich keine weiteren Daten mehr wiederherstellen. Sie können sich diese Grenzwerte mit dem CMDlet *Get-MailboxDatabase* anzeigen. Mit dem Befehl *Get-MailboxDatabase <Datenbank> |fl Recoverable** zeigt die Exchange-Verwaltungsshell nur diese Informationen an.

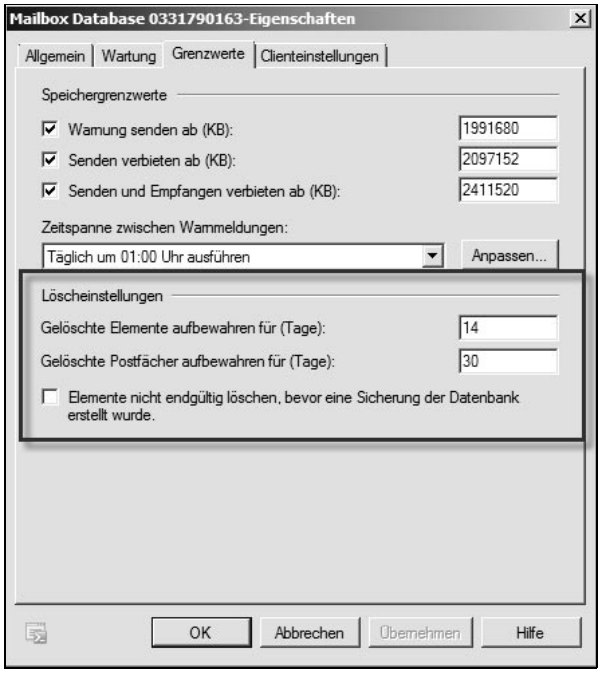


Abbildung 17.26: Konfiguration des Grenzwerts für das Löschen von Postfächern

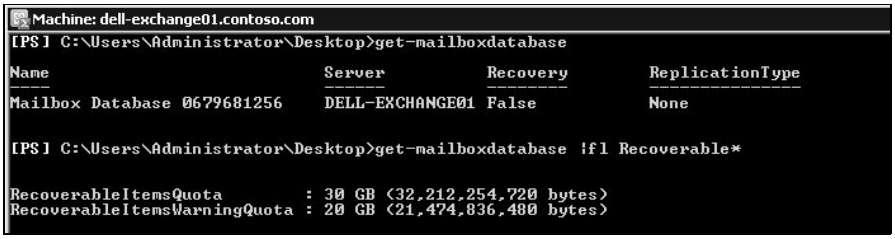


Abbildung 17.27: Anzeigend er Grenzwerte für wiederherstellbare Items

17.12 Löschen und Wiederherstellen gelöschter E-Mails mit Outlook – der Exchange-Server-Papierkorb

Löschen Sie eine E-Mail über das Kontextmenü, durch Drücken der Taste (*Entf*) oder das Auswählen des Icons im Menüband, verschiebt Outlook die Mail in den Ordner *Gelöschte Elemente*, den Sie in den Eigenschaften des Kontos festgelegt haben. Die Elemente verbleiben so lange im Ordner *Gelöschte Elemente*, bis Sie diese auch aus diesem Ordner entfernen oder den Ordner über das Kontextmenü leeren lassen. Bevor Sie den Ordner leeren, erhalten Sie eine Information von Outlook, die Sie bestätigen müssen. Wollen Sie diese Bestätigung deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Registerkarte *Datei*.
2. Klicken Sie auf *Optionen*.
3. Klicken Sie auf *Erweitert*.
4. Ganz unten im Fenster finden Sie den Bereich *Weitere*.
5. Entfernen Sie den Haken bei der Option *Zur Bestätigung auffordern, bevor Elemente endgültig gelöscht werden*.
6. Klicken Sie auf *OK*.
7. Wenn Sie jetzt über das Kontextmenü den Ordner *Gelöschte Elemente* leeren, müssen Sie diese Aktion nicht mehr bestätigen.

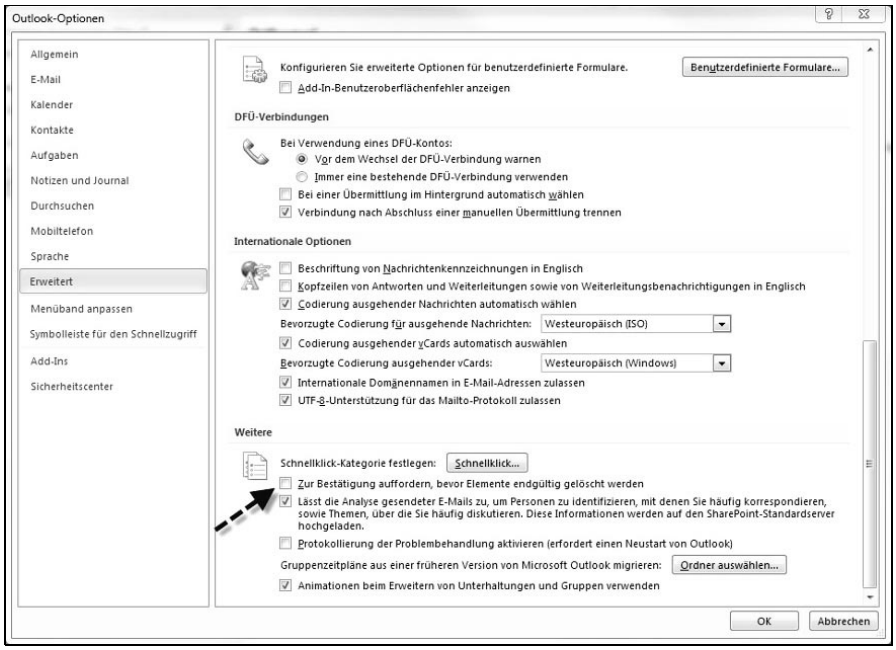


Abbildung 17.28: Deaktivieren der Bestätigung zum Löschen von E-Mails

TIPP

In den Optionen von Outlook 2010, die Sie über die Registerkarte *Datei* erreichen, können Sie im Bereich *Erweitert* bei *Starten und Beenden von Outlook* die Option *Beim Beenden von Outlook die Ordner Gelöschte Elemente leeren* aktivieren. In diesem Fall leert Outlook automatisch den Outlook-Papierkorb der Konten, die Daten auf dem Rechner speichern.

Deaktivieren Sie zusätzlich noch die Option *Zur Bestätigung auffordern, bevor Elemente endgültig gelöscht werden* ganz unten im Fenster im Bereich *Weitere*, erscheint keine Rückfrage dieses Löschvorgangs.

