Kapitel 4

Remotedesktop, Exchange, SharePoint & Co.

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen Tools, die Sie bei der Verwaltung von Remotedesktopservern unterstützen. Auch Tools für die Verwaltung von Exchange und SharePoint finden Sie in diesem Kapitel. Ein weiterer Abschnitt zeigt Tools für das Forefront Threat Management Gateway 2010 und für Small Business Server (SBS) 2011.

Tools für Remotedesktopserver

Für die bessere Verwaltung von Remotedesktopservern bringt Windows Server 2008 R2 bereits einige Bordmitteln mit, welche einzelne Aufgaben deutlich erleichtern. Im folgenden Abschnitt gehen wir auf die wichtigsten Befehlszeilentools für die Verwaltung von Remotedesktopservern ein sowie auf Zusatztools, welche die Arbeit enorm erleichtern.

Remotedesktopverbindungen effizient verwalten – Royal TS

Viele Administratoren kennen das Problem: Im Unternehmen müssen zahlreiche Server verwaltet werden und zwar meist auch noch gleichzeitig. Die Verwaltung einzelner Server findet häufig über Remotedesktop statt. Die Verwaltung der einzelnen Remotedesktop (RDP)-Verbindungen gestaltet sich leider mit Bordmitteln relativ kompliziert. Vor allem, wenn Sie mehrere Verbindungen parallel öffnen, wird die Arbeit schnell unübersichtlich.

Royal TS kann zahlreiche RDP-Verbindungen zentral verwalten. Für bis zu zehn Computer können Sie das Tool kostenlos nutzen. Zunächst laden Sie das Tool von der Internetseite *www.code4ward.net* herunter. Auf der Seite gibt es auch ein Forum, in welchem Fehler und neue Funktionen des Tools besprochen werden und der Programmierer direkt antwortet.

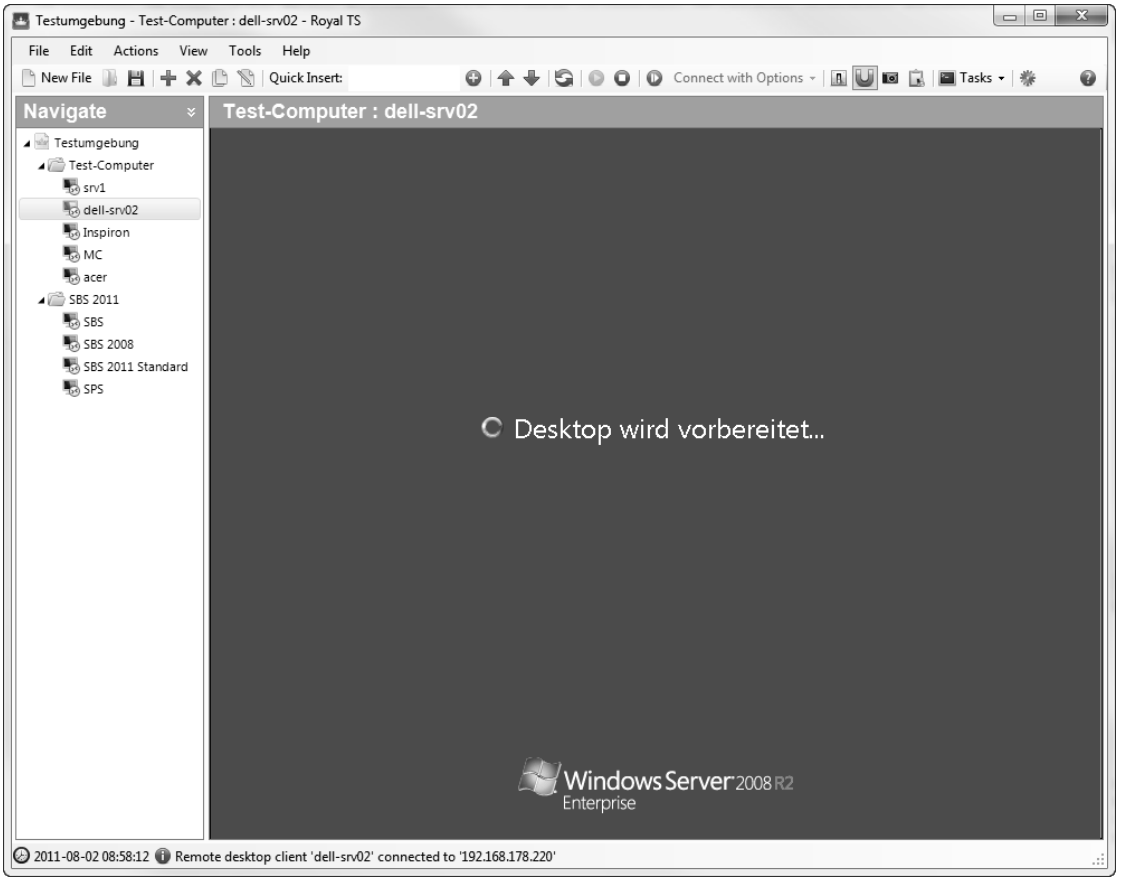

Abbildung 4.1 Verwalten von Remotedesktops mit Royal TS

Die Größe des Tools beträgt etwa 900 KB. Der größte Nutzen ist die gemeinsame Verwaltung von mehreren Remotedesktops, die auch parallel geöffnet sein können. Administratoren können durch einen Mausklick zwischen den verschiedenen geöffneten RDP-Sitzungen wechseln. Den geöffneten Remotedesktop zeigt das Tool in der Mitte der Konsole als Vollbild an. Wem das nicht gefällt, kann einzelne Verbindungen so konfigurieren, dass sich diese in einem eigenen Fenster öffnen.

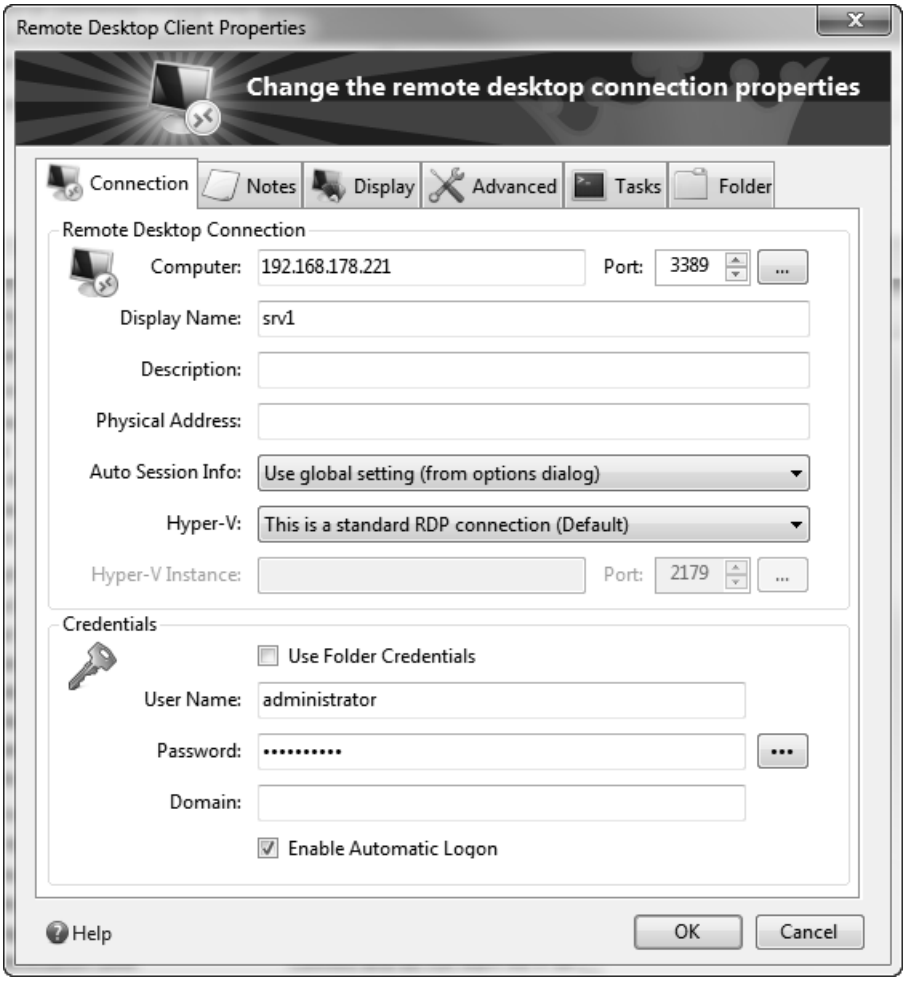

Abbildung 4.2 Konfigurieren der Einstellungen für einzelne Verbindungen

Alle gespeicherten Verbindungen zu anderen Servern sehen Sie auf der linken Seiten der Oberfläche. Die einzelnen Remotedesktopverbindungen lassen sich über einen Assistenten erstellen. Neben den Verbindungsoptionen wie Auflösung, verbundene Laufwerke, IP-Adresse oder Name des Servers lässt sich auch eine Authentifizierung hinterlegen. Sie öffnen eine RDP-Verbindung per Doppelklick. Die einzelnen Verbindungen lassen sich auch gruppieren.

Weiterhin können Sie mehrere Gruppen in einer *.rts*-Datei zusammenfassen. Royal TS lässt sich so konfigurieren, dass das Tool beim Start eine bestimmte Datei mit den enthaltenen Gruppen automatisch öffnet. Die einzelnen Verbindungen lassen sich natürlich jederzeit umgruppieren. Die Authentifizierungsdaten verschlüsselt das Tool in der Verbindungsdatei.

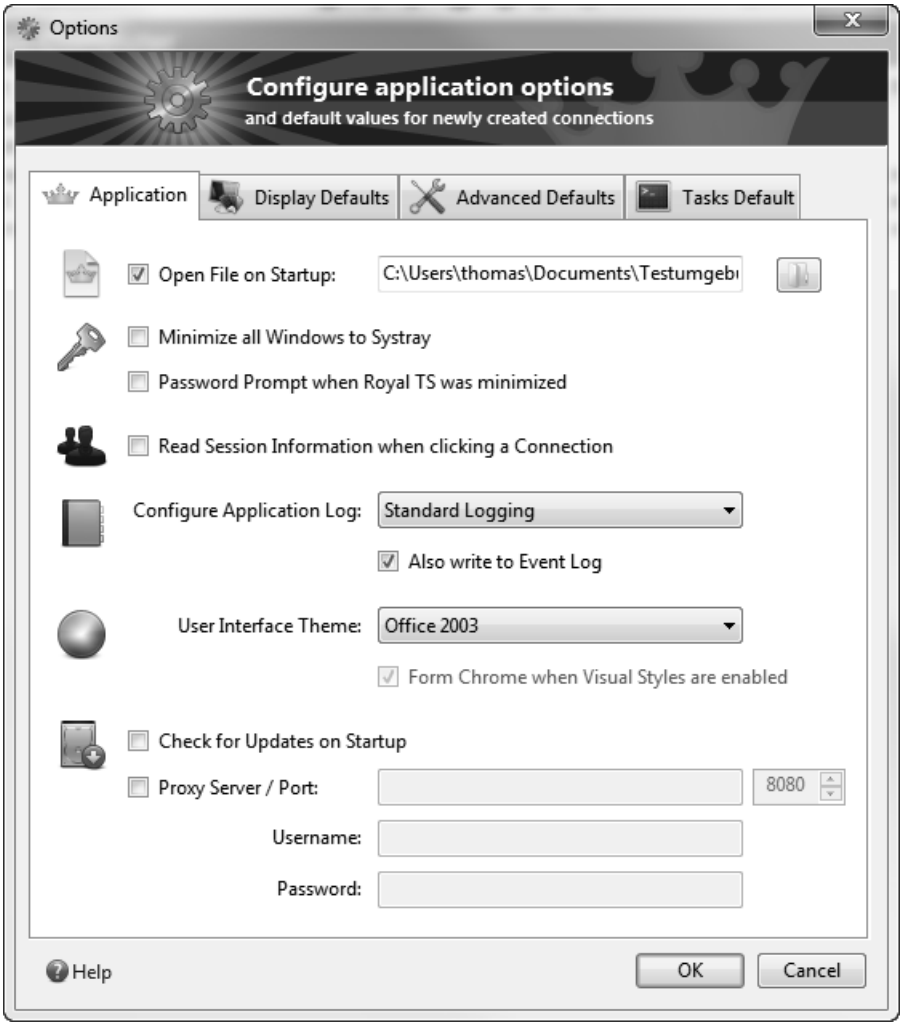

Abbildung 4.3 Konfigurieren der Einstellungen von Royal TS

Wer die Authentifizierungsoptionen speichert, muss diese für alle Verbindungen einzeln hinterlegen. Ändern Sie das Kennwort des hinterlegten Benutzerkontos, müssen Sie auch die einzelnen Verbindungen nachträglich anpassen. Bei aufgebauten Verbindungen können Sie die Größe des Fensters auch dynamisch vergrößern oder verkleinern, der Remotedesktop passt sich daraufhin automatisch an. Wer das nicht will, kann für die einzelnen Verbindungen auch eine Auflösung für den Remotedesktop vorgeben. Für jede Verbindung können Sie die Einstellungen über das Kontextmenü nachträglich anpassen. Auch der RDP-Port, standardmäßig auf TCP 3389 konfiguriert, lässt sich ändern.

Für alle Verbindungen stehen über den Menübefehl *Tools/Options* Möglichkeiten zur Verfügung, die Standardauflösung und Verbindungsoptionen zentral zu bearbeiten. Das Tool unterstützt neben Windows XP auch Windows Vista und Windows 7.

Über die Datei *RTSApp.exe.config* im Installationsordner von Royal TS können Sie zusätzlich einige Einstellungen anpassen, die nicht in der grafischen Benutzeroberfläche zur Verfügung stehen. So können Sie in dieser Datei zum Beispiel über die Einstellung *ConfigurationPath* den Pfad zu den Benutzereinstellungen anpassen, was Unternehmen entgegenkommt, die mit servergespeicherten Profilen arbeiten. Standardmäßig liegen die Benutzereinstellungen des Tools im Profil des Anwenders. Treten nach Windows-Updates Fehler mit dem Tool auf, besonders unter Windows Vista und Windows 7, hilft oft das Löschen dieser Benutzerdateien, die anschließend automatisch neu erstellt werden. Verbindungsdaten gehen dabei nicht verloren, da diese in der *.rts*-Datei gespeichert sind, die Sie mit dem Tool öffnen.

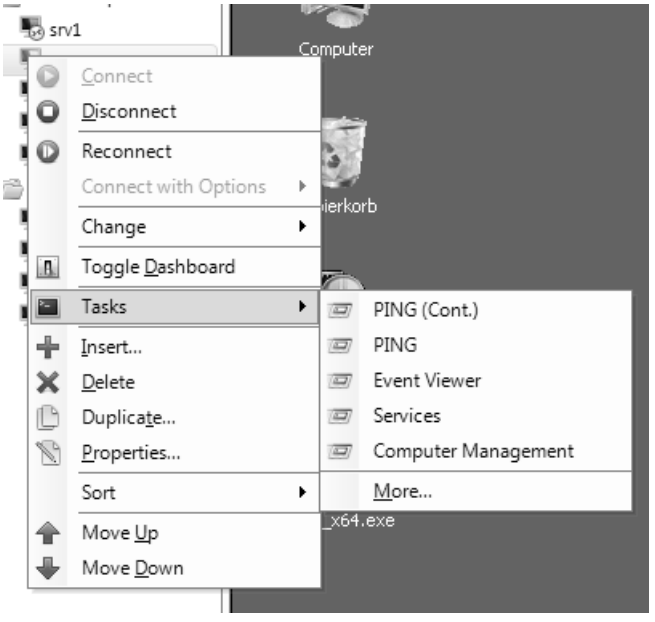

Abbildung 4.4 Kontextmenü von Verbindungen in Royal TS

Remote Desktop Load Simulation Tools

Mit diesen Tools können Sie die Auslastung Ihrer Server planen und simulieren. Vor allem beim Aufbau einer Serverfarm sind die Tools sinnvoll, da Sie festlegen können, mit welcher Gewichtung in der Farm die einzelnen Server konfiguriert sein sollen. Sie können die Installationsdatei und die zwei sehr ausführlichen Anleitungen auf der Seite *http://www.microsoft.com/downloads/details.aspx?FamilyID=C3F5F040-AB7B-4EC6-9ED3-1698105510AD* herunterladen, oder indem Sie nach Remote Desktop Load Simulation Tools in einer Suchmaschine suchen.

Anmeldungen aktivieren oder deaktivieren – Change Logon

Mit diesem über die Eingabeaufforderung direkt verfügbaren Tool können Sie die Anmeldung auf einem Remotedesktopserver aktivieren oder deaktivieren. Wenn Sie zum Beispiel einen Remotedesktopserver warten und nicht wollen, dass sich Benutzer mit dem Server verbinden, können Sie Change Logon verwenden. Dazu stehen Ihnen verschiedene Optionen zur Verfügung:

- **change logon /enable** Aktiviert die Anmeldung auf einem Remotedesktopserver
- **change logon /disable** Deaktiviert die Anmeldung. Es darf sich kein Benutzer mehr auf dem Remotedesktopserver anmelden.
- **change logon /drain** Durch diese Option werden neue Anmeldungen verhindert, aber getrennte Sitzungen auf dem Server können wieder neu aufgebaut werden
- **change logon /drainuntilrestart** Durch diese Option werden neue Anmeldungen bis zu einem Neustart des Servers verhindert, aber getrennte Sitzungen auf dem Server können wieder neu aufgebaut werden
- **change logon /query** Mit dieser Abfrage können Sie den aktuellen Status der Anmeldung abfragen

Prozessinformationen auf Remotedesktopservern abrufen – Query

Mit diesem über die Eingabeaufforderung direkt aufrufenbaren Befehl können Sie verschiedene Abfragen starten, um sich einen Überblick zu verschaffen, welche Prozesse zurzeit laufen und welche Benutzer angemeldet sind. Sie können sich alle Remotedesktopserver des Standorts anzeigen lassen. Grundsätzlich gibt es vier wichtige Optionen, die Sie mit Query nutzen können:

- **query process** Dieser Befehl zeigt alle laufenden Prozesse auf dem Remotedesktopserver
- **query session** Mit diesem Befehl werden alle laufenden Terminalsitzungen angezeigt
- **query termserver** Alle Remotedesktopserver im Subnetz werden angezeigt
- **query user** Alle auf dem Remotedesktopserver angemeldeten Benutzer werden angezeigt

Terminalsitzungen zurücksetzen – Reset

Mit diesem Befehl können Sie anhand Ihrer ID Sitzungen auf dem Remotedesktopserver zurücksetzen. Sie können zum Beispiel mit der Anweisung *query session* alle Sitzungen mit deren ID anzeigen lassen. Im Anschluss können Sie mit *reset session <Nummer der Session>* eine bestimmte Sitzung zurücksetzen. Dieser Vorgang geht oft schneller als in der Remotedesktopserver-Verwaltung.

Terminalsitzungen ab- und anmelden – TSCON und TSDISCON

Mit diesen beiden direkt über die Eingabeaufforderung aufrufbaren Befehlen können Terminalsitzungen verbunden oder abgemeldet werden. Diese Funktion hat die gleiche Bedeutung wie in der Remotedesktopserver-Verwaltung, wenn eine getrennte Sitzung wieder mit einem Client verbunden werden soll. Bei diesen Befehlen werden die Benutzer nicht zurückgesetzt und deren Sitzung gelöscht, sondern nur getrennt oder erneut verbunden.