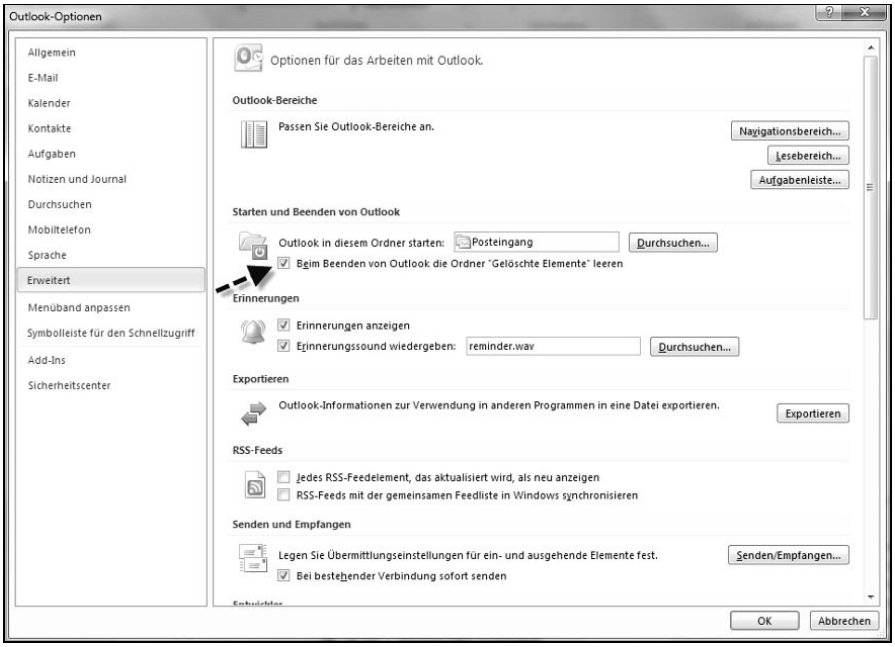


Abbildung 17.29: Automatisches Löschen von E-Mails beim Beenden von Outlook

17.12.1 Wiederherstellen von E-Mails in Outlook 2007/2010

Anwender können mithilfe von Outlook 2003/2007 und Outlook 2010 gelöschte Elemente selbst wiederherstellen. Dazu wird in Outlook am besten der Ordner *Gelöschte Objekte* markiert und anschließend über das Menü *Extras/Gelöschte Elemente wiederherstellen* gewählt. Damit dieser Befehl zur Verfügung steht, muss jedoch ein spezielles Add-In in Outlook 2003/2007 aktiviert sein. Der Anwender kann das Snap-In bei Bedarf selbst installieren, wenn er das Menü aufruft. Die Installation wird anschließend von Outlook selbst durchgeführt.

Nach der Auswahl des Menüpunkts werden die E-Mails angezeigt, die gelöscht wurden und sich nicht mehr im Ordner *Gelöschte Objekte* befinden. Diese E-Mails können in diesem Fenster vom Exchange Server wiederhergestellt werden und sind anschließend im Ordner *Gelöschte Objekte* wieder verfügbar.

Die Anwender können mithilfe von Outlook 2010 gelöschte Elemente selbst wiederherstellen, wenn diese noch innerhalb der besprochenen Grenzwerte im vorangegangenen Abschnitt liegen. Dazu markieren Sie in Outlook am besten den Ordner *Gelöschte Elemente*. In Outlook 2010 finden Sie die Wiederherstellung über den Menüpunkt *Ordner* bei *Gelöschte Elemente wiederherstellen*.

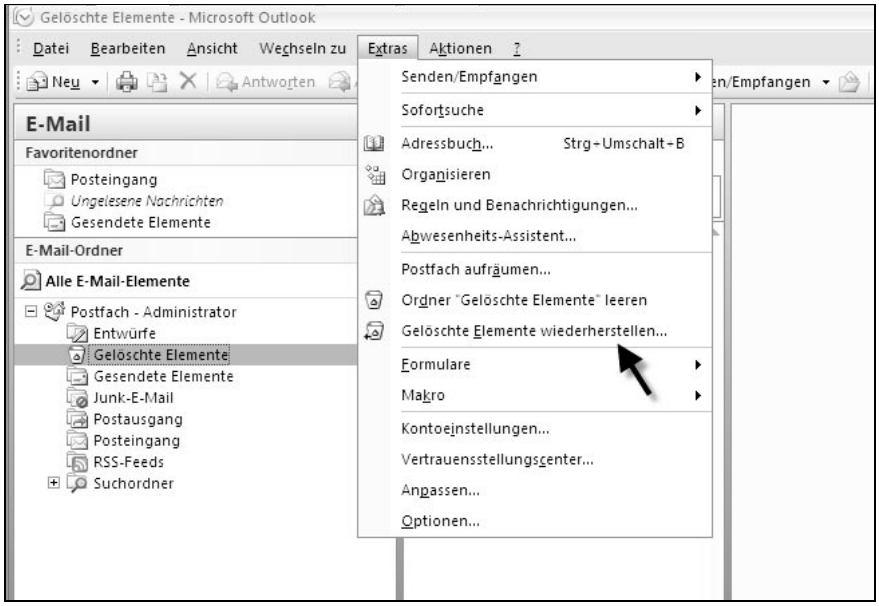


Abbildung 17.30: Wiederherstellen gelöschter Objekte in Outlook 2007

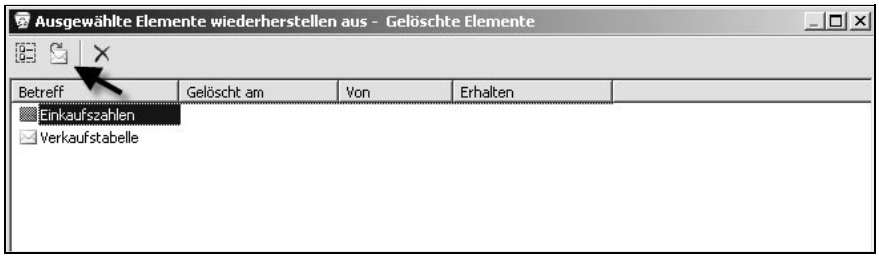


Abbildung 17.31: Wiederherstellen von E-Mails in Outlook

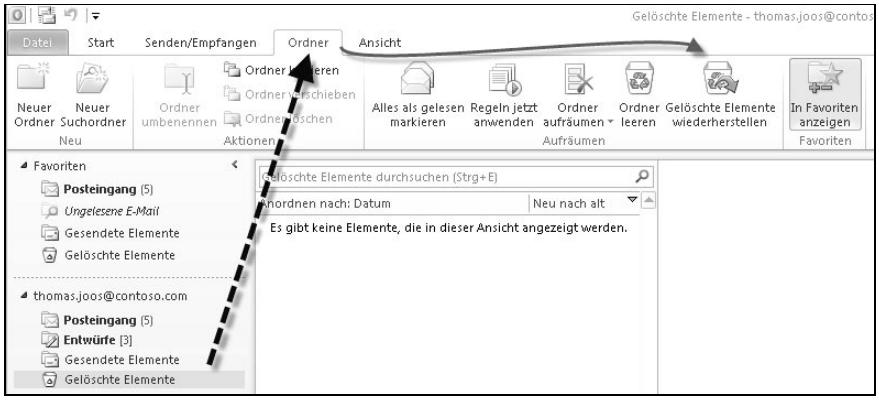


Abbildung 17.32: Wiederherstellen gelöschter Objekte in Outlook 2010

Über das Kontextmenü des Ordners *Gelöschte Elemente* steht in Outlook 2010 die gleiche Option zur Verfügung. Auch über Outlook Web App können Sie über das Kontextmenü des Ordners *Gelöschte Elemente* einzelne E-Mails wiederherstellen.

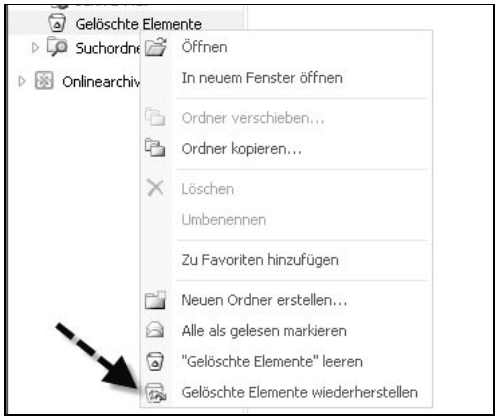


Abbildung 17.33: Wiederherstellen von gelöschten E-Mails über das Kontextmenü

Über diesen Weg lassen sich Anwender auch E-Mails wiederherstellen, die aus dem Papierkorb entfernt wurden.

17.12.2 Single Item-Recovery für Exchange-Administratoren

Neben der Möglichkeit, einzelne Daten über Outlook wiederherzustellen, können auch der Help Desk oder Administratoren Daten wiederherstellen. Damit das funktioniert, müssen Sie Administratoren das Recht zuweisen, Postfächer durchsuchen zu dürfen (siehe Kapitel 16). Dazu ist die Mitgliedschaft in der Verwaltungsrollengruppe *Discovery Management* notwendig. Einzelne Mitglieder fügen Sie mit dem Befehl *Add-RoleGroupMember »Discovery Management« -Member <Benutzer>* hinzu. Standardmäßig enthält diese Verwaltungsrollengruppe keinerlei Mitglieder, auch Exchange-Administratoren dürfen standardmäßig erst Postfächer durchsuchen, wenn das Recht explizit zugewiesen ist. Nach der Zuweisung müssen Sie die Exchange-Verwaltungsshell neu starten, erst dann ist das Recht verfügbar.

Wie Administratoren Postfächer von Empfängern durchsuchen können, hängt von der zugewiesenen CAL des Anwenders ab (siehe Kapitel 1). Ist dem Postfach eine Standard-CAL zugewiesen, können Administratoren nur in der Exchange-Verwaltungsshell nach Elementen suchen, indem diese das CMDlet *Search-Mailbox* verwenden. Verfügt das Postfach des Empfängers, dessen Inhalt der Help Desk nach gelöschten Elementen durchsuchen muss, über eine Enterprise-CAL, ist das Durchsuchen auch über die Exchange-Systemsteuerung in Outlook Web App möglich, ebenso wie mit dem CMDlet *New-MailboxSearch*.

Anwender können eine gelöschte E-Mail über die Wiederherstellungsoption des Papierkorbs in Outlook wiederherstellen, indem sie in Outlook 2010 oder Outlook Web App mit der rechten Maustaste auf den Ordner *Gelöschte Elemente* klicken. Funktioniert das nicht, kann ein Administrator, dem das Recht *Discovery Management* zugewiesen ist, das Postfach durchsuchen und auch solche Objekte wiederherstellen.

Wiederherstellen von E-Mails in der Exchange-Verwaltungsshell

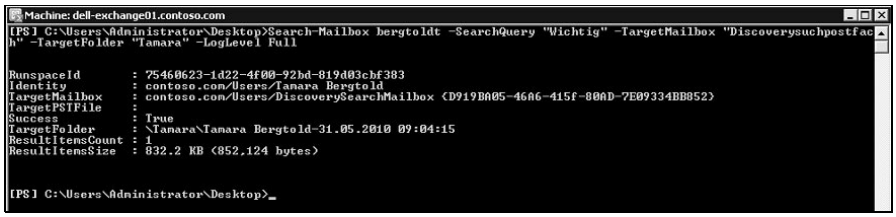
Dazu geben Sie folgenden Befehl in die Exchange-Verwaltungsshell ein:

Search-Mailbox <Name des Anwenders> -SearchQuery »<Betreff oder Text der E-Mail« -TargetMailbox »Discoverysuchpostfach« -TargetFolder »<Ordner im Discoverysuchpostfach« -LogLevel Full

Wollen Sie zum Beispiel beim Anwender mit dem Anmeldenamen *bergtoldt* eine E-Mail wiederherstellen mit dem Betreff *Wichtig*, verwenden Sie den Befehl in der nächsten Abbildung:

Search-Mailbox bergtoldt -SearchQuery »Wichtig« -TargetMailbox »Discoverysuchpostfac« -TargetFolder »Tamara« -LogLevel Full

Abbildung 17.34: Suchen und Finden von gelöschten E-Mails



TIPP

Sie können mit der Option *–SearchDumpsterOnly* des CMDlets *Search-Mailbox* auch nur nach gelöschten Elementen suchen. Die Option ist durch die Installation von Service Pack 1 für Exchange Server 2010 verfügbar.

Gibt die Exchange-Verwaltungsshell ein Ergebnis zurück, können Sie die gefundene E-Mail wiederherstellen. Der nächste Schritt besteht darin, dass Sie das Discovery-Suchpostfach öffnen, am schnellsten geht das über Outlook Web App. Sie können die E-Mail auch direkt in der Exchange-Verwaltungsshell im Postfach des ursprünglichen Anwenders wiederherstellen. Dazu verwenden Sie den Befehl:

Search-Mailbox Discoverysuchpostfach -SearchQuery »<Text aus der E-Mail« -TargetMailbox <Name des Anwenders> -TargetFolder <Beliebiger Ordner im Postfach> -LogLevel Full -DeleteContent

Abbildung 17.35: Öffnen des Discovery-Suchpostfachs in Outlook Web App

Sie können die E-Mail aber auch über Outlook Web App wiederherstellen, wenn Sie das Discovery-Suchpostfach öffnen. Hier ist die gelöschte E-Mail jetzt verfügbar. Sie finden diese in dem Ordner, den Sie bei der Erstellung des Befehls eingegeben haben.

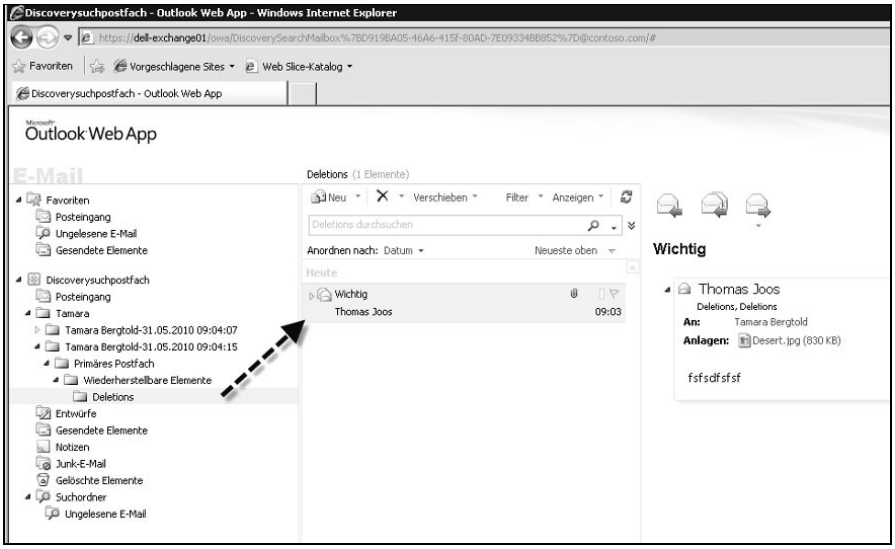


Abbildung 17.36: Anzeigen der wiederhergestellten E-Mail eines Empfängers

Um die E-Mail dem Anwender wieder zur Verfügung zu stellen, können Sie diese aus dem Discovery-Suchpostfach einfach an den Anwender weiterleiten. Das ist der schnellste Weg.

Wiederherstellen von E-Mails über die Exchange-Systemsteuerung

Steht dem Anwender, für den Sie eine E-Mail wiederherstellen wollen, eine Enterprise-CAL von Exchange Server 2010 zur Verfügung (siehe Kapitel 1), können Sie für die Wiederherstellung von E-Mails auch auf die Exchange-Systemsteuerung setzen, die Sie über Outlook Web App starten können. Geben Sie dazu im Browser die Adresse https://<servername>/ecp ein.