TSCON

```
Tscon {<Sitzungskennung> | <Sitzungsname>} [/dest:<Sitzungsname>] [/password:<Kennwort>]
[/v]
```

Wenn Sie den optionalen Parameter */dest:<Sitzungsname>* verwenden, ist dieser die Kennung der Sitzung, mit der eine Verbindung hergestellt werden soll. Dieser gibt den Namen der aktuellen Sitzung an. Diese Sitzung wird getrennt, wenn eine Verbindung mit der neuen Sitzung hergestellt wird. Sie müssen über die Zugriffsberechtigung für den Vollzugriff oder über die beschränkte Zugriffsberechtigung für den Verbindungsaufbau verfügen, um eine Verbindung mit einer anderen Sitzung herstellen zu können. Mit dem Parameter */dest:<Sitzungsname>* können Sie die Sitzung eines anderen Benutzers mit einer anderen Sitzung verbinden. Geben Sie im Parameter *Kennwort* kein Kennwort an und gehört die Zielsitzung einem anderen Benutzer als dem aktuellen, schlägt die Ausführung von TSCON fehl. Mit der Konsolensitzung kann keine Verbindung hergestellt werden.

Beispiele:

- Geben Sie *tscon 12* ein, um eine Verbindung mit Sitzung *12* auf dem aktuellen Remotedesktopserver herzustellen und um die aktuelle Sitzung zu trennen
- Geben Sie *tscon 23 /password:<meinkennwort>* ein, um eine Verbindung mit Sitzung *23* auf dem aktuellen Remotedesktopserver unter Verwendung des Kennworts *<meinkennwort>* herzustellen und um die aktuelle Sitzung zu trennen
- Geben Sie *tscon TERM03 /v /dest:TERM05* ein, um eine Verbindung zwischen der Sitzung *TERM03* und der Sitzung *TERM05* herzustellen und dann die noch verbundene Sitzung *TERM05* zu trennen

TSDISCON

```
Tsdiscon [{Sitzungskennung | Sitzungsname}] [/server:Servername] [/v]
```

Zum Trennen eines anderen Benutzers von einer Sitzung müssen Sie über die Berechtigung zum Vollzugriff verfügen. Wird keine Sitzungskennung oder kein Sitzungsname angegeben, trennt TSDISCON die aktuelle Sitzung. Alle Anwendungen, die beim Trennen der Sitzung ausgeführt wurden, werden beim erneuten Verbinden mit dieser Sitzung automatisch und ohne Datenverlust wieder ausgeführt. Verwenden Sie den Befehl *reset session*, um die aktiven Anwendungen der getrennten Sitzung zu beenden. Dies kann jedoch bei der betreffenden Sitzung zum Verlust von

Daten führen. Der Parameter */server* ist nur erforderlich, wenn Sie TSDISCON von einem Remoteserver aus verwenden. Die Konsolensitzung kann nicht getrennt werden.

Beispiele:

- Geben Sie *tsdiscon* zum Trennen der aktuellen Sitzung ein
- Geben Sie *tsdiscon 10* zum Trennen von Sitzung *10* ein
- Geben Sie *tsdiscon TERM04* zum Trennen der Sitzung mit dem Namen *TERM04* ein

Prozesse auf Remotedesktopservern beenden – TSKILL

Mit diesem Befehl können Sie einzelne Prozesse auf einem Remotedesktopserver beenden. Sie können sich zum Beispiel mit *query process* alle laufenden Prozesse anzeigen lassen und im Anschluss mit *tskill <PID des Prozesses>* den Prozess beenden.

Die Syntax des Befehls lautet:

```
Tskill {<Prozesskennung> | <Prozessname>} [/server:<Servername>] [{/id:<Sitzungskennung> |
/a}] [/v]
```

- **Prozesskennung** Die Kennung des zu beendenden Prozesses (PID)
- **Prozessname** Der Name des zu beendenden Prozesses. Sie können bei der Eingabe dieses Parameters Platzhalterzeichen verwenden.
- **/server:<Servername>** Gibt den Remotedesktopserver an, auf dem sich der zu beendende Prozess befindet. Erfolgt keine Angabe, wird der aktuelle Remotedesktopserver verwendet.
- **/id:<Sitzungskennung>** Beendet den in der angegebenen Sitzung ausgeführten Prozess
- **/a** Beendet den in allen Sitzungen ausgeführten Prozess
- **/v** Zeigt Informationen zu den Aktionen an, die gerade ausgeführt werden

Wenn Sie kein Administrator sind, können Sie den Befehl TSKILL nur zum Beenden der Prozesse verwenden, die Sie besitzen. Administratoren haben Vollzugriff auf alle Funktionen von TSKILL und können Prozesse in Sitzungen anderer Benutzer beenden. Werden alle in einer Sitzung ausgeführten Prozesse beendet, wird die Sitzung ebenfalls beendet.

Beispiele:

- Um den Prozess *6543* zu beenden, geben Sie *tskill 6543* ein
- Um den in Sitzung 5 ausgeführten Prozess *explorer* zu beenden, geben Sie *tskill explorer /id:5* ein

Tools für Exchange

Auf den folgenden Seiten zeigen wir Ihnen einige interessante Tools, die Sie mit Exchange oder SharePoint einsetzen können. Die meisten Tools sind für die neuen Versionen Exchange Server 2010 und SharePoint Server 2010 oder SharePoint Foundation 2010 entwickelt. Einige Tools funktionieren aber auch noch in den Vorgängerversionen.

Exchange-Datenbanken reparieren – Eseutil

Ist eine Exchange-Datenbank defekt, kommt oft das Befehlszeilentool Eseutil zum Einsatz. Mit Eseutil können Sie die einzelnen Datenbankdateien von Exchange bearbeiten und überprüfen. Das Tool finden Sie im Exchange-Installationsordner im Unterordner *\bin*. Unter Exchange Server 2007/2010 können Sie Eseutil aus jedem Pfad heraus starten.

Oft ist auf einem Server nicht genügend Platz, um mit Eseutil eine Datenbank zu reparieren. Auch wenn die Hardware defekt ist und parallel zur Exchange-Datenbank repariert werden soll, ist es sinnvoll, Eseutil auf einem anderen Server oder PC ohne installierten Exchange-Server starten zu können. Dadurch besteht die Möglichkeit, die zeitaufwändige Reparatur von Exchange parallel zum Aufsetzen eines neuen Servers durchzuführen. Damit Sie Eseutil auch von einem anderen Computer aus starten können, müssen Sie die folgenden Dateien zusammen mit den Datenbankdateien kopieren:

- *eseutil.exe*
- *ese.dll*
- *jcb.dll*
- *exosal.dll*
- *exchmem.dll*

Der wichtigste Schritt ist die Überprüfung der Exchange-Datenbank auf Konsistenz. Mit dem Befehl *eseutil /mh* stellen Sie die Konsistenz des Headers der Datenbank fest. Dem Befehl müssen Sie dabei auch den Pfad zur Datenbank mitgeben oder Sie wechseln in der Eingabeaufforderung in den Ordner der Datenbank. Dieses finden Sie in den Eigenschaften der Datenbank in der Exchange-Verwaltungskonsole über *Organisationskonfiguration/Postfach*. Befinden sich im Pfad Leerzeichen, schreiben Sie ihn in Anführungszeichen, zum Beispiel: *eseutil /mh "Mailbox Database 10016895577.edb"*. Bevor Sie den Befehl verwenden können, müssen Sie außerdem die Bereitstellung für die Datenbank aufheben oder den Dienst für den Informationsspeicher beenden, falls Sie den Befehl auf dem Server direkt ausführen.

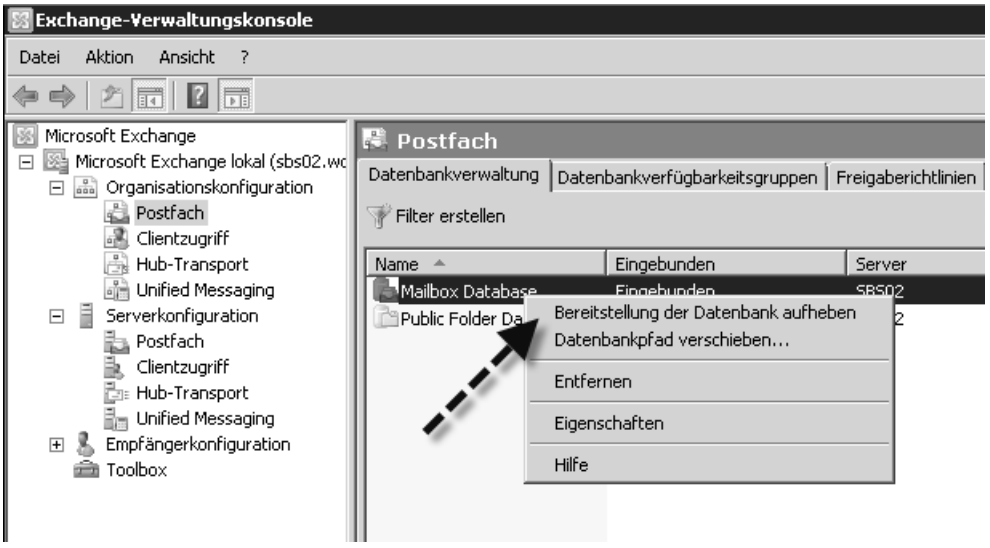

Abbildung 4.5 Vor der Bearbeitung von Datenbankdateien mit Eseutil müssen Sie die Bereitstellung aufheben

Die Ausgabe des Befehls sollte keine Fehler anzeigen. Im Bereich *State* sollte nach einem normalen Herunterfahren des Servers *Clean Shutdown* erscheinen. Ist die Datenbank abgestürzt und wurde nicht korrekt heruntergefahren, erscheint hier *Dirty Shutdown* und der Befehl meldet Transaktionsprotokolle, die noch in der Datenbank fehlen. Diese Protokolle finden Sie direkt unter *State* im Bereich *Log Required*.

Stellen Sie sicher, dass die entsprechenden Transaktionsprotokolle im Ordner liegen, oder kopieren Sie diese aus der Datensicherung in den Ordner. Die Ausgabe von Eseutil erfolgt dezimal, die Bezeichnung der Transaktionsprotokolle jedoch hexadezimal. Hier müssen Sie den Namen umrechnen, um an das oder die fehlenden Transaktionsprotokolle zu kommen. Fehlen Transaktionsprotokolle und können diese auch aus der Datensicherung nicht mehr hergestellt werden, besteht die Gefahr, dass Sie die Datenbank nur mit Datenverlust reparieren können – die Daten aus den fehlenden Transaktionsprotokollen sind verloren.

Steht bei *Bad Checksum Error Count* nicht der Wert *none*, passen Sie mit dem Tool Isinteg die Datenbank an. Das Tool gehört ebenfalls zu den Exchange-Bordmitteln. Zunächst starten Sie hierfür den Dienst für den Informationsspeicher und heben die Bereitstellung des Informationsspeichers, der repariert werden soll, auf. Startet der Dienst nicht mehr, ist eine Reparatur der Datenbank über diesen Weg nicht möglich. Startet der Informationsspeicher, verwenden Sie den Befehl *isinteg –s {Name des Servers} –fix –test alltests*. Sobald das Tool fertig ist, Reparaturen durchgeführt hat und keine Fehler ausgibt, kann die Bereitstellung wiederhergestellt werden. Allerdings sollten in diesem Fall auch die weiteren Tests in diesem Abschnitt durchgeführt werden, da die Datenbank durchaus noch Inkonsistenzen enthalten kann.

Sie können für die Reparatur in Exchange Server 2010 SP1 auch das neue Cmdlet *New-MailboxRepairRequest* verwenden. Die Funktionen von Isinteg sind jetzt in den neuen Cmdlets New-MailboxRepairRequest und New-PublicFolderDatabaseRepairRequest der Exchange-Verwaltungsshell integriert. Die beiden neuen Cmdlets können auch Datenbanken überprüfen, die bereitgestellt sind. Mit den neuen Tools lassen sich leicht korrupte Einträge in den Datenbanken und den Suchordnern beheben. Diese Aufgaben können seit Exchange Server 2010 SP1 online durchgeführt werden. Das Befehlszeilentool Isinteg kann nur Datenbanken reparieren, die nicht online waren. Die Syntax des Befehl lautet:

```
New-MailboxRepairRequest –[Mailbox oder Database] <MailboxIdParameter> –CorruptionType
<MailboxStoreCorruptionType[]> [–Archive <SwitchParameter>] [–Confirm [<SwitchParameter>]]
[–DetectOnly <SwitchParameter>] [–DomainController <Fqdn>] [–WhatIf [<SwitchParameter>]]
```

Sie können mit der Option –Mailbox ein einzelnes Postfach überprüfen, mit –Database eine komplette Datenbank und mit –Archive das Archivpostfach eines Anwenders.

Die Option –CorruptionType gibt mit zusätzlichen Parametern an, welche Überprüfungen das Tool durchführen soll. Hier stehen die Parameter SearchFolder, AggregateCounts, ProvisionedFolder und FolderView zur Verfügung.

Verwenden Sie die Option –DetectOnly, zeigt das Tool die Fehler lediglich an, behebt sie aber nicht. Sie können auf jedem Postfachserver immer nur eine Datenbank gleichzeitig überprüfen.

Einige Beispiel für die Cmdlets sind:

- New-MailboxRepairRequest –Mailbox joost@contoso.com –CorruptionType SearchFolder, AggregateCounts, ProvisionedFolder, FolderView
- New-MailboxRepairRequest –Mailbox joost –CorruptionType SearchFolder, AggregateCounts, ProvisionedFolder, FolderView –WhatIf
- New-MailboxRepairRequest –Database "Mailbox Database" -CorruptionType SearchFolder,AggregateCounts,ProvisionedFolder,FolderView
- New-PublicFolderDatabaseRepairRequest –Database PF1 –CorruptionType ReplState –DetectOnly

Weitere Beispiele erhalten Sie auch in der Exchange-Verwaltungsshell selbst, wenn Sie die folgenden Befehle verwenden:

```
Get-help New-MailboxRepairRequest –examples
Get-help New-PublicFolderDatabaseRepairRequest –examples
```

Die Cmdlets zeigen allerdings keinerlei Ergebnisse in der Exchange-Verwaltungsshell an, sondern in der Ereignisanzeige auf dem Server. Diese öffnen Sie am schnellsten durch Eingabe von eventvwr im Suchfeld des Startmenüs. Die Einträge finden Sie über Windows-Protokolle/Anwendung, allerdings nur auf dem Postfachserver, auf dem Sie die Datenbank oder das Postfach überprüfen lassen. Die Quelle der Ereignisse sind MSExchangeIS Mailbox Store und folgende mögliche IDs:

- 10047: Mailbox-Überprüfung gestartet
- 10064: Öffentliche Ordner-Überprüfung gestartet

- 10048: Überprüfung erfolgreich beendet
- 10050: Ein Postfach wurde vom Assistent übersprungen
- 10059: Datenbanküberprüfung gestartet
- 10062: Korruption entdeckt

Nach dem Test sollten Sie also in der Ereignisanzeige auch den Eintrag mit der ID 10048 finden, die ID 10062 deutet auf einen Fehler hin. Beheben die Cmdlets Fehler auf der Datenbank, können Sie den Reparaturvorgang unterbrechen, indem Sie die Bereitstellung der Datenbank aufheben. Verwenden Sie dazu in der Exchange-Verwaltungsshell den Befehl:

```
DisMount-Database –Identity <Name der Datenbank>
```

Repariert der Assistent ein Postfach, kann der entsprechende Anwender so lange nicht mehr auf sein Postfach zugreifen, bis die Reparatur abgeschlossen ist.

Der nächste Test besteht darin, die Datenbank auf Integrität zu überprüfen. Die Syntax sieht folgendermaßen aus:

```
eseutil /g "Mailbox Database <ID>.edb"
```

Bei diesem Test sollten möglichst keine Fehler auftreten, nur dann ist die Integrität der Datenbanken gewährleistet. Erhalten Sie hier Fehler, sollten Sie die Datenbank reparieren, zum Beispiel durch eine Offlinedefragmentierung.

Die Integrität der Datenbank sollte immer bei einem Ausfall überprüft werden. Ein weiterer Test besteht darin, die Datenbankdatei selbst auf Konsistenz zu überprüfen. Mit diesem Test stellen Sie fest, ob die Datenbankdatei physisch in Ordnung ist. Nutzen Sie hierfür die Option */k* von Eseutil.

Zumindest die Dateien der Datenbank sollten für eine Reparatur konsistent sein. Eine letzte Hoffnung stellt in diesem Fall noch die Offlinedefragmentierung mit der Option */d* dar.

Haben Sie sichergestellt, dass die Hardware des Servers funktioniert, die Datenbankdateien konsistent sind und alle Transaktionsprotokolle im entsprechenden Ordner liegen, können Sie mit der Wiederherstellung fortfahren. Sind die Datenbankdateien nicht konsistent, sollten leere Dateien oder Dateien aus der letzten Sicherung wiederhergestellt werden. Ist nur die Datenbank selbst inkonsistent oder fehlen lediglich Transaktionsprotokolle, wie der Test mit *eseutil /g* geprüft hat, kann die Datenbank unter Umständen gerettet werden. Bei diesem Vorgang werden die fehlenden Transaktionsprotokolle in die Datenbank geschrieben, die nach dem Vorgang hoffentlich wieder konsistent ist. Eseutil stellt dazu die Option */r* zur Verfügung, mit der dieser Vorgang durchgeführt werden kann. Bei diesem Befehl arbeitet Eseutil alle Transaktionsprotokolle ab und überprüft, ob diese in die Datenbank geschrieben wurden. Fehlen Daten, werden diese aus den Transaktionsprotokollen nachgetragen. Die Syntax dazu lautet

```
eseutil /r E{nn}
```

Der Parameterzusatz *{nn}* entspricht einer Zahl, mit der die Transaktionsprotokolldateien bezeichnet sind. Bei der ersten Datenbank handelt es sich hierbei um *"00"*. Wichtig an dieser Stelle ist, dass der Befehl in jenem Ordner ausgeführt wird, in dem die Transaktionsprotokolle und die Checkpointdatei gespeichert sind. Kopieren Sie also alle notwendigen Dateien in den Ordner. Anschließend kann der Soft-Recovery-Vorgang starten, der ohne Fehlermeldung abschließen sollte. Sind die Datenbankdateien konsistent und liegen alle Transaktionsprotokolle vor, kann ein Soft-Recovery-Vorgang zur Wiederherstellung der Datenbank durchgeführt werden.

Leere Bereiche innerhalb der Datenbank werden zwar erneut genutzt, die Größe der Datenbankdateien wird jedoch nicht kleiner. Nach einem Reparaturvorgang ist es also unerlässlich, für die Datenbankdateien eine Offlinedefragmentierung durchzuführen. Auch zum Reparieren taugt die Offlinedefragmentierung, da der Assistent zusätzlich defekte Bereiche aus der Datenbank löscht. Die Offlinedefragmentierung dauert bei entsprechender Datenbankgröße oft mehrere Stunden. Aber nur dadurch stellen Sie sicher, dass die Datenbankdateien nach einer Reparatur vollständig in Ordnung sind. Während der Offlinedefragmentierung löscht Exchange leere und – falls noch vorhanden – korrupte Seiten aus den Datenbanken. Benutzer können während dieser Zeit nicht mit der Datenbank arbeiten, da diese nicht zur Verfügung steht.

Während der Onlinedefragmentierung, die Exchange automatisch durchführt, verkleinert der Server die Datenbanken nicht. Die Onlinedefragmentierung stellt lediglich Festplattenplatz wieder zur Verfügung, den Exchange nicht mehr verwendet. Dabei fasst der Server leere Bereiche innerhalb der Datenbank zusammen, verkleinert aber keine Dateien und überprüft auch nicht die Konsistenz. Die Gesamtgröße der Datei bleibt gleich. Für die Offlinedefragmentierung müssen Sie die Bereitstellung der Datenbanken aufheben oder den Informationsspeicherdienst beenden.

Mit dem folgenden Befehl zeigen Sie die aktuelle Größe der *.edb*-Datei der entsprechenden Datenbank sowie die Datenmenge an, um die Sie die Datenbank verkleinern können. Für den Befehl müssen Sie die Datenbank nicht herunterfahren:

```
get-mailboxdatabase –status | ft name,databasesize,availablenewmailboxspace
```

Ist der Unterschied zwischen DatabaseSize und AvailableNewMailBoxSpace recht groß, bietet es sich an, eine Defragmentierung durchzuführen.