Abbildung 17.37: Starten der Exchange-Systemsteuerung über Outlook Web App

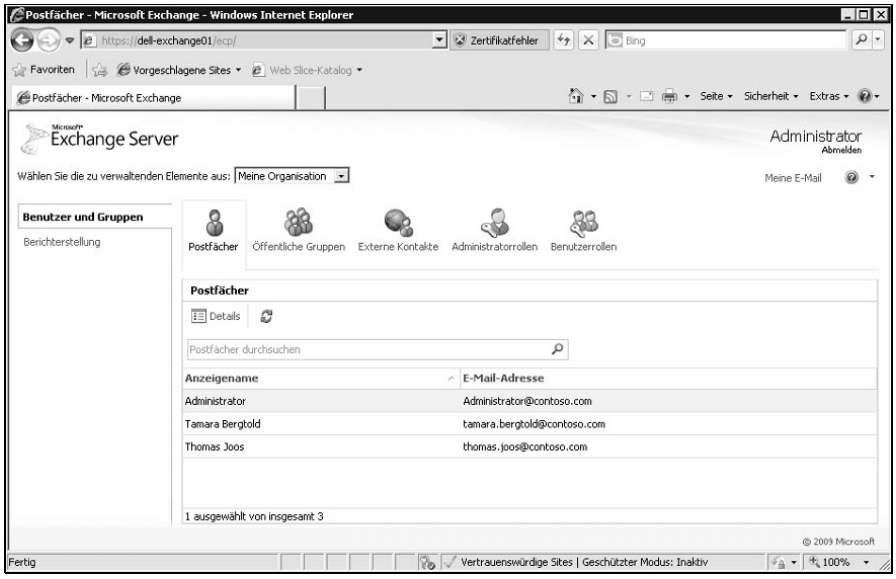
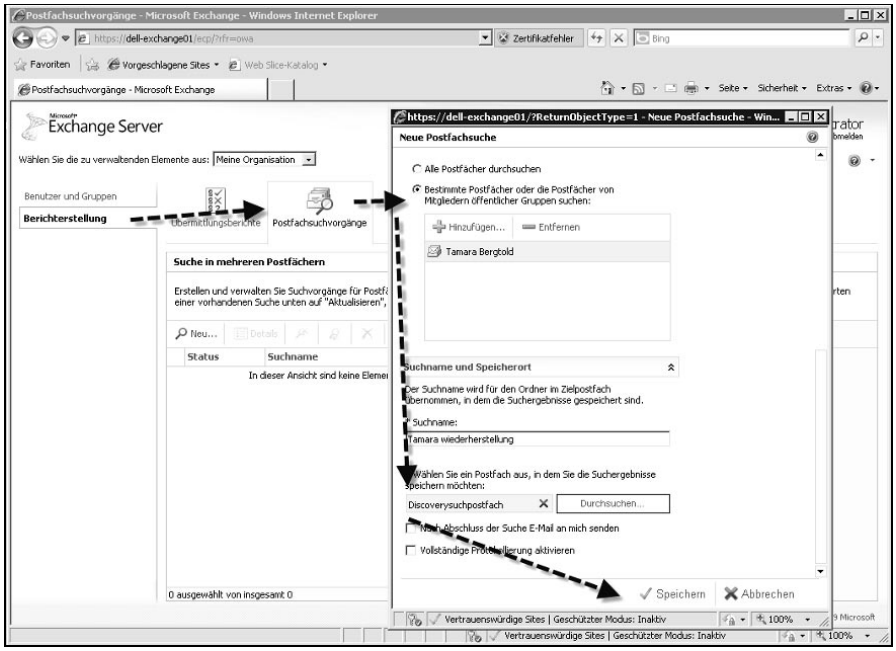


Abbildung 17.38: Wiederherstellen von E-Mails über die Exchange-Systemsteuerung



1. Nach dem Start wählen Sie bei *Wählen Sie die zu verwaltenden Elemente* die Option *Meine Organisation* aus.
2. Rufen Sie die Option *Berichterstellung* und dann *Postfachsuchvorgänge* auf.
3. Erstellen Sie mit *Neu* einen neuen Suchvorgang.

4. Geben Sie den oder die Suchbegriffe ein, nach denen Sie suchen wollen.
5. Wählen Sie im Fenster das Postfach aus, das durchsucht werden soll.
6. Geben Sie als Wiederherstellungsort das Postfach *Discoverysuchpostfach* an.
7. Speichern Sie die Suche.

Exportieren und Importieren in PST-Dateien mit Exchange Server 2010 SP1

Haben Sie das SP1 für Exchange Server 2010 installiert, können Sie gefundene E-Mails auch in PST-Dateien exportieren. Achten Sie aber darauf, dass der Administrator dazu zunächst der entsprechenden Verwaltungsrollengruppe zugewiesen sein muss (siehe Kapitel 16). Verwenden Sie dazu die beiden Befehle:

1. *New-RoleGroup »Mailbox Import-Export Management« -Roles »Mailbox Import Export«*
2. *Add-RoleGroupMember »Mailbox Import-Export Management« -Member <Benutzer>*

Der erste Befehl erstellt eine neue Verwaltungsrollengruppe mit dem Recht, Daten aus Postfächern zu exportieren und zu importieren. Über den zweiten Befehl weisen Sie der Verwaltungsrollengruppe Benutzer hinzu, die ein solches Recht erhalten sollen. Mehr zu diesem Thema erfahren Sie in Kapitel 16. Benutzer, denen dieses Recht zugewiesen ist, können gelöschte E-Mails suchen und in PST-Dateien exportieren. Diese Dateien können auch auf Netzwerkfreigaben gespeichert sein. Dabei hilft folgender Befehl:

New-MailboxExportRequest -Mailbox »Discoverysuchpostfach« -FilePath »\\<Netzwerkpfad zur PST-Datei>« -ContentFilter {Subject -eq »<Inhalt der E-Mail>«} -SourceRootFolder »<Ordner im Discoverysuchpostfach, in dem die E-Mail wiederhergestellt wird>«

Auf dem gleichen Weg lassen sich PST-Dateien auch über die Exchange-Verwaltungsshell wieder in Benutzerpostfächer importieren:

New-MailboxImportRequest -Mailbox <Benutzerpostfach> -FilePath »\\<Pfad zur PST-Datei« -TargetRootFolder »<Ordner im Postfach des Anwenders, in dem die PST-Datei wiederhergestellt werden soll>«

17.13 System Center Data Protection Manager 2010

Mit System Center Data Protection Manager 2010 bietet Microsoft die neue Version seiner Lösung zur Datensicherung im Unternehmen. Durch Sicherung auf Bandlaufwerke und Festplatten, zusammen mit Online-Snapshots und der Unterstützung von Sicherungsfunktionen der Microsoft-Produkte, lassen sich vor allem Daten in Microsoft-Netzwerken schnell und stabil sichern und wiederherstellen. Neben herkömmlichen Dateien unterstützt das Produkt auch die Online-Datensi-

cherung von Exchange-Datenbanken, SharePoint oder SQL Server. DPM ist daher eine ernst zu nehmende Alternative zu gängigen Datensicherungsprodukten von Drittherstellern.

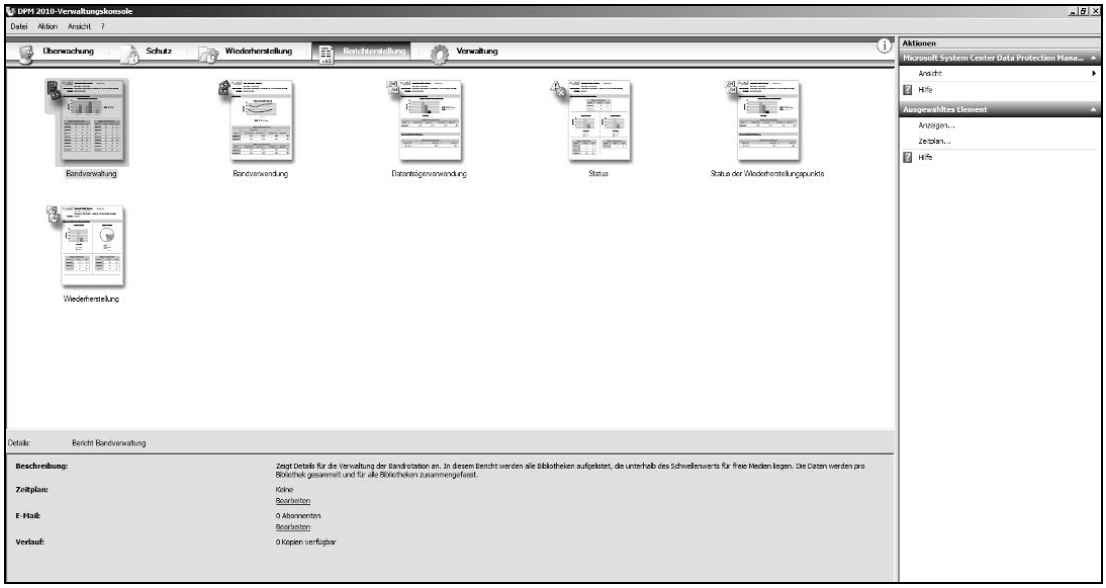


Abbildung 17.39: DPM-Verwaltungskonsole nach der Installation

Data Protection Manager (DPM) 2010 ist vor allem für die Datensicherung auf Festplatten, Backup-To-Disk optimiert. Die Lösung kann aber auch problemlos Daten auf Bandlaufwerke sichern. Bei der Backup-To-Disk-Variante repliziert die Lösung Dateien auf den von DPM verwalteten Festplattenspeicher. Bei der Erstellung von Sicherungsjobs können Administratoren auswählen, ob eine zusätzliche Sicherung auf Band erfolgen soll. Sind die Daten einmal übertragen, muss DPM bei weiteren Sicherungen nur die geänderten Datenblöcke sichern. Das heißt, auch bei großen Datenmengen erhöht sich die Sicherungszeit zwar, der Server vermeidet jedoch unnötigen Datenverkehr. Der große Unterschied zu vielen anderen Lösungen in diesem Bereich ist, dass DPM nicht die kompletten geänderten Dateien, zum Beispiel Exchange-Datenbanken, erneut überträgt, sondern nur die geänderten Datenblöcke innerhalb dieser Dateien. Bereits übertragene Datenblöcke überspringt DPM dazu. Um die geänderten Blöcke zu erkennen, verwendet DPM nicht mehr das NTFS-Journal, sondern direkt die Bitmap. So kann der Server sehr schnell und zuverlässig erkennen, welche Blöcke auf der Festplatte geändert sind, und diese sichern. Diese Technik beherrscht DPM auch bei der Sicherung auf Bandlaufwerke. DPM unterstützt auch die Sicherung über Schattenkopien von Windows Server 2003/2008 und Windows Server 2008 (R2). Windows 2000 Server gehört nicht zu den unterstützten Betriebssystemen, da hier die Voraussetzungen fehlen.

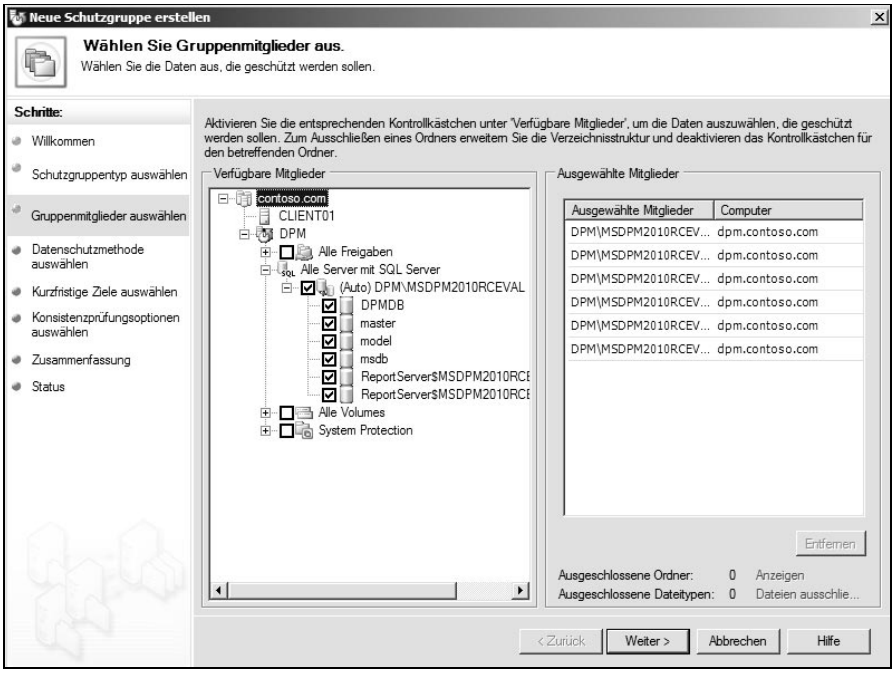


Abbildung 17.40: Neben Freigaben und Laufwerken lassen sich auch SQL-Server online sichern.

Die Systemdienste können dabei weiterlaufen, da die Sicherung die Online-Backup-Funktion der Produkte unterstützt. Neben Exchange und SQL unterstützt DPM auch die Sicherung von Windows-Clustern. Der Vorteil ist, dass die komplette Konfiguration der Sicherung von einer einzelnen Oberfläche aus verfügbar ist. Bei Exchange besteht beispielsweise die Möglichkeit, den kompletten Festplattenspeicher wiederherzustellen oder einzelne Postfächer. Wollen Unternehmen einzelne E-Mails zurücksichern, führt der Weg zunächst über das Zurücksichern des Postfachs und dann zu den einzelnen Objekten im Posteingang. Die Auswahl der zu sichernden Daten, erfolgt über eine grafische Oberfläche. Einer der Vorteile des DPM ist die schnelle und intuitive Einrichtung über die grafische Oberfläche. Auch die Installation ist schnell abgeschlossen. Wollen Sie DPM auf Basis einer Backup-To-Disk-Lösung einrichten, müssen Sie darauf achten, dass das Produkt einen eigenen Festplattenspeicher benötigt, der exklusiv für die Sicherung zur Verfügung steht. Achten Sie darauf, dass der Festplattenspeicher über genug Kapazität verfügt, ideal ist ein Mehrfaches der zu sichernden Daten, damit genug Freiraum bleibt, zusätzliche Sicherungen vorzunehmen, und der Platz auch für zukünftige Anforderungen ausreichend dimensioniert ist.

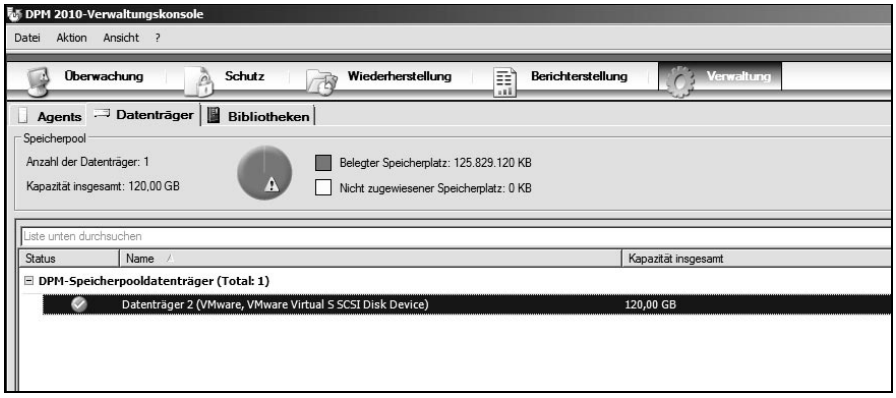


Abbildung 17.41: Zuweisen von Festplattensystemen zur Sicherung mit DPM

Damit DPM eine Sicherung durchführen kann, sollte auf allen geschützten Servern ein Agent vorhanden sein, der mit dem DPM-Server eine Verbindung aufbaut. Die Clients lassen sich übrigens effizient und einfach über die Verwaltungskonsole von DPM im Netzwerk verteilen. Neben der manuellen Installation über die Konsole besteht auch die Möglichkeit, den DPM-Client per Softwareverteilung, zum Beispiel mit dem System Center Configuration Manager (SCCM) 2007 (R2), oder per Gruppenrichtlinie auf den Zielsystemen zu integrieren.