Um eine Offlinedefragmentierung durchzuführen, starten Sie Eseutil mit der Option */d* und dem Pfad zur Datenbank, wie bereits zuvor dargestellt. Das Tool legt vor dem Defragmentierungsvorgang eine temporäre Kopie der Datenbankdatei an, die defragmentiert und nach dem Vorgang wieder zurückkopiert wird. Die Temporärdateien legt das Tool auf dem Laufwerk an, auf dem Sie Eseutil aufrufen. Aus diesem Grund sollte auf dem Datenträger ausreichend Speicherplatz vorhanden sein, also mindestens das Doppelte der Exchange-Datenbanken. Steht nicht genug Platz zur Verfügung, kann Eseutil im Notfall keine Datenbank defragmentieren oder reparieren. Die Alternative stellt das Kopieren der Datenbank- und Eseutil-Dateien auf einen anderen Computer dar. Die Syntax in der Eingabeaufforderung für eine Offlinedefragmentierung lautet zum Beispiel:

```
eseutil /d "C:\Programme\Microsoft\Exchange-Server\v14Mailbox\First Storage Group\Mailbox
Database.edb"
```

Sie können auch direkt in den Ordner der Datenbanken wechseln, um sich die Eingabe des Pfads zu sparen. Hat Eseutil mit der Defragmentierung begonnen, öffnet es die Datenbank und legt eine Kopie an. Während der Defragmentierung werden auch automatisch defekte Bereiche der Datenbank gelöscht. Durch diese Option können Sie also korrupte Datenbanken wieder reparieren oder nach einer Reparatur überprüfen. Unterbrechen Sie die Defragmentierung durch Herunterfahren des Servers, kann es sein, dass die temporär angelegte Datenbankdatei noch nicht über die Originaldateien kopiert ist. Lokalisieren Sie dann die Temporärdatenbank und kopieren Sie diese über die Originaldateien. Erhalten Sie beim Start Fehler angezeigt, dass die Datenbank keine Defragmentierung zulässt, versuchen Sie, die Datenbank wieder bereitzustellen. Starten Sie dann den Systemdienst für den Informationsspeicher neu und heben dann die Bereitstellung wieder auf. Exchange sollte jetzt alle Transaktionsprotokolle in die Datenbank geschrieben haben.

Abbildung 4.6 Offlinedefragmentierung einer Datenbank

Müssen Sie eine Exchange-Datenbank reparieren, ist es wichtig, zu wissen, auf welche Basis der gesicherten Daten Sie zurückgreifen können. Nicht immer gelingt es, eine korrupte Datenbank mit den beschriebenen Mitteln zu reparieren, sondern Sie müssen teilweise Daten oder die komplette Datenbank aus einer Sicherung wiederherstellen und unter Umständen mit Eseutil oder Isinteg bearbeiten.

Unbekannte E-Mails mit Exchange Server 2007 an öffentliche Ordner oder einzelne E-Mail-Adresse umleiten – CatchAllAgent

Sobald eine E-Mail bei einem Exchange-Server eingeht, deren Empfänger in Active Directory nicht bekannt ist, blockiert der Empfängerfilter diese E-Mail. Es ist jedoch möglich, mit einem kleinen Zusatztool den Empfängerfilter so zu konfigurieren, dass bestimmte E-Mails entweder an ein bestimmtes Postfach oder an einen öffentlichen Ordner zugestellt werden. Das Tool funktioniert allerdings nur mit Exchange Server 2007. In Exchange Server 2010 können Sie dazu interne Bordmittel verwenden und benötigen kein Tool.

Das kleine Tool ändert dazu die Empfängeradresse so um, dass diese einem Empfänger in der Organisation entspricht, egal ob Anwender, öffentlicher Ordner oder Verteilerliste. Die Einstellungen für den Spamschutz werden auf einem Edge-Transport-Server automatisch installiert und aktiviert. Sie finden die Spamagenten auf der Registerkarte *Antispam*, wenn Sie auf dem Edge-Transport-Server in der Exchange-Verwaltungskonsole auf *Edge-Transport* klicken.

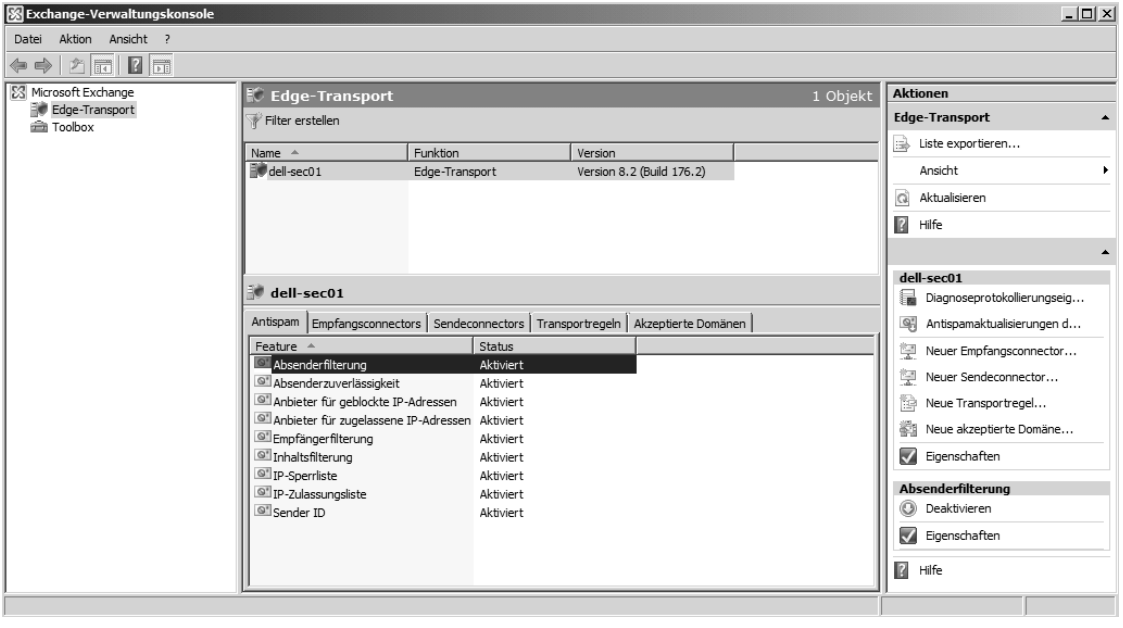

Abbildung 4.7 Spamagenten in Exchange Server 2007 verwalten

Setzen Sie keinen Edge-Transport-Server ein, können die Antispamfilter auch auf einem Hubtransportserver eingerichtet werden: Starten Sie die Exchange-Verwaltungsshell und wechseln in den Unterordner *Scripts* der Exchange Server 2007-Installation auf Ihrem Server. Dieser Ordner befindet sich im Exchange-Installationsordner. Geben Sie dazu in der Verwaltungsshell den Befehl *cd * ein. Anschließend können Sie mit *cd <Pfad>* zum Installationsordner von Exchange wechseln. Achten Sie auf die Anführungszeichen, wenn der Pfad ein Leerzeichen enthält. Geben Sie anschließend den Befehl *.\Install-AntispamAgents* ein. Nach der erfolgreichen Installation starten Sie den Systemdienst *Microsoft Exchange-Transport* neu. Sind die Spamagenten instal-

liert, finden Sie die neue Registerkarte *Antispam* vor, wenn Sie in der Exchange-Verwaltungskonsole auf *Organisationskonfiguration/Hub-Transport* klicken.

Schüsse ins Blaue verhindern – Empfängerfilterung konfigurieren

Eine Option zur Bekämpfung von Spam ist die Empfängerfilterung. Viele Spamversender versenden E-Mails, bei denen die Empfängeradressen nicht existieren, die E-Mail-Domäne aber schon. Das hat die Auswirkung, dass Administratoren im Unternehmen zahlreiche E-Mails erhalten, die nicht zugestellt werden können, aber dennoch gesichtet werden müssen, um normale E-Mails, bei denen ein Schreibfehler vorliegt, von Spam-E-Mails zu unterscheiden.

Mithilfe dieses Filters können E-Mails, die an bestimmte Empfänger innerhalb des Unternehmens geschickt werden, blockiert werden. Hauptsächlich wird dieser Filter aber dazu genutzt E-Mails zu blockieren, für die es im Unternehmen keinen Empfänger gibt. Unter Exchange Server 2007 sollte in den Eigenschaften des Filters auf der Registerkarte *Geblockte Empfänger* das Kontrollkästchen *Nachrichten, die an Empfänger gesendet werden, die nicht in der globalen Adressliste stehen, blocken* aktiviert sein. In diesem Fall werden Sie von Spam-E-Mails verschont, die ungezielt ins Blaue gerichtet sind. Absender, die nur versehentlich die falsche Adresse verwendet haben, erhalten einen Nichtzustellbarkeitsbericht (NDR) zurück und können die E-Mail noch einmal versenden.

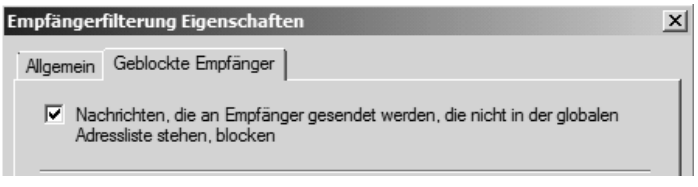

Abbildung 4.8 Spam-E-Mails, die nur an Ihre E-Mail-Domäne, aber mit falschen Empfängerdaten geschickt werden, können durch den Empfängerfilter leicht blockiert werden

CatchAllAgent installieren

Um einen Exchange-Server so zu konfigurieren, dass dieser E-Mails zu unbekannten Empfängern entgegennimmt und weiterleitet, gehen Sie folgendermaßen vor:

1. Laden Sie sich das Tool *CatchAllAgent* von der Internetseite *http://www.codeplex.com/catchallagent/Release/ProjectReleases.aspx?ReleaseId=8668* herunter. Sie benötigen nicht die Quelldateien, sondern nur den Agenten selbst. Sie benötigen die Dateien *CatchAllAgent.dll* und *config.xml*.
2. Kopieren Sie die Dateien in einen Ordner auf dem Server, zum Beispiel *C:\Programme\CatchAllAgent*.
3. Öffnen Sie anschließend die Datei *config.xml* in diesem Ordner mit einem Editor.
4. Die Datei enthält eine Beispielkonfiguration für Ihre Domäne nach der Art:

```
<config>
  <domain name="domain1.com" address="catchall@domain1.com" />
  <domain name="domain2.com" address="admin@domain2.com" />
</config>
```

Der Wert bei *domain name*= legt fest, welche DNS-Domäne der Agent behandeln soll, also Ihre E-Mail-Domäne, zum Beispiel *contoso.com*. Der Wert bei *address* legt fest, wie der Agent den Empfänger von unbekannten E-Mails umändern soll. Hier tragen Sie dann die Adresse ein, zu der unbekannte Mails gesendet werden sollen, zum Beispiel *spam@contoso.com*. Haben Sie den Agenten einmal eingerichtet, können Sie in dieser XML-Datei beliebig weitere Eintragungen vornehmen. Diese werden anschließend sofort übernommen, ohne dass Sie Dienste neu starten müssen. Fehler in der XML-Datei ignoriert Exchange einfach. Bearbeiten Sie die Datei mit der Domäne und dem Empfänger. Alle anderen E-Mail-Domänen, die Sie nicht in der Konfigurationsdatei hinterlegen, filtert der Empfängerfilter jedoch weiterhin.

Anschließend öffnen Sie auf dem Server eine Exchange-Verwaltungshell. Der Agent muss das erste Mal nach dem Download in Exchange integriert und gestartet werden. Zum Installieren geben Sie in der Verwaltungsshell den folgenden Befehl ein:

```
install-transportagent -Name "CatchAll Agent" -
TransportAgentFactory:CatchAll.CatchAllFactory -AssemblyPath:"C:\Program Files
(x86)\CatchAllAgent\CatchAllAgent.dll"
```

Achten Sie auf den korrekten Pfad zur Datei.

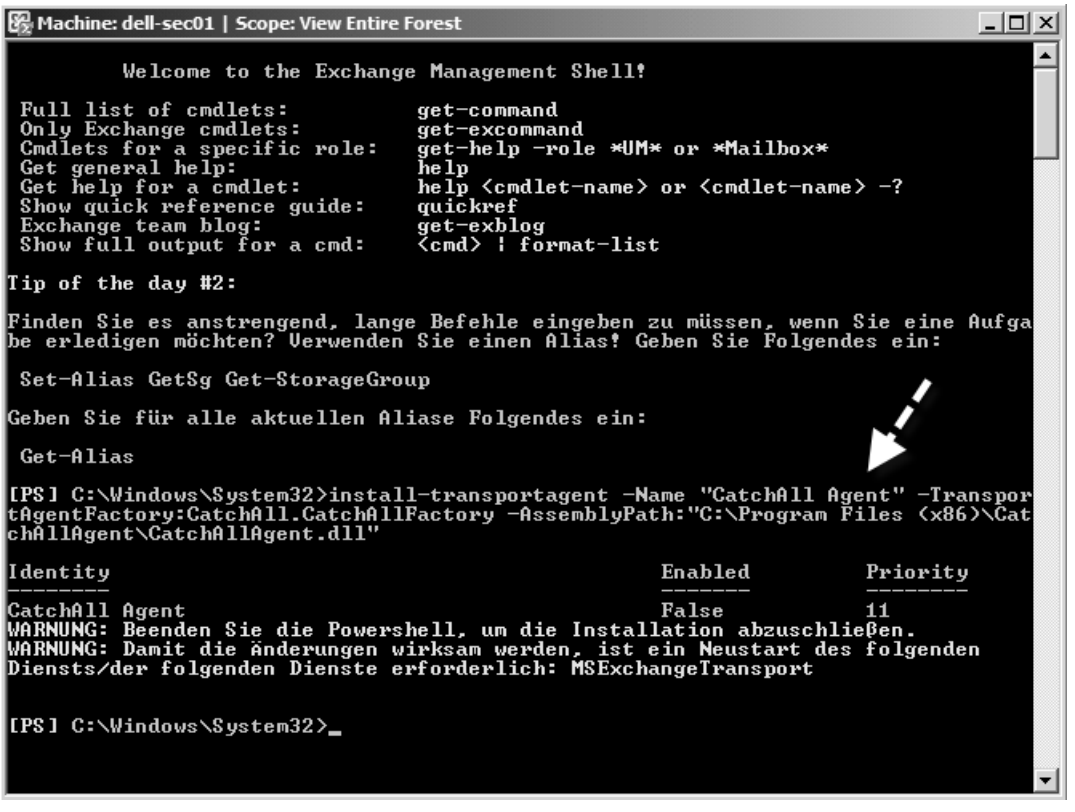

Abbildung 4.9 Installieren von CatchAllAgent auf dem Exchange-Server

Mit dem Befehl *Get-TransportAgent* lassen Sie sich alle installierten Transportagenten anzeigen. Dies sind die installierten Spamagenten von Exchange Server 2007 und der neu installierte *CatchAllAgent*. Dieser wird allerdings noch als nicht gestartet angezeigt und ist als Priorität ganz hinten angeordnet, wird also als letzter Agent und Filter ausgeführt.

Abbildung 4.10 Anzeigen der installierten Transportagenten von Exchange sowie deren Status

Der Empfängerfilter (Recipient Filter Agent) hat die Priorität 7, wird also vorher verwendet. Damit Exchange den *CatchAllAgent* verwendet, müssen Sie diesen von der Priorität vor den Empfängerfilter setzen. Dazu verwenden Sie den Befehl *Set-TransportAgent "CatchAll Agent" –Priority:7*. Überprüfen Sie anschließend wieder mit *Get-TransportAgent*, dass der Agent jetzt ordnungsgemäß vor dem Empfängerfilter angesetzt ist.

Im nächsten Schritt aktivieren Sie den Agenten mit dem Befehl *Enable-TransportAgent "CatchAll Agent"*. Auch diesen Vorgang kontrollieren Sie wieder mit *Get-TransportAgent*. Im nächsten Schritt müssen Sie noch den Systemdienst *MSExchangeTransport* neu starten. Verwenden Sie dazu die beiden folgenden Befehle:

```
net stop MSExchangeTransport
net start MSExchangeTransport
```

Neben der Möglichkeit, Nachrichten an Administratoren zu senden, können Sie auch Nachrichten an öffentliche Ordner senden. Dazu legen Sie einen entsprechenden öffentlichen Ordner an und aktivieren diesen für den E-Mail-Empfang. Über den Befehl *Enable-MailPublicFolder* können Sie einen öffentlichen Ordner mit E-Mail aktivieren, mit dem Befehl *Disable-MailPublicFolder* heben Sie die E-Mail-Erreichbarkeit wieder auf. Dem öffentlichen Ordner wird, genau wie Ihren Benutzern, eine E-Mail-Adresse durch die E-Mail-Adressenrichtlinien zugeteilt. Sie können die E-Mail-Aktivierung eines öffentlichen Ordners widerrufen. Die E-Mail-Adresse des öffentlichen Ordners wird gelöscht und sein Eintrag aus den Adresslisten entfernt. Benutzer können weiterhin Nachrichten im öffentlichen Ordner mit Outlook oder einem anderen Client bereitstellen, der Ordner ist aber nicht mehr per E-Mail direkt erreichbar. Daten gehen bei der E-Mail-Deaktivierung nicht verloren.

Standardmäßig darf jeder Benutzer E-Mails an diesen öffentlichen Ordner senden. Wollen Sie, dass ein öffentlicher Ordner E-Mails aus dem Internet erhalten soll, müssen Sie ihn zunächst für E-Mails aktivieren und Benutzern den anonymen Zugriff gestatten. Entziehen Sie einem öffentlichen Ordner die Berechtigung, von anonymen Benutzern E-Mails zu empfangen, ist dieser Ordner nicht per E-Mail über das Internet erreichbar. E-Mail-Absender, die über das Internet E-Mails an Ihre Exchange-Organisation schicken, sind immer anonym. Die Syntax des Befehls lautet:

```
Enable-MailPublicFolder -Identity <PublicFolderIdParameter> [-Confirm [<SwitchParameter>]]
[-DomainController <Fqdn>] [-HiddenFromAddressListsEnabled <$true | $false>] [-Server
<ServerIdParameter>] [-WhatIf [<SwitchParameter>]]
```

Verwenden Sie den Parameter *HiddenFromAddressListsEnabled*, um festzulegen, dass der Ordner in der Adressliste ausgeblendet werden soll. Alternativ können Sie auch die Öffentliche Ordner-Verwaltungskonsole im Bereich *Toolbox* der Exchange-Verwaltungskonsole verwenden. Klicken Sie dazu im linken Bereich auf *Öffentliche Standardordner* und im Ergebnisbereich auf den Ordner, für den Sie E-Mail aktivieren wollen. Wählen Sie im Aktionsbereich *E-Mail aktivieren*. Über den gleichen Weg deaktivieren Sie die E-Mail-Adresse auch wieder.

Normalerweise erhalten öffentliche Ordner die E-Mail-Adresse *<Name des Ordners>@<Ihre E-Mail-Domäne>*. Sie können die Adresse in der Öffentliche Ordner-Verwaltungskonsole in der Exchange-Verwaltungskonsole überprüfen, die Sie in der Toolbox finden. Klicken Sie auf den Ordner und rufen Sie im Ergebnisbereich dessen Eigenschaften auf. Auf der Registerkarte *E-Mail-Adressen* sehen Sie die E-Mail-Adresse des Ordners.

Microsoft Exchange Server SMTP-Diagnose-Tool

Ein wichtiges Diagnoseprogramm für den E-Mail-Fluss ist Smtpdiag, das Sie von der Microsoft-Internetseite *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=bc1881c7-925d-4a29-bd42-71e8563c80a9* kostenlos herunterladen können. Mit diesem Tool können Sie Probleme beim SMTP-Versand in der Eingabeaufforderung diagnostizieren und so die Sendeconnectors des Servers testen. Die Installationsdateien des Tools enthalten ein ausführliches Word-Dokument, in dem der Umgang erläutert wird.