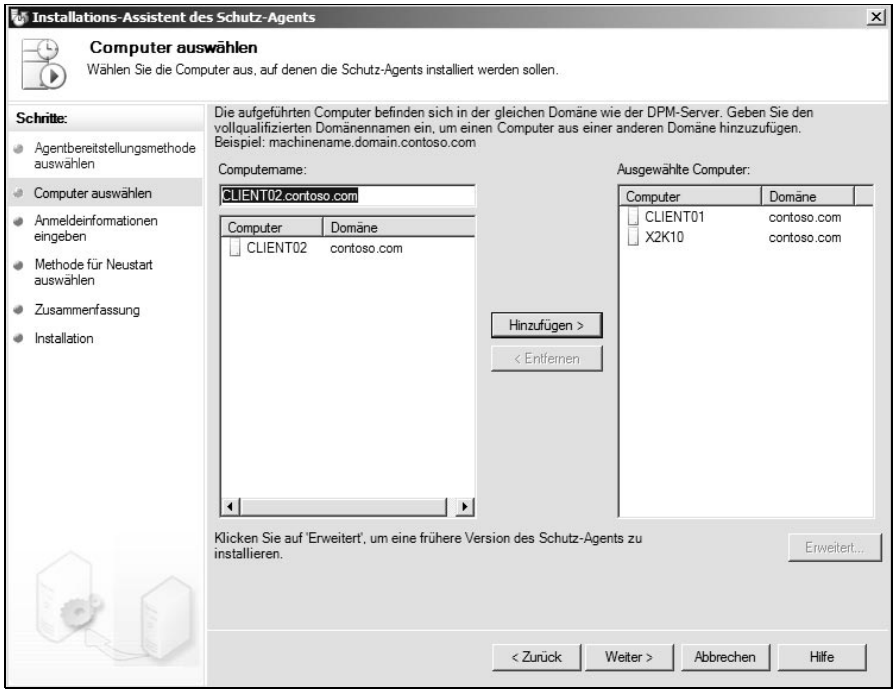


Abbildung 17.42: Der zur Sicherung notwendige Agent von DPM lässt sich über einen Assistenten leicht installieren.

Neben den herkömmlichen Verlaufsdaten kann DPM auch den Systemstatus der Server sichern. Gemeinsame Systemdaten mehrerer Server fasst DPM zusammen und sichert nur beim ersten Server das komplette Betriebssystem. Das hat den Vorteil, dass sich neben den Daten auch Server wiederherstellen lassen, aber nur so wenig Daten wie möglich auf der Sicherung vorhanden sind. Doppelte Datenmengen in der Datensicherung gehören daher der Vergangenheit an.

Immer mehr Unternehmen betreiben Niederlassungen, in denen natürlich auch Daten zu sichern sind. Ideal ist es, diese Daten über bestehende Leitungen zentral zu sichern. Auch diese Einsatzmöglichkeiten unterstützt DPM. Damit DPM über WAN-Leitungen Daten sichern kann, muss die Bandbreite mindestens 512 Kbit/s betragen. Außerdem sollte es sich bei der Verbindung möglichst nicht um eine Wählleitung, sondern um eine permanente Standleitung handeln. Natürlich lässt sich in DPM die zur Sicherung verwendete Bandbreite begrenzen. Auch den Zeitpunkt der Sicherung über die WAN-Leitung können Sie über einen Scheduler einrichten. DPM unterstützt darüber hinaus spezielle Regeln für die Datensicherung, mit denen sich Server zu einzelnen Gruppen zusammenfassen lassen. Diese *Schutzgruppen* haben einen gemeinsamen Regelsatz. In diesen Regeln legen Sie beispielsweise fest, wie oft der Server die Daten sichern soll oder wie lange die Daten rückwirkend auf dem Server verfügbar sein sollen. Nicht erwünschte Dateien lassen sich außerdem von der Sicherung ausschließen. Dadurch verhindern Sie, dass wertvoller Speicherplatz zum Beispiel durch unnötige Multimediadateien belegt wird.

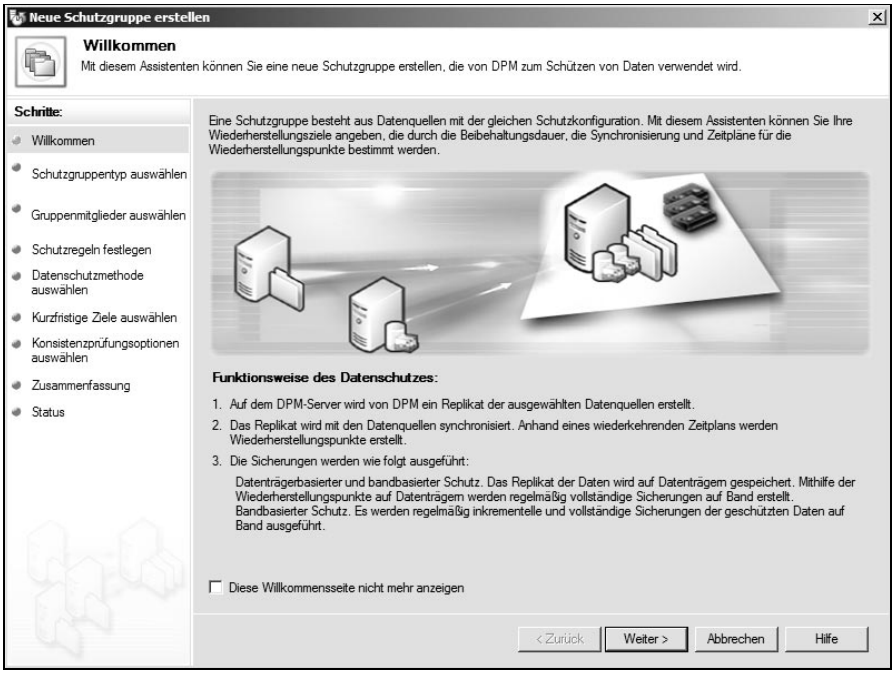


Abbildung 17.43: Die Sicherung erfolgt durch Definition von Schutzgruppen.

Mit der grafischen Oberfläche lassen sich einzelne Dateien, Verzeichnisse oder der komplette Systemstatus des Servers wiederherstellen. DPM ermöglicht, wie die meisten Produkte, die Herstellung am Ursprungsort oder in einem alternativen Verzeichnis. Eine Besonderheit von DPM ist die Möglichkeit, dass Anwender selbst eigene Daten wiederherstellen können. Dazu verbindet sich DPM mit dem Schattenkopie-Client. Über diesen Client können Anwender dann schnell und einfach einzelne Daten wiederherstellen. Der Vorteil dabei ist neben der Entlastung der IT-Abteilung, dass die Ausfallzeiten bei Anwendern sehr gering ausfallen, wenn diese eine Datei wiederherstellen müssen. Der Vorgang der Wiederherstellung erfordert keine Schulung, sondern ist effizient und leicht in Windows möglich. In Windows Vista und Windows 7 gehört der dazugehörige Schattenkopie-Client übrigens bereits zu den Bordmitteln. Unternehmen, die Windows XP einsetzen, können diese Funktion zwar auch nutzen, müssen den Client aber nachträglich installieren. Wollen Sie über den Data Protection Manager einen kompletten Server wiederherstellen, bietet DPM ein spezielles Tool an, über das Sie eine bootfähige CD/DVD erstellen. Auch das Booten über Netzwerk ist mit DPM möglich. Anschließend baut der Client eine Verbindung zum DPM-Server auf und sichert die hinterlegten Daten zurück.

Neben der grafischen Oberfläche bietet DPM auch eine Verwaltung auf Basis der Windows PowerShell an. Während der Installation integriert DPM dazu weitere CMDlets, speziell für die Verwaltung der Sicherungsfunktionen. Neben der lokalen Verwaltung lassen sich mit den Befehlen in der PowerShell DPM-Server auch von Arbeitsstationen oder anderen Servern im Netzwerk verwalten. Wollen Sie eine ausfallsichere Datensicherungslösung aufbauen, unterstützt Data Protection Manager auch die Verbindung von zwei DMP-Servern zu einer Disaster-Recovery-Lösung. Beim Ausfall eines einzelnen Servers übernimmt der zweite dessen Aufgaben vollkommen automatisiert.

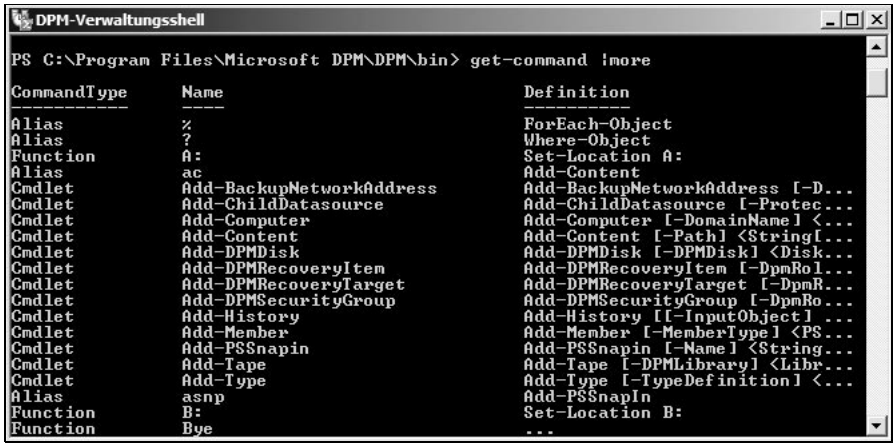


Abbildung 17.44: Wie alle neuen Serverprodukte von Microsoft, unterstützt DPM auch die PowerShell.

In der neuen Version, hat Microsoft auch die Möglichkeiten des Vorgängers DPM 2007 deutlich überarbeitet. DPM 2010 kann zum Beispiel fehlgeschlagene Sicherungsjobs automatisch wiederholen (Self Healing), was die Zuverlässigkeit von Einmalsicherungen erhöht. Das kann zum Beispiel sinnvoll sein, wenn Administratoren vor geplanten Aktualisierungen nachts eine Sicherung aktivieren und diese beim ersten Mal nicht startet. Vor allem für Sicherungsaufträge, die nicht regelmäßig stattfinden, sondern nur einmal starten sollen, kann diese Wiederholung helfen, Sicherungen effizient durchzuführen, auch wenn beim ersten Versuch Fehler auftreten. Administratoren können festlegen, ob sie diese Funktion nutzen wollen und wann, sowie bestimmen, wie oft DPM die Sicherung erneut durchführen soll, wenn Fehler auftreten. Auf DPM-Server replizierte Daten lassen sich in der neuen Version auf Konsistenz überprüfen, indem die Lösung die Daten mit den originalen Daten auf dem gesicherten Server vergleicht. So ist sichergestellt, dass die auf Festplatten gesicherten Daten immer korrekt sind. DPM 2010 ist in der Lage, die Sicherungs-Volumes automatisch zu verwalten und zu vergrößern, wenn der Plattenplatz für die Sicherung nicht mehr ausreicht. Administratoren können dazu bei der Einrichtung festlegen, welche Volumes DPM verwalten soll und auf welchen Datenträgern die Serverlösung Rechte hat, Volumes zu vergrößern. DPM 2010 fertigt von den unterstützten Produkten zur Sicherung im laufenden Betrieb Snapshots an, sichert die Daten dieser Online-Snapshots auf ein Festplattensystem und legt diese Daten dann wiederum auf Band ab. Das bedeutet, dass die gesicherten Serverlösungen weiterhin den Anwendern zur Verfügung stehen. Auch die direkte Sicherung auf Bandlaufwerke ist möglich, ohne den Umweg über Festplatten oder parallel dazu. Die jeweilige Variante lässt sich bequem im Sicherungsjob festlegen. Ist auf dem Server kein Bandlaufwerk verfügbar, deaktiviert der Assistent die Sicherung auf Band.

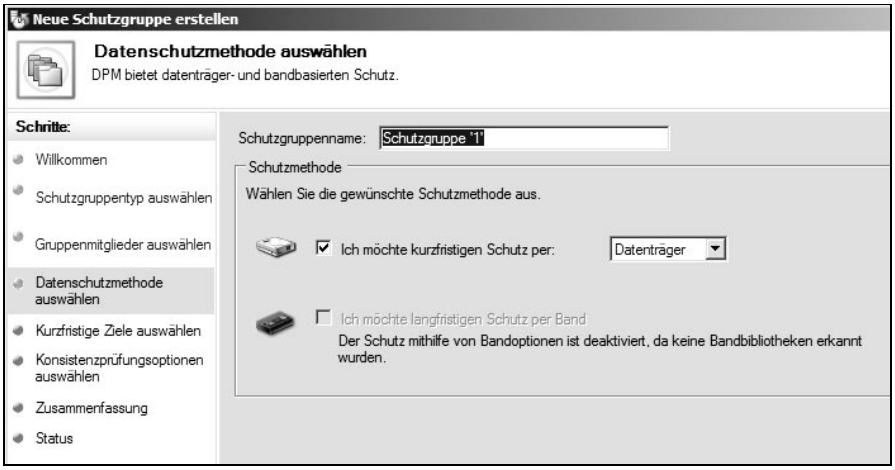
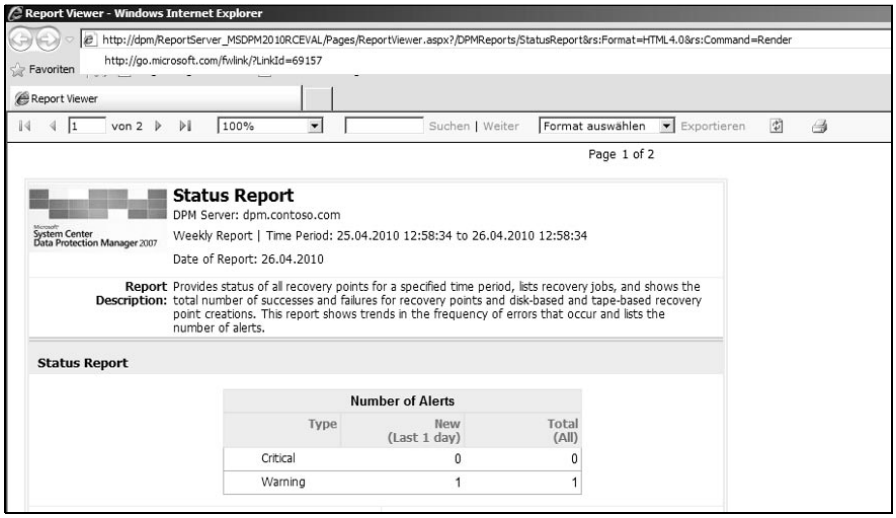


Abbildung 17.45: Auswählen der Sicherung für die jeweilige Schutzgruppe

Durch die Integration der wichtigsten Microsoft-Server-Produkte in DPM lässt sich die Sicherung teilweise effizienter und flexibler gestalten als mit anderen Lösungen, da DPM-Server genau wissen, welche Daten und Verzeichnisse der gesicherten Server-Lösungen wichtig sind. Besonders optimal arbeitet DPM 2010 mit Exchange, SharePoint, SQL Server (auch mit SAP), Microsoft Dynamics und Hyper-V zusammen. In der neuen Version müssen Sie zur Wiederherstellung von SharePoint-Daten zum Beispiel keine eigene Wiederherstellungsfarm erstellen. Müssen Sie Daten wiederherstellen, die schon älter sind, holt DPM diese Daten automatisch von der Bandsicherung zurück. Neben der Sicherung und Wiederherstellung von Daten lassen sich mit DPM 2010 auch Disaster-Recovery-Vorgänge durchführen, zum Beispiel die vollständige Wiederherstellung einer SharePoint-Farm. DPM 2010 sichert auf Wunsch alle 15 Minuten die Daten von Exchange-Servern ab Version Exchange Server 2003 SP2 im laufenden Betrieb. Genauso leicht wie die Sicherung, ist die Wiederherstellung dieser Daten.

Abbildung 17.46: Berichte erstellt DPM auf Basis der SQL-Server-Reporting-Services.