Das Tool überprüft, ob eine E-Mail per SMTP zugestellt werden kann. Geben Sie den Befehl *smtpdiag <Absenderadresse> <Empfängeradresse>* ein, zum Beispiel *smtpdiag joost@contoso.com thomas.joos@web.de*. Das Tool überprüft, ob der Server die E-Mail durch die DNS-Auflösung zustellen könnte, und gibt Probleme sehr detailliert aus. Sie sehen bei der Ausgabe auch, wenn Server Verbindungen nicht akzeptieren oder andere Fehler, und können gezielt bei den entsprechenden Servern zur Fehlerbehebung ansetzen.

Abbildung 4.11 SMTP-Diagnosetest

Sie erkennen im Test, ob ein Server Fehler meldet und ob eventuell der empfangende Server keine Verbindungen von anderen Servern akzeptiert. Mit dem Tool erkennen Sie genau, woran der Fehler bei der Übertragung liegt, und können genau recherchieren.

Exchange Pre-Deployment Analyzer und Exchange Deployment Assistant

Bei der Migration und Einführung von Exchange Server 2010 unterstützt Microsoft Unternehmen mit den beiden kostenlosen Tools Exchange Pre-Deployment Analyzer und Exchange Deployment Assistant.

Organisation mit dem Exchange Pre-Deployment Analyzer testen

Vor einer Migration zu Exchange Server 2010 sollten Sie sich den Exchange Pre-Deployment Analyzer auf der Seite *http://www.microsoft.com/downloads/details.aspx?FamilyID=88b304e7-9912-4cb0-8ead-7479dab1abf2&displaylang=en* herunterladen. Mit diesem Tool können Sie bestehende Exchange-Organisationen auf eventuelle Konfigurationsprobleme scannen lassen, die eine Integration von Exchange Server 2010 verhindern.

Vor dem Exchange Pre-Deployment Analyzer sollten Sie alle Server in der vorhandenen Organisation zusätzlich noch mit dem Exchange Best Practices Analyzer scannen lassen und gefundene Fehler beheben.

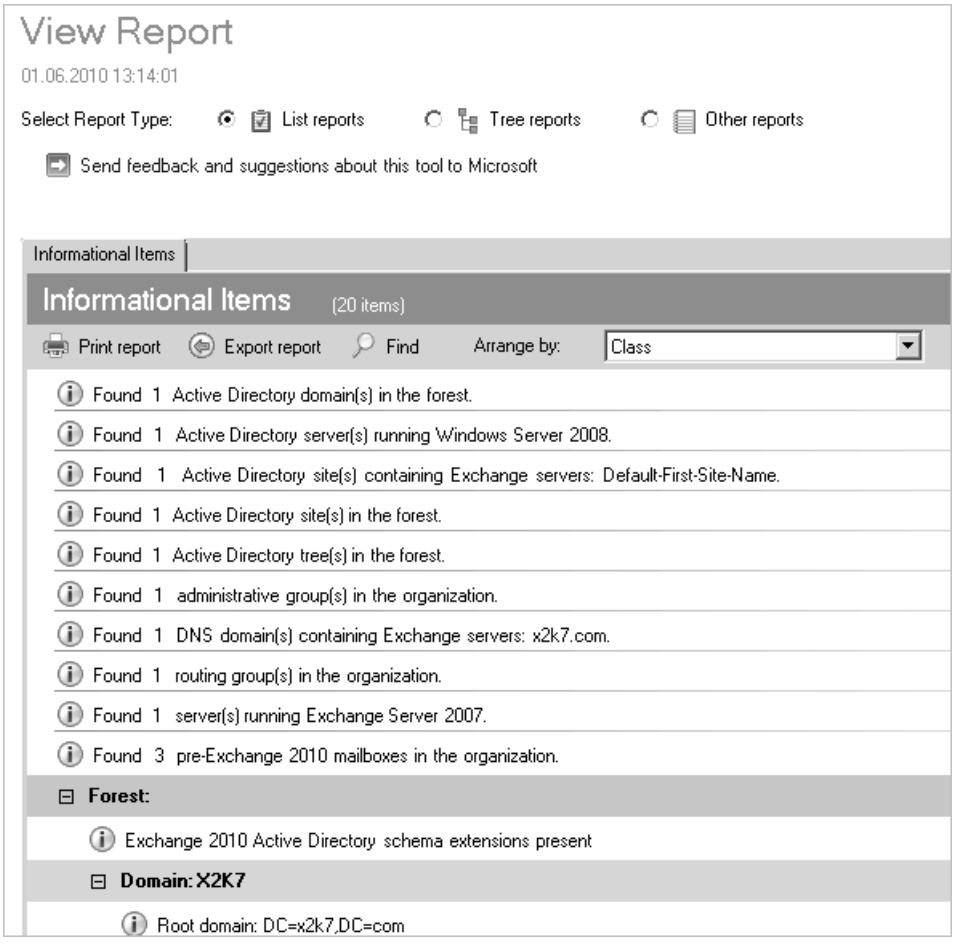

Abbildung 4.12 Exchange-Organisation für die Unterstützung von Exchange Server 2010 scannen

Der Umgang mit dem *Exchange Pre-Deployment Analyzer* entspricht dem Exchange Best Practices Analyzer. Haben Sie das Tool gestartet, erscheint unter Umständen ein Fehler, dass das Tool seine Konfigurationsdatei nicht finden kann. Kopieren Sie in diesem Fall die Dateien aus dem Ordner *C:\Program Files (x86)\Microsoft\Exchange Server\V14\ExPDA\en* in den Stammordner *C:\Program Files (x86)\Microsoft\Exchange Server\V14\ExPDA*. Wie beim Best Practices Analyzer sollten Sie auch beim *Microsoft Exchange Pre-Deployment Analyzer* nach dem Start zunächst eine Aktualisierung durchführen lassen und erst dann die Quellorganisation scannen lassen.

Migration planen mit dem Exchange Deployment Assistant

Haben Sie alle Probleme beseitigt, die der Exchange Best Practices Analyzer oder Exchange Pre-Deployment Analyzer findet, können Sie mit dem Exchange Deployment Assistant die einzelnen Schritte der Migration planen. Rufen Sie dazu die Seite *http://technet.microsoft.com/de-de/exdeploy2010* für eine deutschsprachige Unterstützung und die Seite *http://technet.microsoft.com/en-us/exdeploy2010* für den Assistenten in englischer Sprache auf. Achten Sie darauf, dass

für die Anzeige der Seite Microsoft Silverlight (*http://www.microsoft.com/germany/silverlight*) installiert sein muss. Der Assistent stellt Ihnen einige Fragen und gibt dann spezifische Hinweise und Anleitungen für die Migration zu Exchange Server 2010. Das Tool unterstützt auch die Migration zu Office 365.

Exchange Remote Connectivity Analyzer

Über die Microsoft-Seite *https://www.testexchangeconnectivity.com* können Sie die Verbindung Ihrer Exchange-Organisation mit dem Internet testen. Das Tool dient zum Testen der Verbindung von Outlook, Smartphones oder Office 365.

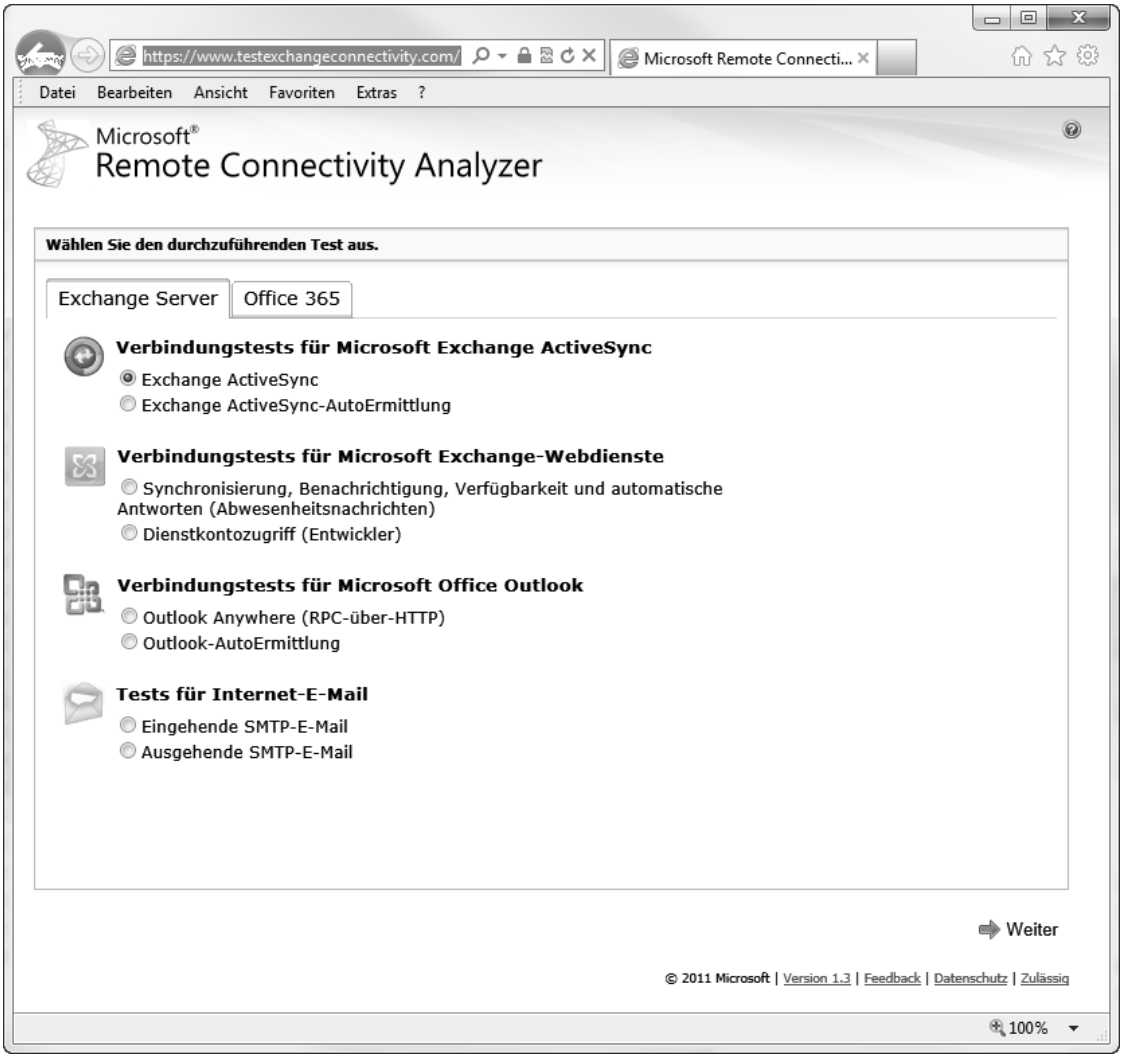

Abbildung 4.13 Verbindungstests für Exchange aus dem Internet

Haben Sie den gewünschten Test ausgewählt, geben Sie noch die Daten des Exchange-Servers ein, den Sie testen wollen, und die Benutzerdaten, mit denen Sie die Verbindung aufbauen. Anschließend testet das Tool die Verbindung und zeigt an, ob die Konfiguration funktioniert.

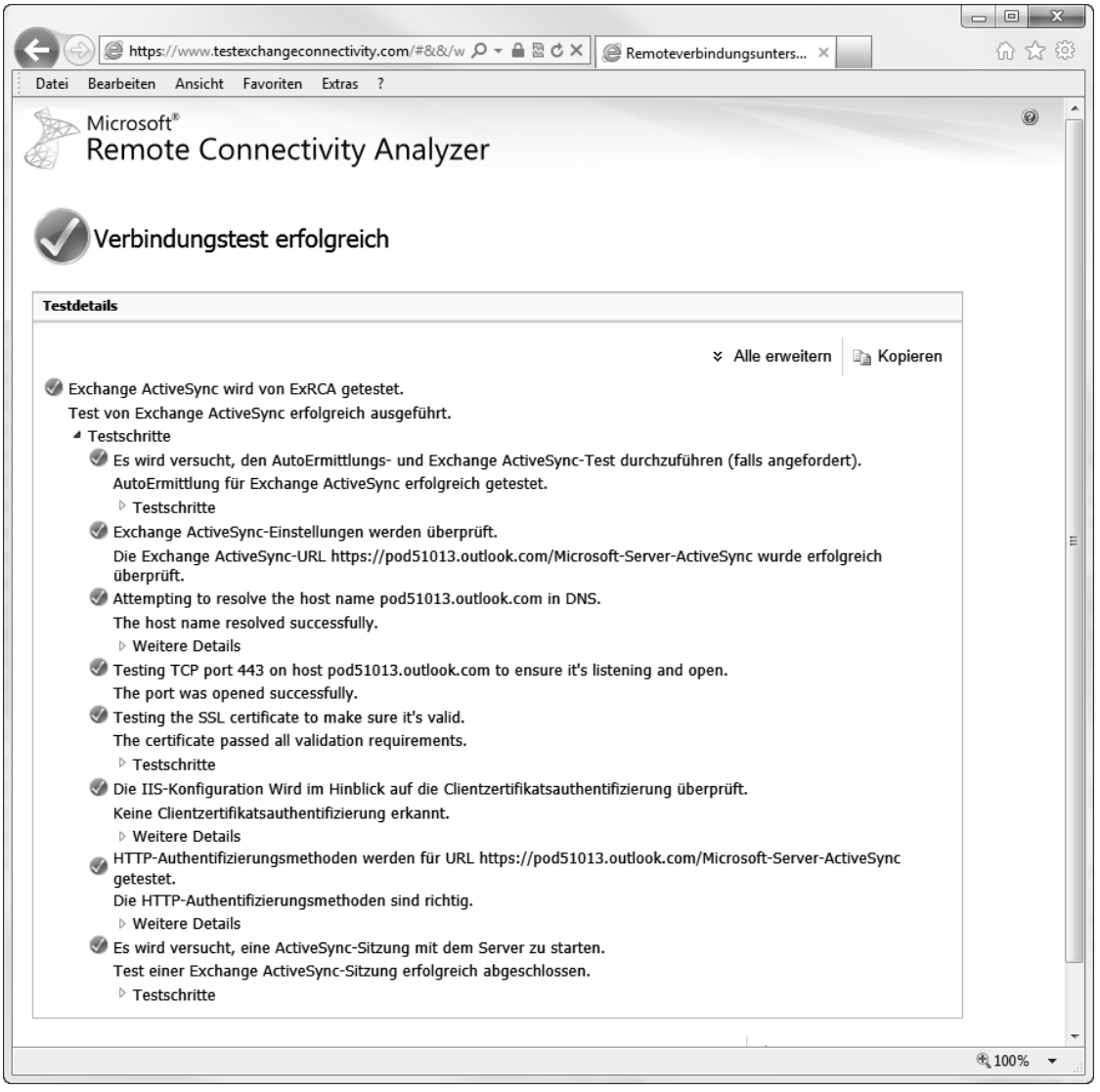

Abbildung 4.14 Verbindungstests mit dem Remote Connectivity Analyzer

Dateien aus Exchange-Datenbanken in .pst-Dateien exportieren

Eine häufig verwendete Methode, Inhalte aus Exchange-Datenbanken zu migrieren, besteht darin, die Inhalte der Postfächer in *.pst*-Dateien zu exportieren. Zum Beispiel können Sie diese Daten zur Wiederherstellung oder bei Migrationen in andere Exchange-Organisationen verwenden oder Anwender können diese Dateien direkt in Outlook einbinden.

Seit dem Service Pack 1 für Exchange Server 2007 lassen sich diese Vorgänge bequem über die Exchange-Verwaltungsshell durchführen. Und auch in Exchange Server 2010 und damit SBS 2011 ist dies problemlos möglich, allerdings mit neuen Cmdlets. Das Zusatztool ExMerge von den Vorgängerversionen benötigen Sie nicht mehr. Wir zeigen Ihnen aber auch die Möglichkeiten dieses Tools.

Zusätzlich müssen Sie bei Exchange Server 2007 und SBS 2008 noch Outlook 2007 auf dem Server installieren. Alternativ können Sie auch auf einer Arbeitsstation die PowerShell, Outlook 2010 x64 und die Exchange-Verwaltungstools installieren. Nach der Installation von Service Pack 1 für Exchange Server 2010 ist kein Outlook mehr notwendig, um Daten zu exportieren. Handelt es sich bei dem Computer, auf dem Sie den Exportvorgang durchführen, nicht um den Exchange-Server selbst, muss dieser dennoch Mitglied der gleichen Active Directory-Gesamtstruktur sein. Außerdem müssen Sie sich am Computer mit einem Konto anmelden, das in der Exchange-Organisation über umfassende Administratorrechte verfügt.

Der Vorgang beim Export ist denkbar einfach. Exchange Server 2010 verfügt über eine sehr granulare Berechtigungsstruktur auf Basis zahlreicher Rollen. Mit dem SP1 für Exchange Server 2010 sind die bekannten Cmdlets *Import-Mailbox* und *Export-Mailbox* nicht mehr vorhanden. Hier gibt es neue Cmdlets, die wir in den folgenden Abschnitten behandeln. Die beiden Cmdlets sind aber in Exchange Server 2007 noch verfügbar.

Postfächer in Exchange Server 2007 exportieren

Um Postfächer in Exchange Server 2007 oder SBS 2008 zu exportieren, verwenden Sie andere Cmdlets. Zunächst lassen Sie sich mit dem Befehl *Get-MailboxDatabase* eine Liste aller Exchange-Datenbanken anzeigen. Mit dem Befehl *Get-Mailbox –Database <Name des Exchange Servers>\<Postfachdatenbank> | Export-Mailbox –PSTFolderPath <Pfad>* exportiert die Exchange-Verwaltungsshell nach Bestätigung der Abfrage alle Postfächer eines Servers in *.pst*-Dateien.

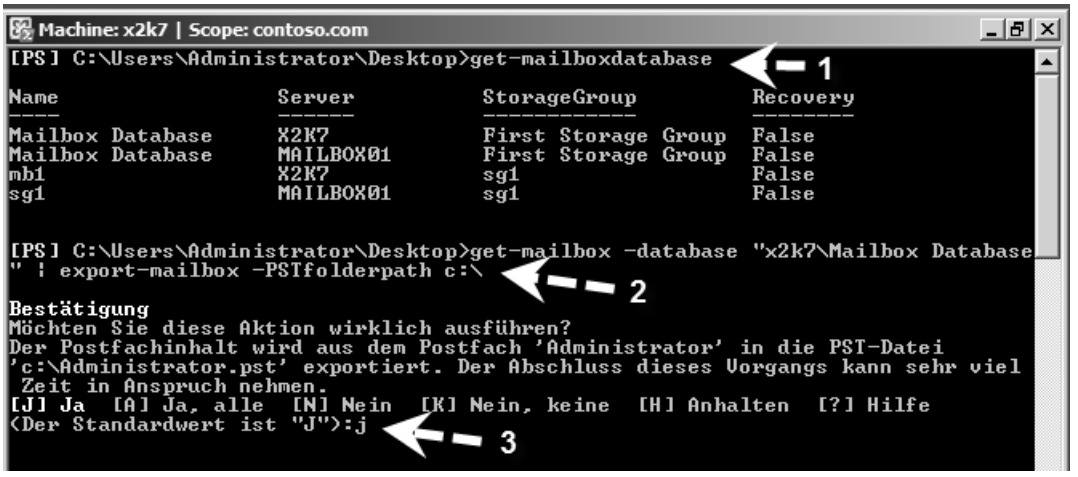

Abbildung 4.15 In drei kleinen Schritten werden alle Postfächer in Exchange Server 2007 von einer Datenbank in *.pst*-Dateien exportiert

Mit dem folgenden Befehl importieren Sie *.pst*-Dateien aus einem Ordner in eine bestimmte Datenbank:

```
Get-Mailbox –Database <Name des Exchange Servers>\<Postfachdatenbank> | Import-Mailbox –
PSTFolderPath <Pfad>
```

Was mit allen Benutzern geht, funktioniert auch mit einzelnen Anwendern. Hängen Sie am Ende des Befehls noch die Option *–confirm:$false* an, erfolgt der Export sofort ohne Rückfrage, zum Beispiel über Skripts.

Berechtigung für den Export in Exchange Server 2010 erteilen

Bevor Sie die Cmdlets für den Export und Import in Exchange Server 2010 verwenden können, müssen Sie Rechte für den Export vergeben. Standardmäßig dürfen auch Organisationsadministratoren oder Domänenadministratoren keine Exportvorgänge durchführen und sehen die entsprechenden Cmdlets auch nicht.

Als Administrator dürfen Sie sich zwar diese Rechte erteilen, haben diese aber standardmäßig noch nicht automatisch. Geben Sie daher in der Verwaltungsshell zunächst den folgenden Befehl ein:

```
New-ManagementRoleAssignment –Role "Mailbox Import Export" –User "<Benutzername>"
```

Alternativ können Sie auch eine Gruppe berechtigen. Verwenden Sie dazu den folgenden Befehl:

```
New-ManagementRoleAssignment –Role "Mailbox Import Export" –SecurityGroup "<Gruppe>"
```

Anschließend müssen Sie die Verwaltungsshell neu starten, da erst dann die Rechte verfügbar sind.

Ohne diese Rechte haben Sie als Administrator noch nicht mal das Recht, die entsprechenden Cmdlets überhaupt nur anzuzeigen.

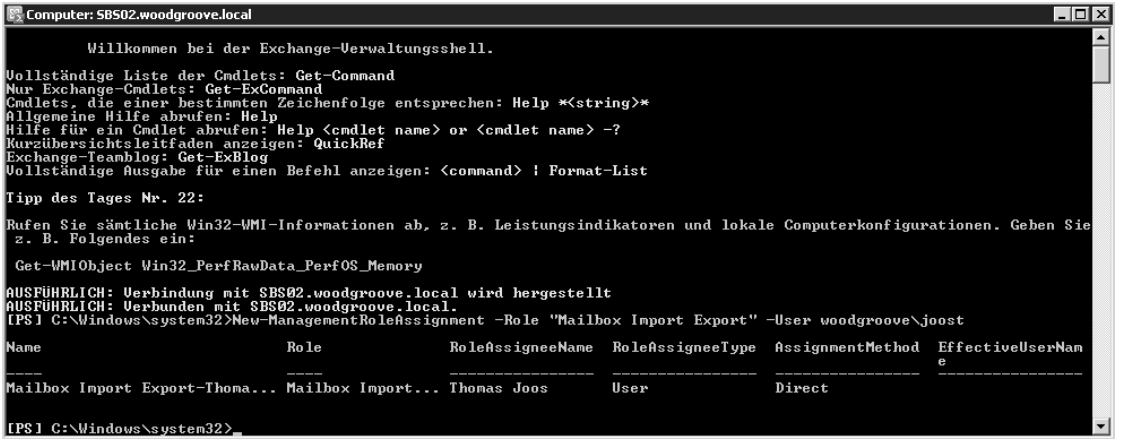

Abbildung 4.16 Zuweisen von Rechten für das Exportieren von Postfächern

Nach dem Neustart der Verwaltungsshell stehen die beiden neuen Cmdlets *New-MailboxExportRequest* und *New-MailboxImportRequest* zur Verfügung. Hilfe erhalten Sie über *Help New-MailboxExportRequest*, der Befehl *Help New-MailboxExportRequest –detailed* gibt ausführlichere Hilfen. Mit *Help New-MailboxExportRequest –examples* zeigt die Verwaltungsshell auch Beispiele an. Das Ganze funktioniert ebenfalls für *New-MailboxImportRequest*. Auf der TechNet-Seite *http://technet.microsoft.com/de-de/library/ff607299.aspx* finden Sie eine Erläuterung zu allen Optionen der beiden Cmdlets.

Die beiden alten Cmdlets *Import-Mailbox* und *Export-Mailbox* hat Microsoft in der finalen Version von SP1 für Exchange Server 2010 entfernt.

Mit SP1 für Exchange Server 2010 gibt es die bereits erwähnten Cmdlets, die das Exportieren und Importieren deutlich erleichtern. In der Tabelle 4.1 gehen wir auf diese Cmdlets und deren Möglichkeiten ein.

Cmdlet	Beschreibung
New-MailboxImportRequest	Mit diesem Cmdlet importieren Sie Daten einer *.pst*-Datei in Exchange-Datenbanken. Der Befehl überprüft den Import auf Duplikate und übergeht diese beim Import.
Get-MailboxImportRequest	Mit diesem Cmdlet erhalten Sie Informationen über aktuelle Importvorgänge und deren Status
Get-MailboxImportRequestStatistics	Mit diesem Befehl lassen sich weiterführende Informationen anzeigen, die über die Möglichkeiten von *Get-MailboxImportRequest* hinausgehen

Tabelle 4.1 Neue Cmdlets für den Export und Import von Postfächern

Cmdlet	Beschreibung
Remove-MailboxImportRequest	Dieses Cmdlet löscht Importvorgänge, die noch in der Warteschlangen stehen. Auch bereits durchgeführte Importe lassen sich mit dem Befehl aus der Anzeige entfernen.
Resume-MailboxImportRequest	Mit diesem Cmdlet starten Sie einen fehlgeschlagenen Import erneut. Auch mit *Suspend-MailboxImportRequest* pausierte Importvorgänge lassen sich mit dem Cmdlet wieder starten.
Set-MailboxImportRequest	Mit diesem Cmdlet passen Sie Optionen eines bereits erstellten Importvorgangs nachträglich an
Suspend-MailboxImportRequest	Mit diesem Befehl halten Sie einen oder mehrere Importvorgänge an
New-MailboxExportRequest	Mit diesem Befehl exportieren Sie Postfächer in *.pst*-Dateien
Get-MailboxExportRequest	Dieses Cmdlet zeigt Informationen zu den anstehenden Exportvorgängen an
Get-MailboxExportRequestStatistics	Mit diesem Cmdlet zeigen Sie erweiterte Informationen an, die *Get-MailboxExportRequest* nicht anzeigt
Remove-MailboxExportRequest	Löscht anstehende Exportvorgänge oder entfernt die Anzeige bereits durchgeführter Vorgänge
Resume-MailboxExportRequest	Mit diesem Cmdlet starten Sie einen fehlgeschlagenen Export erneut. Auch mit *Suspend-MailboxExportRequest* pausierte Exportvorgänge lassen sich mit dem Cmdlet wieder starten
Set-MailboxExportRequest	Mit diesem Cmdlet passen Sie Optionen eines bereits erstellten Exportvorgangs nachträglich an
Suspend-MailboxExportRequest	Mit diesem Befehl halten Sie einen oder mehrere Exportvorgänge an

Tabelle 4.1 Neue Cmdlets für den Export und Import von Postfächern *(Fortsetzung)*

Die Cmdlets zum Importieren und Exportieren bieten mit der Option *ContentFilter* weitreichende Möglichkeiten zur Filterung an. Mit dem Cmdlet *Get-Mailbox –Database <Name der Datenbank>* lassen Sie sich die Postfächer einer Datenbank anzeigen, zum Beispiel mit *Get-Mailbox –Database "Mailbox Database 2011011114"*.

```
[PS] C:\Windows\system32>get-mailboxdatabase

Name                           Server          Recovery        ReplicationType
----                           ------          --------        ---------------
Mailbox Database 2011011114    SBS2011         False           None


[PS] C:\Windows\system32>Get-Mailbox -Database "Mailbox Database 2011011114"

Name                      Alias                ServerName      ProhibitSendQuota
----                      -----                ----------      -----------------
Administrator             Administrator        sbs2011         unlimited
Thomas Joos               joost                sbs2011         unlimited
Tamara Bergtold           bergtoldt            sbs2011         unlimited
DiscoverySearchMailbox... DiscoverySearchMa... sbs2011         50 GB (53,687,091,200 bytes)
Fynn Joos                 fynn                 sbs2011         2 GB (2,147,483,648 bytes)
Super User                SuperUser            sbs2011         2 GB (2,147,483,648 bytes)
```

Abbildung 4.17 Anzeigen der Postfachdatenbanken eines Servers und der enthaltenen Postfächer

Wollen Sie *.pst*-Dateien in ein Exchange-Postfach importieren, verwenden Sie das Cmdlet *New-MailboxImportRequest*. Die *.pst*-Dateien, die Sie importieren, müssen über eine Dateifreigabe zur Verfügung stehen, da die neuen Cmdlets nur noch UNC-Pfade akzeptieren. Um eine *.pst*-Datei zu importieren, verwenden Sie folgenden Befehl:

```
New-MailboxImportRequest –Mailbox <Name des Postfachs> –FilePath <UNC-Pfad und Name der
.pst-Datei>
```

Bei dem folgenden Befehl importieren Sie den kompletten Inhalt der *.pst*-Datei:

```
New-MailboxImportRequest –Mailbox joost –FilePath \\sbs2011\temp\outlook1.pst
```

Verwenden Sie zusätzlich die Option *–verbose*, erhalten Sie weitere Informationen während des Imports und finden auch schneller eventuelle Fehler. Erhalten Sie eine Fehlermeldung angezeigt, überprüfen Sie mit dem Befehl *Get-ManagementRoleAssignment –RoleAssignee <Gruppe oder Benutzer>*, ob der Benutzer, mit dem Sie den Befehl durchführen, auch über die Rechte *Mailbox Import Export* verfügt. Außerdem muss das entsprechende Zielpostfach vorhanden sein.

Dieses Verhalten können Sie mit dem Befehl *Get-Mailbox –Identity <Name>* überprüfen. Mit dem Befehl *Get-Mailbox –identity <Name> | Get-MailboxPermission* überprüfen Sie, ob Sie über genügend Rechte für das Postfach verfügen. Mit den beiden Cmdlets *Get-MailboxImportRequest* und *Get-MailboxImportRequestStatistics* lassen Sie sich Informationen zu dem Importvorgang anzeigen. Auch bei diesen Cmdlets können Sie mit Pipes arbeiten, um ausführlichere Informationen zu erhalten:

```
Get-MailboxImportRequest <Name des Importvorgangs> | fl
```

Nachdem der Import erfolgreich durchgeführt wurde, müssen Sie die Anzeige des Importvorgangs noch löschen. Dazu verwenden Sie das Cmdlet *Remove-MailboxImportRequest*. Neben der Möglichkeit, die komplette *.pst*-Datei zu importieren, können Sie auch einzelne Ordner auswählen, die importiert werden sollen. Andere Ordner ignoriert der Befehl dann:

```
New-MailboxImportRequest –Mailbox <Name> –FilePath <UNC-Pfad und Name der .pst-Datei –
IncludeFolders <Name des Ordners aus der .pst-Datei>
```

Wollen Sie alle Ordner importieren und einzelne auslassen, verwenden Sie die Option *–Exclude-Folders*. Mit der Option *–ExcludeDumpster* schließen Sie den Papierkorb aus dem Import aus.

Sie haben auch die Möglichkeit, den Zielordner im Postfach genau festzulegen, in den das Cmdlet die Daten importieren soll:

```
New-MailboxImportRequest –Mailbox <Name> –FilePath <UNC-Pfad und Name der .pst-Datei> –
TargetRootFolder <Ordner im Postfach>
```

Den Ordner erstellt das Cmdlet automatisch, er muss nicht vorhanden sein. Verwenden Sie die Option *IsArchive*, importiert der Assistent die *.pst*-Datei in das Archiv des Benutzers:

```
New-MailboxImportRequest –Mailbox <Name> –IsArchive -FilePath <UNC-Pfad und Name der .pst-
Datei>
```

Wollen Sie Postfächer exportieren, verwenden Sie den Befehl:

```
New-MailboxExportRequest –Mailbox <Name> –FilePath <UNC-Pfad und Name der .pst-Datei>
```

Auch hierbei berücksichtigt das Cmdlet alle Ordner des Postfachs und importiert sie in die *.pst*-Datei. Mit den Cmdlets *Get-MailboxExportRequest* und *Get-MailboxExportRequestStatistics* lassen Sie sich Informationen anzeigen. Auch hier können Sie mit den gleichen Optionen zum Ein- und Ausschließen von Ordnern arbeiten wie beim Import.

Zusätzlich steht Ihnen beim Export noch die Option *–ContentFilter* zur Verfügung, mit der Sie filtern können, welche E-Mails exportiert werden sollen.

Sie haben auch die Möglichkeit, mit etwas Scripting alle Postfächer eines Servers in *.pst*-Dateien zu exportieren. Verwenden Sie dazu folgende Befehle:

```
$Export = get-mailbox –Database <Name der Datenbank>
$Export|%{$_|New-MailboxExportRequest –FilePath "<UNC-Pfad>\$($_.alias).pst"}
```

Anschließend exportiert das Cmdlet alle Postfächer in den von Ihnen angegebenen Ordner.

Abbildung 4.18 Exportieren mehrerer Postfächer

Entfernen Sie noch die Option *–Database* vom ersten Befehl, exportiert das Cmdlet sämtliche Postfächer aller Exchange-Server in der Organisation, wenn Sie von einer externen Organisation Postfächer zu SBS 2011 übernehmen wollen. Sie haben auch die Möglichkeit, die Exportvariable nur mit Benutzerkonten zu füllen, deren Benutzerkonto sich in einer bestimmten OU befindet. Dazu verwenden Sie folgenden Befehl:

```
$Export = Get-Mailbox –OrganizationalUnit "<Name der OU>"
```

Sie haben die Möglichkeit, *.pst*-Dateien direkt in das Benutzerarchiv des Anwenders zu importieren. Allerdings haben Sie auch die Möglichkeit, das Archivpostfach in eine *.pst*-Datei zu exportieren:

```
New-MailboxExportRequest –Mailbox <Name> –IsArchive –FilePath <Pfad und Name der .pst-
Datei>
```

Um mehrere Archivpostfächer zu exportieren, verwenden Sie wieder eine Variable, die Sie entsprechend füllen:

```
$Export = Get-Mailbox –Database <Name>
$Export|%{$_|New-MailboxExportRequest –FilePath \\<UNC-Pfad>\$($_.alias).pst –IsArchive}
```

Exchange Mailbox Merge Wizard (ExMerge)

Mit diesem Tool können Sie die Inhalte der Postfächer eines Exchange-Servers unter Exchange Server 2000 oder Exchange Server 2003 in *.pst*-Dateien exportieren und auf einen anderen Server wieder importieren. Sie können *.pst*-Dateien auch nur exportieren und mit den neuen Cmdlets wieder importieren. Die Bedienung ist recht einfach, da Sie eine grafische Oberfläche zum Tool enthalten. Kopieren Sie die Datei am besten direkt in den *\bin*-Ordner der Exchange-Installation.

Das Tool kann auch Elemente basierend auf dem Datum aus der Datenbank in *.pst*-Dateien verschieben und damit zur Archivierung dienen. Sie können Nachrichten auch basierend auf Kriterien wie Betreff oder Anlagen extrahieren und löschen. Auf diese Weise können Administratoren bestimmte Nachrichten oder Anlagen aus der Exchange-Datenbank entfernen. In einer gemischten Umgebung lässt sich ein Postfach aus einer administrativen Gruppe in eine andere Gruppe übertragen oder in eine andere Exchange-Organisation übernehmen.

Die Versionen von ExMerge sind für Exchange 5.5 und Exchange 2000/2003 unterschiedlich. ExMerge finden Sie auf der Exchange 2000-CD im *Support*-Ordner. Für Exchange Server 2003 können Sie das Tool von der Seite *http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=429163EC-DCDF-47DC-96DA-1C12D67327D5&displaylang=en* herunterladen. ExMerge ist nicht für den Einsatz für Exchange Server 2007/2010 oder SBS 2008/2011 geeignet. Verwenden Sie zum Export der Postfächer ausschließlich das Exchange-Dienstkonto oder ein Konto, welches explizit über Leserechte für alle Postfächer verfügt. Die *.ini*-Datei von ExMerge ist allerdings auf englische Exchange-Server ausgelegt. Wenn Sie bei sich einen deutschen Exchange-Server einsetzen, müssen Sie den Inhalt der *.ini*-Datei bearbeiten. Die Datei sollte so aussehen:

```
; EXEMERGE.INI
[EXMERGE]
LocalisedExchangeServerServiceName=Microsoft Exchange-Nachrichtenspeicher
LocalisedPersonalFoldersServiceName=Persönliche Ordner
LoggingLevel=3
LogFileName=C:\ExMerge.log
DataDirectoryName=C:\EXMERGEDATA
MergeAction=0
SourceServerName=COMPUTER
DomainControllerForSourceServer=
SrcServerLDAP-Port=
DestServerName=
DomainControllerForDestServer=
DestServerLDAP-Port=
SelectMessageStartDate=
SelectMessageEndDate=
ListOfFolders=
FileContainingListOfFolders=
FoldersProcessed=2
ApplyActionToSubFolders=1
FileContainingListOfMailboxes=
RemoveIntermediatePSTFiles=1
DateAttribute=0
DataImportMethod=2
ReplaceDataOnlyIfSourceItemIsMoreRecent=1
CopyUserData=1
CopyAssociatedFolderData=1
CopyFolderPermissions=1
CopyDeletedItemsFromDumpster=1
FileContainingListOfMessageSubjects=
SubjectStringMatchCriteria=0
FileContainingListOfAttachmentNames=
AttachmentNameStringMatchCriteria=1
MapFolderNameToLocalisedName=1
[International]
DefaultLocaleID=1031
[Folder Name Mappings]
Inbox = Posteingang
Deleted Items = Gelöschte Objekte
Sent Items = Gesendete Objekte
Outbox = Postausgang
```

Vor dem Einsatz von ExMerge lesen Sie sich ausführlich noch folgende Knowledge Base-Artikel durch:

- *http://support.microsoft.com/kb/292509/de*
- *http://technet.microsoft.com/en-us/library/aa996410(EXCHG.65).aspx*
- *http://support.microsoft.com/kb/174197*
- *http://support.microsoft.com/kb/265441*
- *http://blogs.technet.com/sbs/archive/2009/01/13/sbs-2008-how-to-export-and-import-mailboxes-to-and-from-pst.aspx*

- *http://blogs.technet.com/sbs/archive/2009/05/21/cannot-reply-to-old-emails-or-modify-old-calendar-items-after-pst-mail-migration.aspx*

Jetstress für Exchange Server 2010

Jetstress simuliert auf einer Serverhardware den realen Einsatz von Exchange mit allen Features, die Exchange auch auf einem richtigen Server ausführt. Da Exchange ein sehr festplattenlastiges Serverprogramm ist, sollten vor allem Administratoren großer Exchange-Organisationen die Hardware eines potenziellen Exchange-Servers vor der Installation testen.

Laden Sie sich die Jetstress-Version für Exchange Server 2010 herunter, da diese für die neuen Funktionen in Server Exchange 2010 optimiert ist. Sie können Jetstress kostenlos von der Homepage von Microsoft herunterladen (*http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=13267027-8120-48ed-931b-29eb0aa52aa6*). Nach dem Entpacken der Datei können Sie über die neue Programmgruppe Microsoft Exchange Jetstress starten. Das Tool dient vor allem für Tests des Festplattensystems von Postfachservern.

Tools für SharePoint

In den folgenden Abschnitten zeigen wir Ihnen einige Tools, die bei der Verwaltung von SharePoint helfen. Vor allem bei der Migration oder der Suche von Fehlern bieten die Tools einiges an Informationen.

Pre-Upgrade-Checker, WssAnalyzeFeature und Co.

Durch die Installation von Service Pack 2 für SharePoint Server 2007 erweitern Sie auch die Möglichkeiten des Befehlszeilentools Stsadm um die Option *–o preupgradecheck*. Dieser Befehl überprüft, ob die Umgebung kompatibel zu SharePoint Server 2010 ist und sich ein In-Place-Update durchführen lässt.