Die neue Hochverfügbarkeitslösung in Exchange Server 2010 mit der Bezeichnung Database Availability Groups (DAG), dem Nachfolger von SCR, SCC und CCR von Exchange Server 2007, gehört auch zu den unterstützten Technologien in DPM 2010. SQL-Datenbanken sichern Sie ab SQL Server 2000 SP4 und auch Daten unter SQL Server 2008 (R2). Auch SAP-Datenbanken lassen sich auf diese Weise sichern. Da DPM immer die ganze SQL-Instanz sichern kann, erkennt DPM neue Datenbanken und integriert diese automatisch in die Datensicherung. SharePoint-Farmen unterstützt DPM ab SharePoint Portal Server 2003 genauso wie auf dem neuen SharePoint Server 2010 und den SharePoint Services 2.0, 3,0, aber auch SharePoint Foundation 2010, dem Nachfolger der SharePoint Services 3.0. Legen Administratoren neue Inhaltsdatenbanken in einer Share-

Point-Farm an, erkennt das DPM 2010 und sichert diese neuen Datenbanken automatisch mit. DPM 2010 ist darüber hinaus wesentlich leistungsfähiger als DPM 2007. Mit einem einzelnen DPM-Server lassen sich bis zu 100 Server, 1000 Notebooks und 2000 Datenbanken sichern. Virtuelle Computer unter Hyper-V und Hyper-V R2 unter Windows Server 2008 (R2) sind kein Problem für DPM. DPM 2010 kann zum Beispiel die neuen Cluster Shared Volumes (CSV) sichern, die Hyper-V R2 für die Live Migration von virtuellen Computern zwischen Clusterknoten benötigt. Bei der Live Migration von Windows Server 2008 (R2) verlieren Anwender nicht die Verbindung zu den virtuellen Computern. Quick Migration unter Windows Server 2008 hat die Benutzer beim Verschieben eines virtuellen Computers auf einen anderen Clusterknoten noch von den Servern getrennt. DPM 2010 kann auch Daten von virtuellen Computern sichern, die zur Live Migration vorgesehen sind. Ebenfalls möglich ist die Wiederherstellung einzelner Daten innerhalb von virtuellen Festplatten (VHD). Virtuelle Computer lassen sich nicht nur auf der ursprünglichen Host-Maschine wiederherstellen, sondern auf jedem anderen Hyper-V-Host in der Infrastruktur. Daten von Arbeitsstationen mit Windows Vista, XP und Windows 7 lassen sich ebenfalls sichern. Die Sicherung von Arbeitsstationen ist zum Beispiel für Notebooks interessant. Hier arbeitet DPM optimal mit dem Schattenkopiedienst zusammen. Auch Daten aus dem Active Directory oder Freigaben auf Servern mit Windows Server 2003/2008 und Windows Server 2008 (R2) lassen sich sichern. Gesicherte Daten von Freigaben können sogar Anwender selbst über den Windows-Explorer wiederherstellen, wenn Administratoren diese Möglichkeit im Unternehmen bieten wollen. Auch Windows Essential Business Server 2008 und Small Business Server 2008 unterstützt DPM 2010. Eine Neuerung in DPM 2010 ist auch die Möglichkeit, Daten von Microsoft Dynamics ab Version AX 2009 auf die gleiche Art zu sichern. Auch hier können Sie Online-Snapshots im 15-minütigen Abstand erstellen. DPM ist optimal für den Einsatz in Umgebungen mit Active Directory-Domänen. DPM 2010 lässt sich aber auch als Workgroup-Server außerhalb von Domänenumgebungen betreiben oder wenn Server in einer Domäne gesichert werden sollen, für die keine Vertrauensstellung existiert. Die Kommunikation mit anderen DPM-Servern erfolgt in diesem Fall über DCOM (Port 135) und WinSock (Ports 5718 und 5719). Als Authentifizierung zum Workgroup-Server dient ein lokales Benutzerkonto. System Center Data Protection Manager integriert sich in die anderen Produkte der System-Center-Reihe und ist auch Bestandteil der Server Management Suite zusammen mit System Center Operations Manager 2007 R2, System Center Configuration Manager 2007 R2 und System Center Virtual Machine Manager 2008 R2. Die System-Center-Produkte arbeiten perfekt zusammen. So kann zum Beispiel System Center Operations Manager einen Disaster-Recovery-Vorgang starten, wenn ein Management Pack einen Ausfall bemerkt.

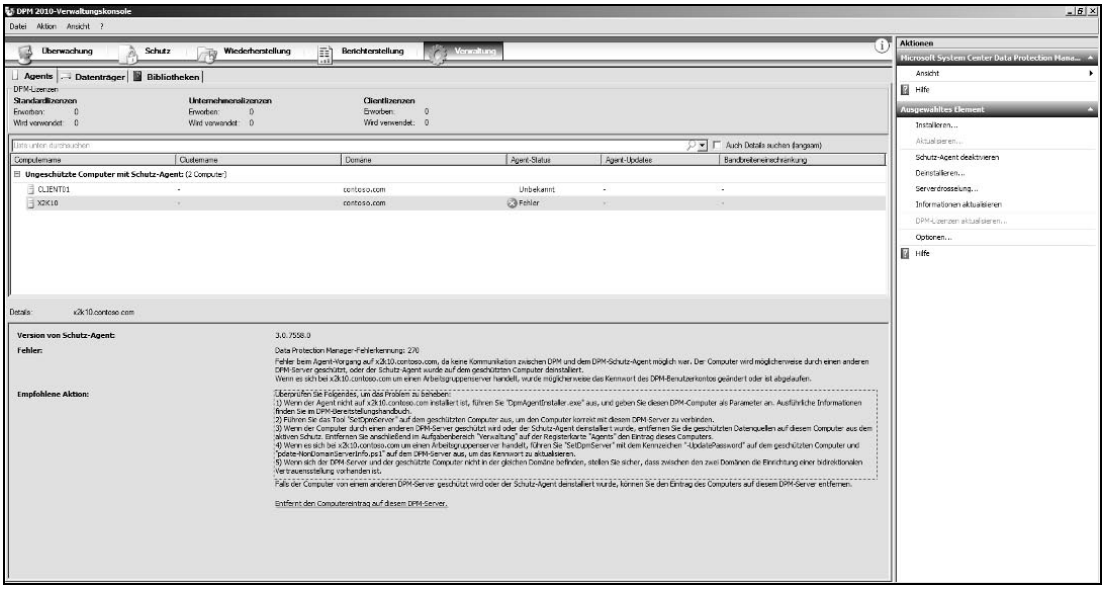


Abbildung 17.47: Bei Problemen weist DPM auch auf mögliche Problemlösungen hin.

Um DPM 2010 zu lizenzieren, benötigen Unternehmen zunächst eine Serverlizenz für System Center Data Protection Manager 2010. Für jeden gesicherten Server ist eine Enterprise-Lizenz für DPM erforderlich, wenn es sich um spezielle Sicherungstechnologien oder Daten handelt, die für ein Disaster-Recovery notwendig sind, also zum Beispiel für Exchange, SQL, SharePoint oder Hyper-V. Wollen Sie Arbeitsstationen sichern, benötigen diese eine Client-Lizenz für DPM, Sicherungen von Domänencontrollern und Freigaben erfordern eine Standardlizenz für jeden Server. Neben der Testversion stellt Microsoft Webcasts und Whitepapers zu DPM 2010 zur Verfügung. DPM 2010 kann, neben der herkömmlichen Sicherung auf Festplatten und Bandlaufwerken, auch Disaster-Wiederherstellungsvorgänge durchführen, die Administratoren mit einem Klick starten können. Dazu verwendet die Lösung einen dedizierten Wiederherstellungsserver, auf dem DPM die notwendigen Daten wiederherstellt. Über System Center Operations Manager 2007 R2 lassen sich diese Vorgänger über ein spezielles Management Pack sogar automatisieren. Disaster-Recovery funktioniert in DPM 2010 auch über WAN-Leitungen. Auf diese Weise lassen sich auch Exchange, SQL und SharePoint wiederherstellen.

Links

Technet DPM-Blog
– http://blogs.technet.com/dpm

Infoseite Server Management-Suite
– http://www.microsoft.com/systemcenter/en/us/management-suites.aspx

Website zu DPM 2007 und 2010
– http://www.microsoft.com/systemcenter/dataprotectionmanager/en/us/default.aspx

TechNet zu DPM
– http://technet.microsoft.com/en-us/systemcenter/dm/default.aspx

Kundenreferenzen zu DPM
– Http://www.microsoft.com/germany/kundenreferenzen/?qu=&industry=&product=42