Verwenden Sie zusätzlich noch die Option *–localonly*, testet Stsadm nur den lokalen Server der Farm. Der Befehl liefert ihnen wichtige Informationen, die für die Migration notwendig sind:

- Eine Liste aller Server und Komponenten der Farm und deren Unterstützung für 64-Bit
- Die verschiedenen URLs, die Sie in der Farm nutzen
- Eine Liste aller Vorlagen, Features und Sprachpakete, die installiert sind
- Eine Liste aller nicht unterstützten Änderungen, die Sie in der Farm vorgenommen haben und die eine direkte Aktualisierung verhindern
- Eine Aufstellung fehlender Einstellungen, Hostnamen oder ungültiger Dienstkonten
- Größe der Datenbanken

Abbildung 4.19 SharePoint Server 2007 kann sich selbst auf Kompatibilität zu SharePoint Server 2010 testen

Um die Aktualisierung vorzubereiten, verwenden Sie den Befehl *stsadm –o preupgradecheck* auf dem Quellserver. Bevor Sie die Aktualisierung zu SharePoint Server 2010 durchführen, sollten Sie alle Fehler beseitigen, die das Tool meldet.

Meist wird für Stsadm kein Pfad angelegt, sodass Sie direkt in den Ordner des Tools wechseln müssen. Unter Windows Server 2008 R2 und Windows Server 2008 finden Sie das Tool im Ordner *C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN*. Das Tool gibt in der Eingabeaufforderung Informationen aus und speichert im Ordner *%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\12\LOGS* die HTML-Datei *SharePoint Products and Technologies Pre-Upgrade Check Report*. Die Datei erhält als Namen die Bezeichnung *PreUpradeCheck-<Datum>-<Uhrzeit>-<3-Stellige-Nummer>.htm*, die Sie auch auf anderen Rechnern auswerten können.

Das Tool liest lediglich Informationen aus und ändert keinerlei Einstellungen in SharePoint. Im Gegensatz zum Vorgänger in SharePoint Portal Server 2003 hat Microsoft das Tool nur für den lesenden Zugriff und zur Informationsgewinnung entwickelt. Sie sollten daher den Pre-Upgrade-Checker immer ausführen, egal welche Migrationsmethode Sie verwenden. Ebenfalls sollten Sie ihn auch dann ausführen, wenn Sie keine direkte Aktualisierung auf SharePoint Server 2010 durchführen, da Sie auch bei anderen Migrationen über das Tool wertvolle Hinweise erhalten. Wichtig in der HTML-Datei sind die Bereiche mit der Überprüfung von Sitedefinitionen. Hier sehen Sie die jeweiligen Bezeichnungen und deren Status.

Information Only : Site Definition Information
The following site definitions are either installed on this farm or referenced by the content:

- name = STS, language = 1031, template id = 1, count = 0, status = Internal
- name = MPS, language = 1031, template id = 2, count = 0, status = Internal
- name = CENTRALADMIN, language = 1031, template id = 3, count = 1, status = Internal
- name = WIKI, language = 1031, template id = 4, count = 0, status = Internal
- name = BLOG, language = 1031, template id = 9, count = 0, status = Internal
- name = BDR, language = 1031, template id = 7, count = 1, status = Installed
- name = OFFILE, language = 1031, template id = 14483, count = 0, status = Installed
- name = OSRV, language = 1031, template id = 40, count = 1, status = Installed
- name = SPS, language = 1031, template id = 20, count = 1, status = Installed
- name = SPSPERS, language = 1031, template id = 21, count = 0, status = Installed
- name = SPSMSITE, language = 1031, template id = 22, count = 0, status = Installed
- name = SPSTOC, language = 1031, template id = 30, count = 0, status = Installed
- name = SPSTOPIC, language = 1031, template id = 31, count = 0, status = Installed
- name = SPSNEWS, language = 1031, template id = 32, count = 0, status = Installed
- name = CMSPUBLISHING, language = 1031, template id = 39, count = 0, status = Installed
- name = BLANKINTERNET, language = 1031, template id = 53, count = 0, status = Installed
- name = SPSNHOME, language = 1031, template id = 33, count = 1, status = Installed
- name = SPSSITES, language = 1031, template id = 34, count = 1, status = Installed
- name = SPSCOMMU, language = 1031, template id = 36, count = 0, status = Installed
- name = SPSREPORTCENTER, language = 1031, template id = 38, count = 1, status = Installed
- name = SPSPORTAL, language = 1031, template id = 47, count = 0, status = Installed
- name = SRCHCEN, language = 1031, template id = 50, count = 1, status = Installed
- name = PROFILES, language = 1031, template id = 51, count = 1, status = Installed
- name = BLANKINTERNETCONTAINER, language = 1031, template id = 52, count = 0, status = Installed
- name = SPSMSITEHOST, language = 1031, template id = 54, count = 1, status = Installed
- name = SRCHCENTERLITE, language = 1031, template id = 90, count = 0, status = Installed

Abbildung 4.20 Status installierter Sitedefinitionen

Hier sollten Sie überprüfen, ob es für einzelne Sites Probleme gibt. Sie sehen das am Ende der entsprechenden Spalte im Bereich *status*=. In einigen Fällen kann es passieren, dass Vorlagen von Microsoft fehlen. Diese finden Sie zum Beispiel im Downloadcenter bei Microsoft. Haben Sie einen Fehler behoben, können Sie den Test erneut starten und überprüfen, ob SharePoint hier keine Fehler mehr findet. Ebenfalls wichtig in der HTML-Datei sind die installierten Features. Auch hier sollten keine Fehler auftreten.

Features, die SharePoint nicht identifizieren kann, sollten Sie vor der Migration deaktivieren. Dazu verwenden Sie den Befehl *stsadm –o deactivatefeature*. Die ausführliche Syntax des Befehls

finden Sie auf der Seite *http://technet.microsoft.com/en-us/library/cc288714%28office.12%29.aspx*. Ein einfacher Weg zum Deaktivieren eines Features ist der Befehl:

```
stsadm –o deactivatefeature –id <GUID, die Sie im HTML-Bericht sehen> –url <URL der
Websitesammlung> –force
```

Gelingt die Bereinigung der Features nicht, sind weitere Aktionen notwendig. Hier hilft das Tool WssAnalyzeFeatures von der Seite *http://code.msdn.microsoft.com/WssAnalyzeFeatures*. Das Tool laden Sie als in eine *.zip*-Datei verpackte *.exe*-Datei herunter. Die Syntax ist folgende:

```
WssAnalyzeFeatures –url <Website, die Sie prüfen wollen>
```

Das Tool prüft die installierten Features und listet in der Eingabeaufforderung eventuell vorhandene Fehler auf.

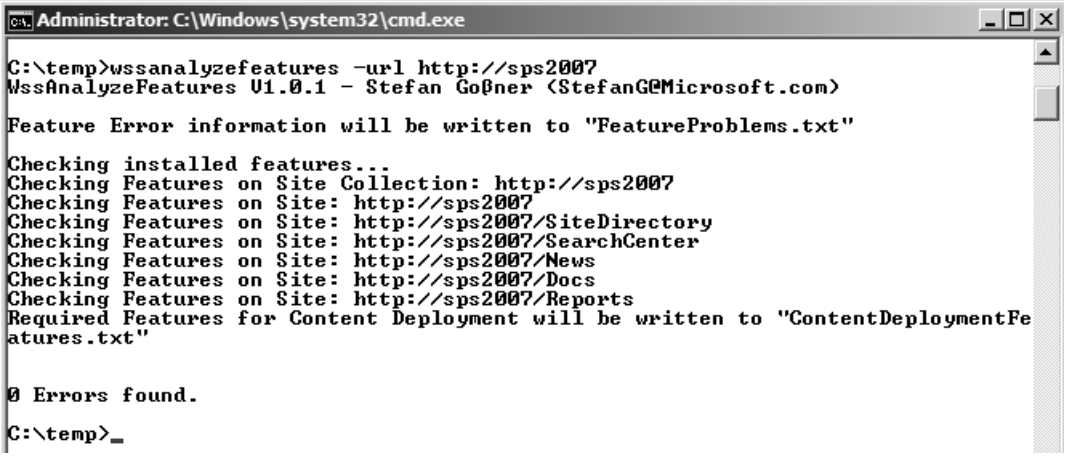

Abbildung 4.21 Überprüfen der installierten Features in SharePoint

Das Tool speichert zusätzlich im gleichen Ordner die Textdatei *ContentDeploymentFeatures.txt*. Hier sehen Sie alle installierten Features, die das Tool gefunden hat. In der Datei *FeatureProblems.txt* finden Sie die Probleme aufgelistet, die das Tool gefunden hat.

Lassen sich Features nicht mit Stsadm deaktivieren, verwenden Sie das Tool WssRemoveFeatureFromSite von der Seite *http://code.msdn.microsoft.com/WssRemoveFeatureFrom*. Die Syntax für den Befehl lautet:

```
WssRemoveFeatureFromSite –scope (Website|Websitesammlung) –url <URL der Seite> –featureid
<ID des Features> –force
```

Ein weiteres Tool in diesem Bereich ist das SharePoint Feature Administration and Clean Up Tool. Dieses Programm laden Sie von der Seite *http://featureadmin.codeplex.com*. Das Tool kann über eine grafische Oberfläche fehlerhafte Features finden und diese aus dem System entfernen.

Sie müssen auch dieses Tool nicht installieren, sondern können es einfach starten. Über die Schaltfläche *Load* lädt das Tool alle Features der ausgewählten Site und Sie können die Features verwalten, testen, aktivieren oder löschen.

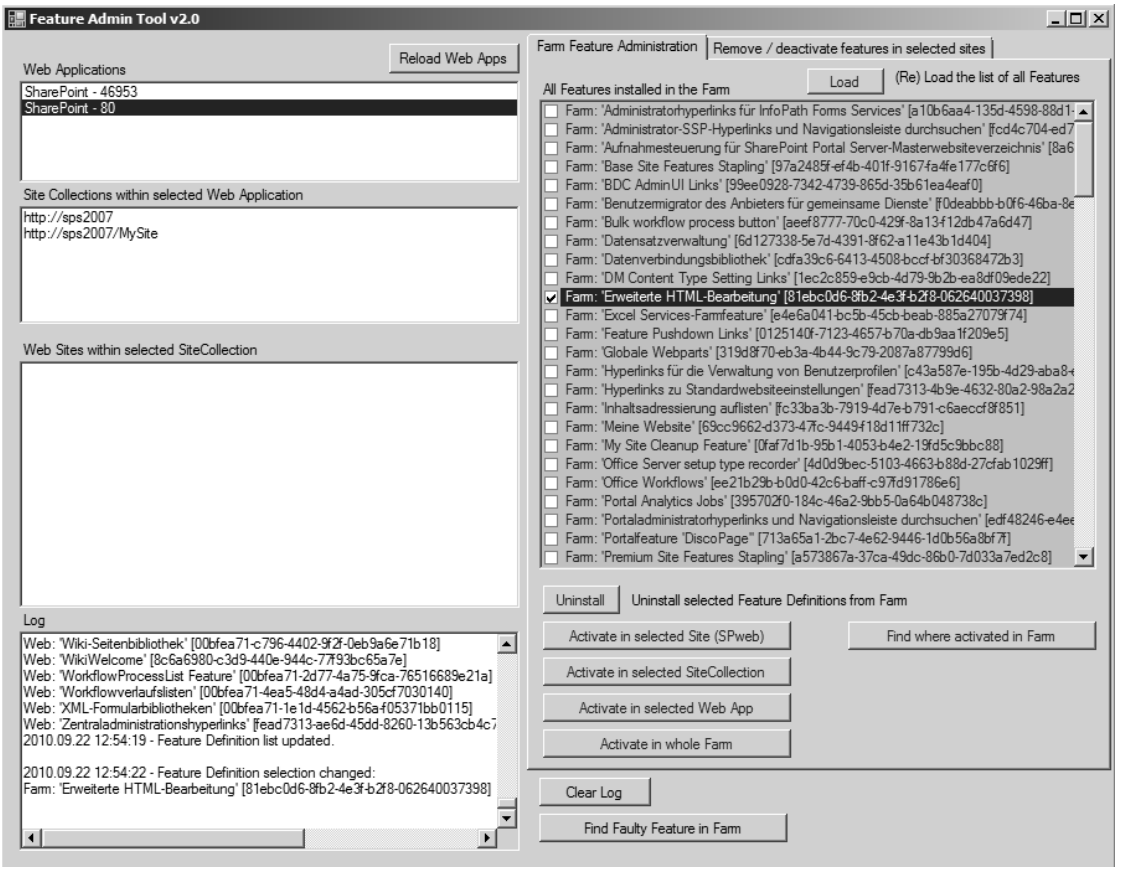

Abbildung 4.22 Verwalten der Features in SharePoint 2007 mit dem Feature Admin Tool

Klicken Sie auf die Schaltfläche *Find Faulty Feature in Farm*, zeigt das Tool Features in der Farm an, die Probleme bereiten. Sind alle Features in Ordnung, erhalten Sie eine entsprechende Meldung.

Ein weiteres wertvolles Tool in diesem Bereich ist der ebenfalls kostenlose SharePoint Manager 2007 von der Seite *http://spm.codeplex.com/releases/view/22762*. Das Tool gibt es zusätzlich als SharePoint Manager 2010. Auch dieses Tool müssen Sie nicht installieren. Sie können mit dem SharePoint Manager 2007 (wie bei der SharePoint-Zentraladministration) alle Einstellungen am Server vornehmen.

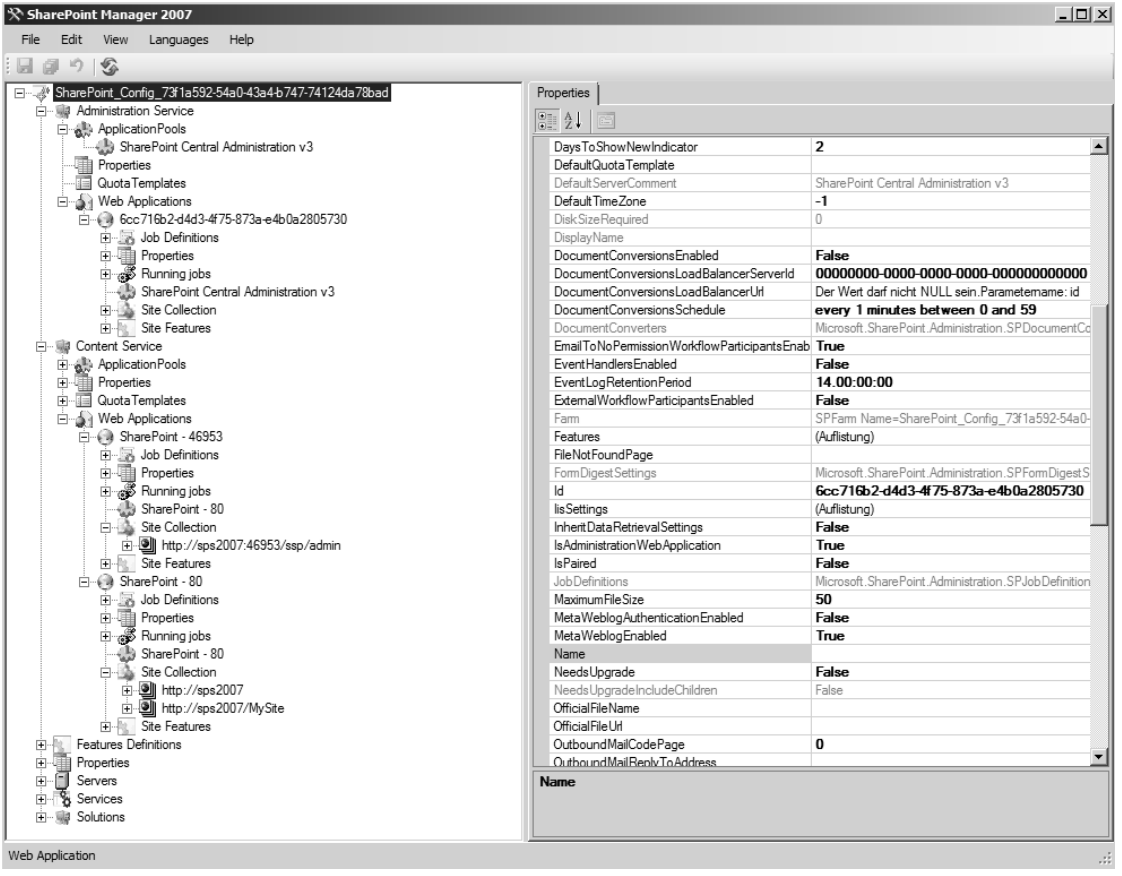

Abbildung 4.23 SharePoint mit Zusatztools verwalten

Sie können mit dem Tool alle Server der Farm verwalten und an zentraler Stelle alle Einstellungen, die eine Migration verhindern könnten, noch mal überprüfen.

Ein weiteres wichtiges Tool für die Analyse vor der Migration ist Bamboo SharePoint Analyzer von der Seite *http://community.bamboosolutions.com/blogs/bambooteamblog/archive/2008/11/07/introducing-bamboo-sharepoint-analyzer.aspx*. Das Freewaretool kann SharePoint ebenfalls zuverlässig analysieren.

Zusätzlich sollten Sie auf den SharePoint-Servern noch *stsadm –o enumallwebs* ausführen. Sie erhalten mit dem Befehl eine Auflistung aller Websites, die Sie bei der Migration berücksichtigen müssen. Außerdem sehen Sie so die IDs der Seiten sowie die Vorlagen, auf welche die Seiten aufbauen. Mit dem Aufruf von *stsadm –o enumallwebs >c:\webs.txt* lassen Sie die Ausgabe in eine Textdatei umleiten.

Außerdem sollten Sie das SharePoint Administration Toolkit für SharePoint Server 2007 herunterladen und installieren. Dieses Toolkit enthält ebenfalls Diagnoseprogramme für SharePoint Server 2007. Mehr dazu finden Sie auf der folgenden Seite:

http://blogs.msdn.com/sharepoint/archive/2009/08/27/announcing-the-fourth-release-of-the-microsoft-sharepoint-administration-toolkit.aspx

Sie benötigen das SharePoint Diagnostics Tool aus dem Administration-Toolkit vor allem dann, wenn Sie selbst programmierte Anwendungen und Lösungen auf den Websites suchen wollen.

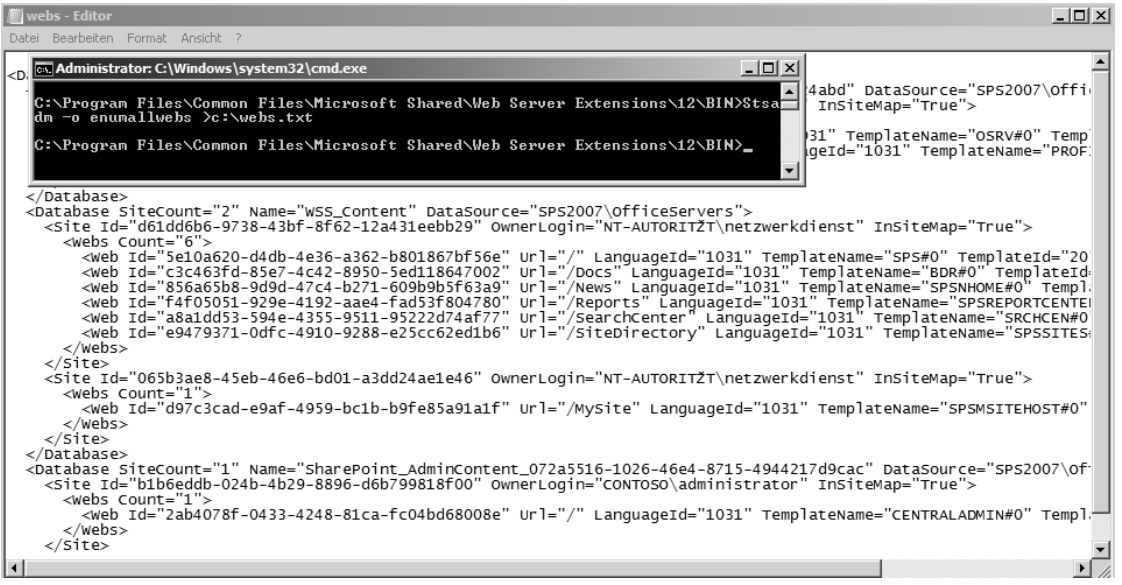

Abbildung 4.24 Anzeigen der Daten einer Serverfarm mit Stsadm

Bevor Sie eine Migration starten, sollten Sie die alte Farm von alten Daten und Fehlern befreien, damit Sie Altlasten vermeiden. Verwaiste Seiten, Listen und andere Objekte entfernen Sie mit dem Befehl *stsadm –o databaserepair*. Die Syntax des Befehls lautet:

```
stsadm –o databaserepair –url <URL der Websitesammlung> –databasename <Datenbank> [–
deletecorruption]
```

Häufig erhalten Sie auch Fehler angezeigt, wenn SharePoint Sitedefinitionen nicht finden kann, weil entsprechende Sprachpakete fehlen. In diesem Fall ist es hilfreich, wenn Sie die Sprachpakete für Windows SharePoint Services 3.0 oder SharePoint Server 2007 erneut installieren. Die Sprachpakete enthalten auch meist die fehlenden Sitedefinitionen, und die Installation ändert keine Daten. Sie finden die Sprachpakete auf den folgenden Seiten:

- **Windows SharePoint Services 3.0 Language Pack** *http://www.microsoft.com/downloads/en/details.aspx?FamilyId=36EE1BF0-652C-4E38-B247-F29B3EEFA048&displaylang=en*
- **Windows SharePoint Services 3.0 Language Pack Service Pack 2** *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=085e5ac8-58f6-4cf9-8012-33b95ee36c0f&displaylang=en*
- **2007 Office System Language Packs for SharePoint Server 2007, Forms Server 2007, Project Server 2007, and SharePoint Server 2007 for Search** *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=2447426b-8689-4768-bff0-cbb511599a45&DisplayLang=en*

- **The 2007 Microsoft Office Servers Language Pack Service Pack 2** *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=01c6a3e8-e110-4956-903a-ad16284bf223&displaylang=en*

SharePoint Designer 2010

Neben der Zentraladministration und der SharePoint 2010-Verwaltungsshell können Sie SharePoint Server 2010 und SharePoint Foundation 2010 auch mit dem kostenlosen SharePoint Designer 2010 verwalten, den Sie im Downloadcenter von Microsoft als 32-Bit- oder als 64-Bit-Version herunterladen können.

SharePoint Designer 2010 dient nicht nur zum Anpassen des Designs von Websites, sondern Sie verwalten mit diesem Werkzeug auch Systemeinstellungen der verschiedenen SharePoint-Bereiche.

Sie finden SharePoint Designer 2010 auf den folgenden Webseiten:

- **32-Bit-Version** *http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=D88A1505-849B-4587-B854-A7054EE28D66*
- **64-Bit-Version** *http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=566D3F55-77A5-4298-BB9C-F55F096B125D*

Mit SharePoint Designer 2010 können Sie auch ohne Programmierkenntnisse SharePoint verwalten, Berechtigungen und Designs ändern sowie Workflows erstellen.

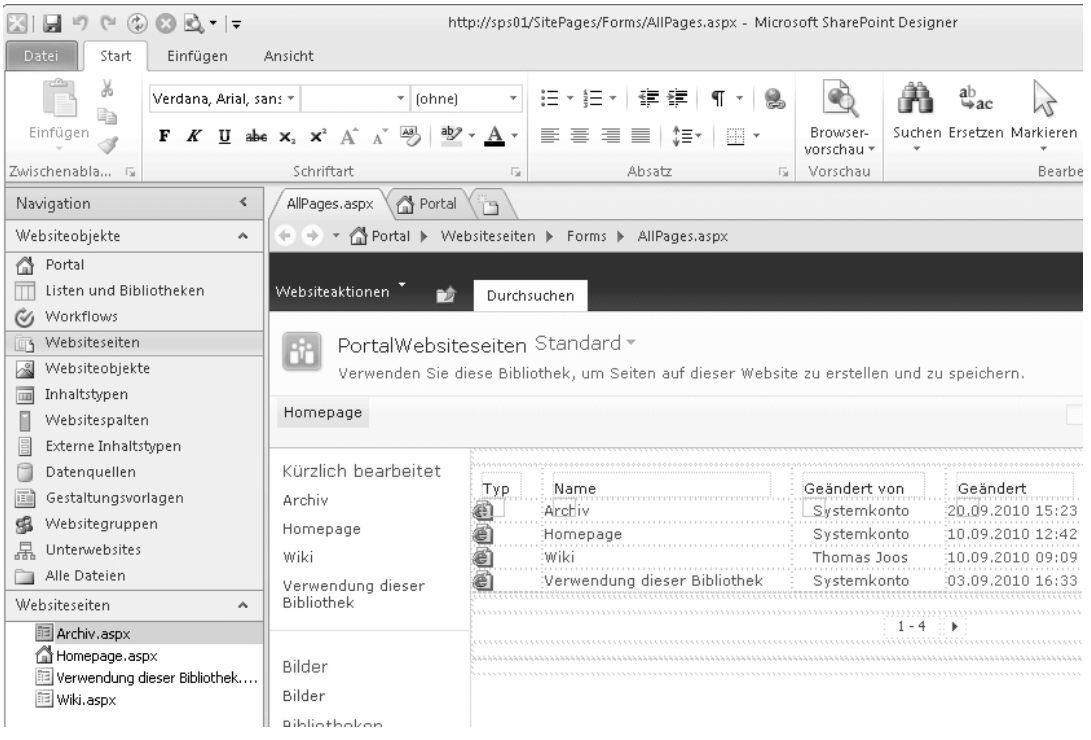

Abbildung 4.25 SharePoint 2010 mit dem kostenlosen SharePoint Designer verwalten

Daten über Dateifreigaben zu SharePoint übernehmen – FciSharePointUpload.ps1

Neben der Vorbereitung der Serverfarm und Bibliotheken ist es in vielen Fällen notwendig, dass Administratoren große Mengen an Dokumenten in die SharePoint-Bibliotheken von den Netzwerkfreigaben übernehmen müssen. Bei dieser Aufgabe besteht die Möglichkeit, die Daten einzeln zu übernehmen oder zu automatisieren. SharePoint 2010 bietet für Bibliotheken auch die Möglichkeit, mehrere Dateien auf einmal hochzuladen.

Zusätzlich lassen sich Bibliotheken in SharePoint 2010 auf den Clientcomputern oder Servern als Netzlaufwerk verbinden. Der Vorteil dabei ist, dass die Anwender auf die Daten in SharePoint zugreifen können, genauso wie über normale Dateiserver. Auch mehrere Dateien gleichzeitig lassen sich über diesen Weg in Bibliotheken kopieren, was vor allem bei Migrationen sehr hilfreich ist. Der Verbindungsaufbau findet dazu mit WebDAV (Web-based Distributed Authoring and Versioning) statt.

Der Verbindungsaufbau auf den Clients mit Windows 7 ist denkbar einfach: Sie verbinden ein neues Netzlaufwerk und geben als Adresse *http://<Servername>/<Bibliothek>* an, zum Beispiel *http://companyweb/einkauf*.

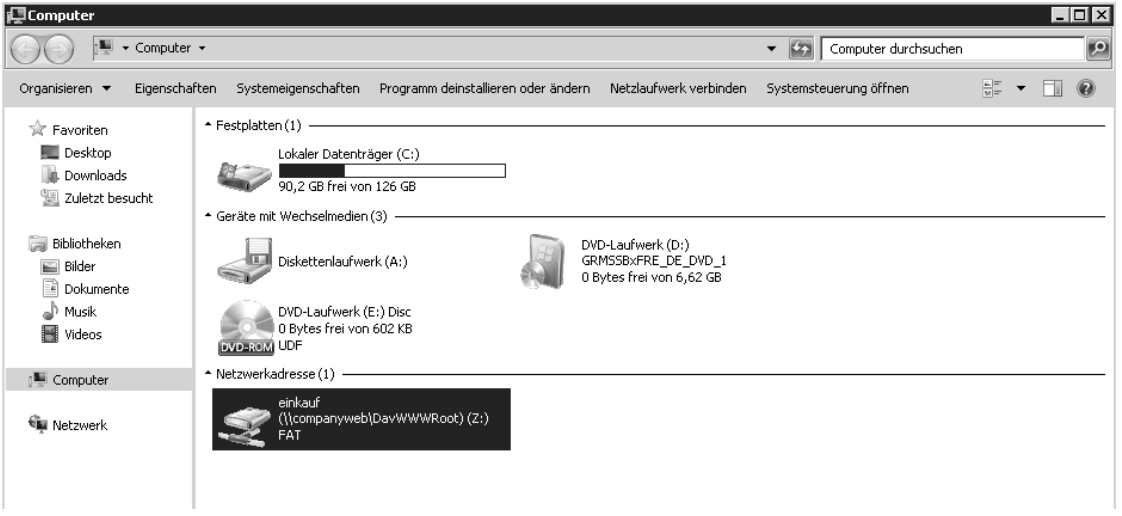

Abbildung 4.26 Bibliotheken aus dem Companyweb lassen sich auch als Netzlaufwerke verbinden

Nach der Verbindung sehen Sie die Bibliothek und alle Dateien im Windows-Explorer. Der Umgang entspricht dem Zugriff auf herkömmliche Dateifreigaben. Das heißt, Sie können Daten von Dateiservern sehr schnell kopieren. Die kopierten Dateien sind dann ebenfalls in der Bibliothek verfügbar. Neben der grafischen Oberfläche können Sie die Verbindung auch mit *net use* herstellen lassen, zum Beispiel über Anmeldeskripts. Die Syntax dazu ist:

```
net use <Buchstabe> "http://companyweb/Bibliothek>" /User:<Domäne><Benutzername>
<Kennwort>
```

Der Verbindungsaufbau über WebDAV erfolgt durch den Dienst *WebClient Service*. Dieser ist standardmäßig in Windows XP, Windows Vista sowie Windows 7 enthalten und gestartet, aber in Windows Server 2008 und Windows Server 2008 R2 nicht installiert. Aus diesem Grund können Sie auf Servern standardmäßig nicht mit WebDAV arbeiten. Sie haben aber die Möglichkeit, über den Server-Manager das Feature *Desktopdarstellung* zu installieren. Dieses enthält auch den WebClient Service. Nach der Installation können Sie auch in Windows Server 2008 und Windows Server 2008 R2 mit Netzlaufwerken und SharePoint-Bibliotheken arbeiten.

Sollte auch nach der Installation des Features der Verbindungsaufbau nicht funktionieren, starten Sie den Systemdienst *WebClient* neu. Der Verbindungsaufbau mit WebDAV ist in vielen Umgebungen sehr langsam. Meist lässt sich das Problem beheben, indem Sie das Kontrollkästchen *Automatische Suche der Einstellungen* im Internet Explorer deaktivieren. Sie finden diese Einstellung in den Internetoptionen auf der Registerkarte *Verbindungen* über die Schaltfläche *LAN-Einstellungen*. Außerdem sollten Sie dafür sorgen, dass die SharePoint-Server zur Intranetzone gehören. Diese Einstellung finden Sie auf der Registerkarte *Sicherheit*. Sie sehen die Zuordnung im unteren Bereich des Internet Explorers, wenn Sie die Bibliothek aufrufen. Achten Sie auch darauf, dass die Ports 137,138,139 und 445 zwischen Client und Server verfügbar sind.

Arbeiten Sie mit SSL, muss noch der Port 443 offen sein. Haben Sie Webanwendungen mit anderen Ports konfiguriert, müssen Sie auch diese öffnen. Sie können für die Datenübernahme auch direkt *Companyweb* als Netzlaufwerk verbinden und mit dem Explorer Dokumente kopieren.

Microsoft bietet ein kostenloses Skript zum Upload von Dokumenten an. Sie finden das PowerShell-Skript auf der Seite *http://gallery.technet.microsoft.com/ScriptCenter/en-us/f538c34c-4f74-4645-9649-fd25e49805d6*. Das Skript hat allerdings den Nachteil, ziemlich komplex zu sein, da sich Administratoren zum einen mit den neuen Dateiklassifizierungsdiensten in Windows Server 2008 R2 auseinandersetzen müssen, zum anderen mit der PowerShell und den Rechten im Dateisystem und in SharePoint. Das Skript funktioniert ausschließlich nur mit Windows Server 2008 R2 und SharePoint 2010.

Für den Upload verwendet das PowerShell-Skript Metadaten, die Sie über die Dateiklassifizierungsdienste für Freigaben beziehungsweise als Dateiverwaltungsaufgaben (einem Teil der Dateiklassifizierungsdienste) definiert haben. Das Produkt ist eigentlich für SharePoint Server 2007 gedacht, funktioniert aber mit Einschränkungen auch in SharePoint Server 2010. Damit Sie Daten von einem Server über das Skript in SharePoint-Bibliotheken übernehmen können, müssen Sie den Ressourcen-Manager für Dateiserver auf dem Server nutzen. Dieser ist standardmäßig aktiviert. Außerdem muss die Bibliothek, in die Sie Daten übernehmen wollen, vorher angelegt sein, und der Benutzer, mit dem Sie Dokumente hochladen, muss das Recht für den Upload in der Bibliothek erhalten.

Zusätzlich bietet es sich an, für das Skript nicht direkt die PowerShell zu verwenden, sondern die Skriptumgebung PowerShell ISE. Diese müssen Sie als Feature über den Server-Manager installieren. Um das Skript zu testen, kopieren Sie am besten den Inhalt von der oben genannten Skriptseite in eine neue Textdatei, die Sie mit dem Editor erstellt haben. Markieren Sie alles ab den Kommentaren, die mit # gekennzeichnet sind. Benennen Sie die Datei anschließend um in

FciSharePointUpload.ps1 und kopieren Sie diese auf den Server, auf dem Sie den Upload testen wollen.

Bevor Sie den Upload eines ganzen Ordners durchführen, sollten Sie in der PowerShell oder der PowerShell-ISE zunächst eine Datei hochladen, um Fehler zu vermeiden. Die Syntax eines solchen Befehls ist zum Beispiel:

```
c:\windows\FciSharePointUpload.ps1 –file "c:\vertrieb\auftrag.vsd" –url "http://sps01" –
libPath "Vertrieb" –sourceAction url –user contoso\administrator –password hallohallo
```

Sie müssen den kompletten Pfad zur *.ps1*-Datei angeben. Haben Sie die Befehle von der Seite korrekt eingeben und kann der Befehl auf die lokale Datei sowie die Bibliothek zugreifen, sollte sich die Datei nach wenigen Sekunden in der Bibliothek befinden. Im Quellordner legt das Skript automatisch eine Verknüpfung zur Datei in der Bibliothek an. Das heißt, sobald ein Anwender diese Datei anklickt, öffnet sie sich in der Bibliothek. Dieses Verhalten können Sie mit der Option *–sourceAction* steuern. Die einzelnen Werte und verschiedenen Optionen finden Sie auf der Downloadseite des Skripts.

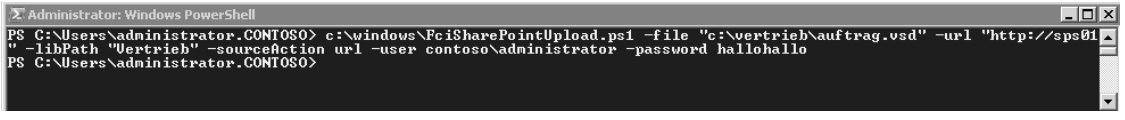

Abbildung 4.27 Hochladen von Dokumenten mit der PowerShell

Wollen Sie den Benutzernamen und das Kennwort nicht in den Befehl mit aufnehmen, können Sie hier mit einer Variablen arbeiten. Geben Sie *$auth = Get-Credential* ein, erscheint ein Authentifizierungsfenster. Hier geben Sie die Daten des Benutzers ein, mit dem sich das Skript mit der Bibliothek und dem Ordner verbinden soll. Um die Daten aus der Variablen zu verwenden, geben Sie anschließend beispielsweise den folgenden Befehl ein:

```
c:\windows\FciSharePointUpload.ps1 –file "c:\vertrieb\kunden.docx" –url "http://
companyweb" –libPath "Vertrieb" –sourceAction url –user $auth
```

Auf diese Weise können Sie mit allen Cmdlets der PowerShell arbeiten, die eine Authentifizierung benötigen. Sie müssen bei der Ausführung des PowerShell-Skripts darauf achten, wie die Sicherheitsrichtlinie der PowerShell auf dem Server eingestellt ist. Standardmäßig blockiert die Windows PowerShell nicht signierte Skripts über die Ausführungsrichtlinie.

Sie können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. Die Ausführungsrichtlinie speichert ihre Daten in der Windows-Registrierung, Sie müssen diese also nur einmal anpassen. Sie können folgende Einstellungen vornehmen:

- **Restricted** Standardeinstellung, keine Skripts erlaubt, SharePoint-Skripts funktionieren nicht

- **AllSigned** Nur signierte Skripts sind erlaubt. Auch hier funktionieren keine SharePoint-Skripts, da diese nicht signiert sind.
- **RemoteSigned** Bei dieser Einstellung müssen Sie Skripts für eine Zertifizierungsstelle signieren
- **Unrestricted** Mit dieser Einstellung funktionieren auch die SharePoint-Skripts

Nach der Eingabe von *Set-ExecutionPolicy unrestricted* müssen Sie die Ausführung noch bestätigen. Neben dem manuellen Upload einer Datei können Sie jetzt diese Aufgabe mit dem Skript automatisieren. Dazu benötigen Sie die Dateiklassifizierungsdienste des Ressourcen-Managers für Dateiserver. Klicken Sie mit der rechten Maustaste auf *Dateiverwaltungsaufgaben* und wählen Sie im Kontextmenü den Eintrag *Dateiverwaltungsaufgabe erstellen* aus. Weisen Sie der Aufgabe einen Namen und eine Beschreibung zu. Im unteren Teil des Fensters wählen Sie bei *Bereich* den Ordner aus, dessen Dateien Sie in SharePoint hochladen wollen.

Auf der Registerkarte *Aktion* aktivieren Sie den Typ *Benutzerdefiniert*. Im Bereich *Ausführbare Datei* verwenden Sie den Befehl *C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*. In der Zeile *Argumente* tragen Sie die entsprechende Zeile ein, welche das Skript startet, mit dem die Dateiverwaltungsaufgabe die Dateien des ausgewählten Ordners in die entsprechende Bibliothek hochlädt. Zum Beispiel:

```
–noninteractive –file c:\windows\FciSharePointUpload.ps1 –file "[Source File Path]" –url
"http://companyweb" –libPath "Vertrieb" –sourceAction url –user contoso\administrator –
password hallohallo
```

Die Option *"[Source File Path]"* sorgt dafür, dass die Dateiverwaltungsaufgabe die Datei hochlädt, die aktuell bearbeitet wird. Diese Variable versteht aber nur der Ressourcen-Manager für Dateiserver, Sie können die Option nicht in einer normalen PowerShell verwenden. Achten Sie auf die Anführungszeichen. Im Bereich *Befehlssicherheit* wählen Sie *Lokales System* aus.

Auf der Registerkarte *Bedingung* können Sie noch weitere Bedingungen hinterlegen, wie Windows die Datei ausfiltern soll, zum Beispiel auf Basis von Metadaten, die Sie wiederum vorher mit den Dateiklassifizierungsdiensten festgelegt haben. Über die Registerkarte *Zeitplan* legen Sie fest, wann der Befehl starten soll. Nachdem Sie die Aufgabe erstellt haben, können Sie diese über das Kontextmenü starten lassen. Auf der Downloadseite für das Skript erhalten Sie weiterführende Informationen zu allen Optionen.

Überprüfen Sie, ob die Aufgabe alle Dateien findet und diese hochlädt. Leider funktioniert das Skript nicht immer zuverlässig, was sich darin äußert, dass die Dateiverwaltungsaufgabe keine Dateien hochlädt. Hier erhalten Sie Hilfe auf der Downloadseite und den hinterlegten Links zum Scripting-Forum.

Da die Übernahme von Dokumenten ein komplizierter Vorgang sein kann, sollten Administratoren entweder manuell Daten übernehmen, Skripts verwenden, wie vorher besprochen, oder besser auf Tools setzen, die bei der Migration helfen. Für die meisten Tools stellen die Unternehmen umfassende Hilfen sowie Webcasts und Demovideos zur Verfügung.

SharePoint Manager 2010

Administratoren, die SharePoint Server 2010 verwalten müssen, sollten sich auch die Open-Source-Lösung SharePoint Manager 2010 von der Seite *http://spm.codeplex.com/releases/view/35932* ansehen.

Mit dem Tool können Sie die komplette Farm und alle beteiligten Server in einer grafischen Oberfläche verwalten und finden alle Einstellungen auf einen Blick. Das Tool greift direkt auf die Einstellungen in der Konfigurationsdatenbank zu. Änderungen, die Sie im Tool vornehmen, sind sofort in der Konfigurationsdatenbank verfügbar.

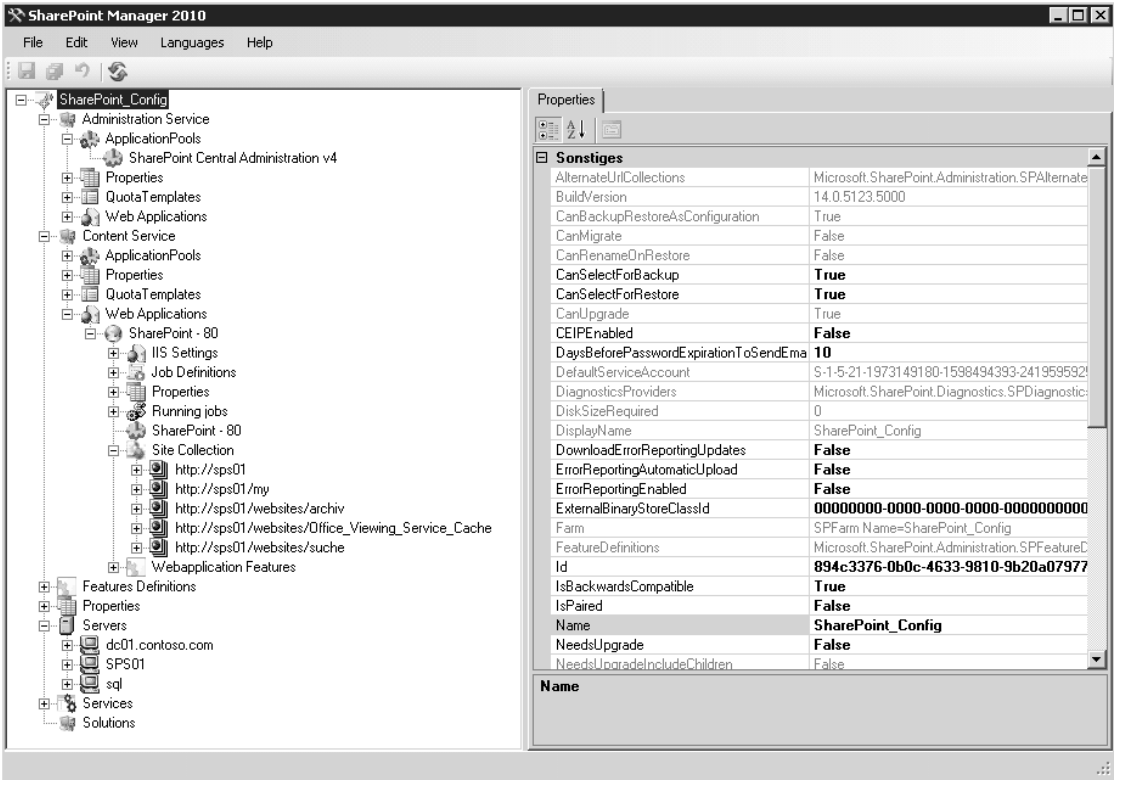

Abbildung 4.28 SharePoint-Verwaltung mit dem kostenlosen SharePoint Manager 2010

Lasttests und Server-Hardening – SharePoint 2010 Administration Toolkit

Vor allem bei Messungen der Leistung und der Planung von SharePoint-Servern hilft das kostenlose SharePoint 2010 Administration Toolkit. Dieses besteht aus mehreren Tools, die Administratoren bei der Planung und Leistungsmessung unterstützen. Wir gehen in den nächsten

Abschnitten ausführlicher auf die verschiedenen Werkzeuge ein. Das Toolkit besteht aus den folgenden Komponenten:

- Das *Load Testing Kit* führt Lasttests aus
- Das *Manifest des Sicherheitskonfigurations-Assistenten* fügt SharePoint zum Sicherheitskonfigurations-Assistenten (SCW) von Windows Server 2008 x64 SP2 oder Windows Server 2008 R2 hinzu
- Mit dem *Benutzerprofilreplikations-Modul* können Administratoren Benutzerprofile und Daten in die Benutzerprofil-Dienstanwendung in SharePoint Server 2010 replizieren
- Der CMIS-Connector (*Content Management Interoperability Services*) für Microsoft SharePoint Server 2010 ermöglicht SharePoint-Benutzern, auf Datenquellen zuzugreifen, die mit dem CMIS-Standard an SharePoint angebunden sind. Zur Verbindung steht ein neues Webpart zur Verfügung, das Sie in SharePoint-Seiten einbinden und mit dem Anwender arbeiten können.

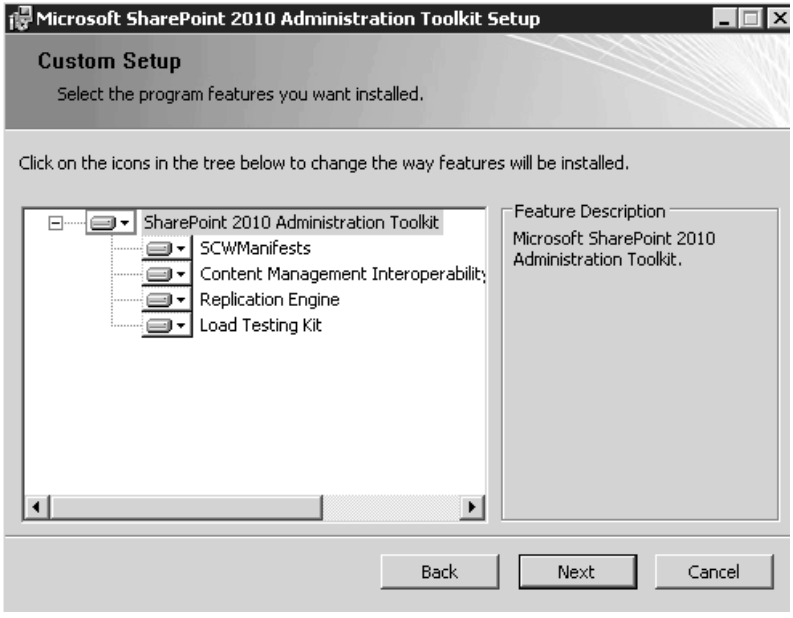

Abbildung 4.29 Installieren des SharePoint 2010 Administration Toolkit

Sie können das gesamte Toolkit oder jeweils nur einzelne Tools installieren. Wollen Sie eine skriptbasierte Installation durchführen, extrahieren Sie das Toolkit mit dem Befehl:

```
SharePoint2010AdministrationToolkit.exe /extract:<Pfad>
```

Sie können das Toolkit von der Seite *http://go.microsoft.com/fwlink/?linkid=196866&clcid=0x407* herunterladen.

Windows Server Solutions Best Practices Analyzer 1.0

Mit dem kostenlosen Windows Server Solutions Best Practices Analyzer (WSSBPA) 1.0 können Sie eine Installation von SBS 2011 grundlegend testen. Das Tool verwendet dazu von den SBS-Entwicklern vorgegebene Regeln und kann auch versteckte Probleme und Fehlerursachen erkennen und diagnostizieren.

Laden Sie das Tool von der Seite *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d40dcc5b-8f97-49e2-ae79-9c7a7a69dec4* herunter. Setzen Sie die Vorgängerversion mit der Bezeichnung Small Business Server 2011 Best Practices Analyzer ein, müssen Sie diesen vor der Installation des WSSBPA zunächst deinstallieren. Bevor Sie den BPA installieren können, benötigen Sie aber noch Microsoft Baseline Configuration Analyzer 2.0 von der Seite *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1B6E9026-F505-403E-84C3-A5DEA704EC67*. Dieses Tool müssen Sie – wie erwähnt – vor dem BPA installieren.

Installieren Sie am besten beide Tools auf dem SBS-Server und starten anschließend den BPA. Sie können während der Installation des BPA festlegen, dass der Server auch über das Netzwerk scanbar ist, wenn Sie den BPA zusätzlich auf einer Arbeitsstation installieren, die sich in der SBS-Domäne befindet. Zusätzlich können Sie die Ergebnisberichte des BPA in die Windows SBS-Konsole integrieren lassen. Dadurch scannt der BPA regelmäßig den Server auf Fehler und zeigt diese an. Da dadurch der Server nicht belastet wird, Sie aber immer eine Übersicht über die aktuelle Konfiguration haben, ist dies durchaus zu empfehlen.

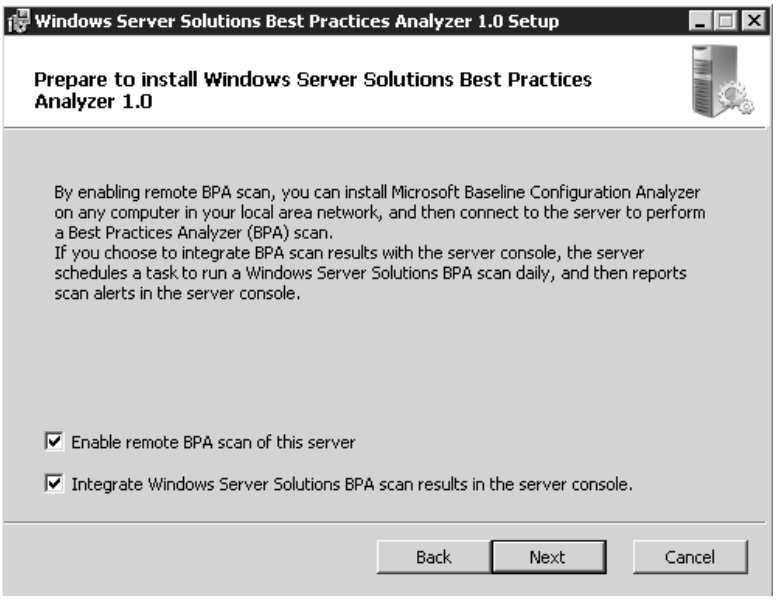

Abbildung 4.30 Installieren von Windows Server Solutions Best Practices Analyzer 1.0

Nach dem Start des Tools wählen Sie bei *Select a product* zunächst *Windows Server Solutions Best Practices 1.0* aus. Klicken Sie anschließend auf *Start Scan*. Daraufhin überprüft BPA die Installation des Servers.

Nach dem Scan sehen Sie das Ergebnis und können bei mehreren Meldungen diese sortieren. Beheben Sie alle Fehler, die der BPA während des Vorgangs findet. Auf der Startseite des Tools können Sie den Bericht des vorherigen Scanvorgangs noch mal aufrufen.

Zusatztools für das Forefront Threat Management Gateway 2010

Microsoft bietet auf der Seite *http://www.microsoft.com/downloads/details.aspx?FamilyID=01B2F7A5-8165-4EAD-9693-994504F66449&displayLang=en* das Forefront Threat Management Gateway 2010 Capacity Planning Tool an. Dieses hilft vor allem in größeren Umgebungen bei der Planung der Hardware, die für Forefront Threat Management Gateway (TMG) notwendig ist. Im Grunde genommen handelt es sich bei dem Tool um eine assistentengestützte Excel-Tabelle, die Sie bei der Planung unterstützt.

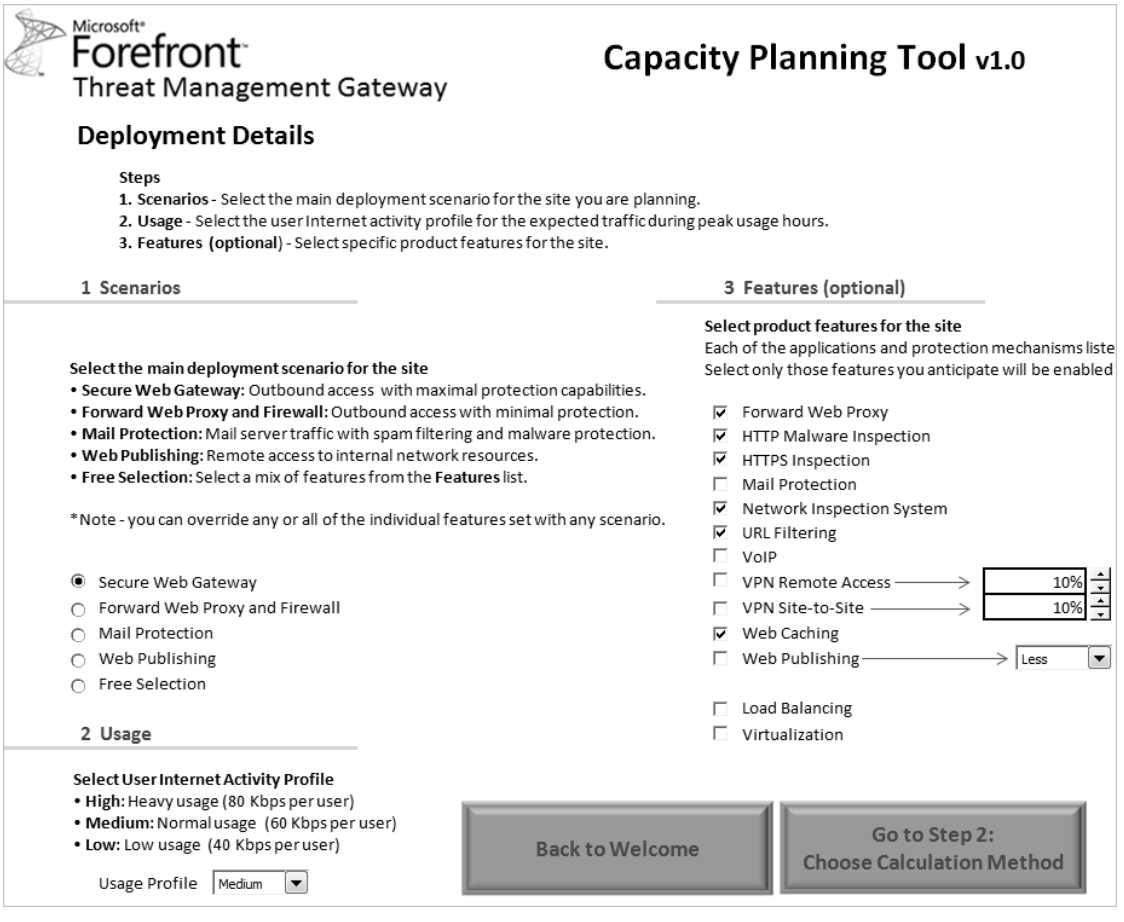

Abbildung 4.31 Kapazitätsplanung für TMG mit einer eigenen Excel-Tabelle

Microsoft Forefront Threat Management Gateway (TMG) 2010 Tools & Software Development Kit

Eine sehr wichtige Toolsammlung ist das Microsoft Forefront Threat Management Gateway (TMG) 2010 Tools & Software Development Kit von der Seite *http://www.microsoft.com/downloads/details.aspx?FamilyID=8809CFDA-2EE1-4E67-B993-6F9A20E08607&displayLang=en*. Hierbei handelt es sich um zahlreiche Zusatztools, die das Leben mit dem TMG erleichtern:

- **ADAM Sites Tool for Forefront TMG Enterprise Edition** Verwalten des zentralen Speichers eines TMG-Arrays
- **Auto Discovery Configuration Tool for Forefront TMG** Mit dem Auto-Discovery Configuration Tool (*AdConfigPack.exe*) können Sie in Active Directory ein Attribut setzen, welches auf den TMG-Server zeigt. Anwender, die den TMG-Client einsetzen (in ISA 2006 noch als Firewallclient bezeichnet), können Sie so automatisch mit TMG verbinden. Den TMG-Client laden Sie von der Seite *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=53010a09-3c5c-4d5d-9ae1-692e7447c5bd* herunter. Dieser funktioniert auch für ISA 2006
- **Cache Directory Tool for Forefront TMG** Mit dem Cache Directory Tool (*CacheDirPack.exe*) können Sie sich eine Echtzeitanzeige des Cacheinhalts anzeigen lassen sowie den Cache bearbeiten. Das Tool steht auch für ISA 2006 zur Verfügung.
- **CertTool for TMG** Das CertTool steuert die zertifikatbasierte Authentifizierung zwischen Array-Mitgliedern der Enterprise Edition von TMG 2010 und dem zentralen Konfigurationsspeicher
- **DNS Cache Tool for Forefront TMG** Das DNS Cache Tool (*DNSToolsPack.exe*) zeigt den aktuellen DNS-Cache auf dem Server an und erlaubt, einzelne Einträge zu löschen
- **EE Single Server Conversion Tool for Forefront TMG** EESingleServerConversion hilft bei der Migration eines alleinstehenden ISA-Servers (2004 und 2006) zu TMG 2010. Mit dem Tool lassen sich zum Beispiel die bereits vorhandenen Regeln übertragen.
- **MSDEToText Tool for Forefront TMG** MSDEToText konvertiert Forefront TMG SQL Server zu einer Textdatei
- **Remote Access Quarantine Tool for Forefront TMG (RQSUtils.exe)** Quarantänetool für VPN-Clients. Das Tool konfiguriert den TMG als RQS-Listener
- **RSA Test Authentication Utility for Forefront TMG** Mit dem RSA Test Authentication Utility (*SdTestPack.exe*) können Sie überprüfen, ob das TMG einen Computer authentifizieren kann, der RSA Authentication Manager nutzt
- **Security Configuration Wizard (SCW) Update for Forefront TMG Standard Edition and Enterprise Edition** Forefront TMG Security Configuration Wizard Update fügt TMG-Sicherheitseinstellungen zum Security Configuration Wizard (SCW) hinzu

Microsoft Forefront Threat Management Gateway Best Practices Analyzer Tool

Wie für Exchange gibt es auch für den ISA/TMG ein kostenloses Analysetool von Microsoft, das die Installation und Konfiguration eines ISA/TMGs überprüfen kann. Der TMG BPA analysiert dabei auf Basis der Konfigurationsdaten, ob ein TMG fehlerfrei installiert wurde, und gibt im Bedarfsfall entsprechende Meldungen aus.

Laden Sie sich das Tool auf der Internetseite *http://www.microsoft.com/downloads/details.aspx?FamilyID=8AA01CB0-DA96-46D9-A50A-B245E47E6B8B&displaylang=en* von Microsoft herunter und führen Sie die Installation auf dem TMG durch. Nach der Installation des Tools finden Sie den TMG BPA in der Programmgruppe *Microsoft Forefront TMG/TMG-Tools*.

Haben Sie das Programm gestartet, können Sie mit dem Link *Start a Scan* eine erste Überprüfung des ISA/TMGs durchführen, nachdem das Tool notwendige Aktualisierungen bei Microsoft heruntergeladen hat. Wählen Sie beim Starten *HealthCheck* aus. Nachdem Sie dem Scanvorgang einen Namen gegeben und einen Domänencontroller konfiguriert haben, starten Sie mit *Start scanning* einen Scanvorgang.

Microsoft veröffentlicht in regelmäßigen Abständen Aktualisierungen für die TMG-Konfiguration. Diese Aktualisierungen können beim Starten des BPA automatisch von heruntergeladen und integriert werden. Dadurch ist sichergestellt, dass die Analyse eines installierten TMGs immer auf der aktuellsten Basis erfolgt. Es gibt sicherlich keine schnellere Möglichkeit, TMG auf Herz und Nieren zu prüfen, als den TMG-BPA. Experimentieren Sie mit diesem Tool und lesen Sie sich die ausführliche Hilfedatei durch. Normalerweise reicht der *HealthCheck* aus, um Ihnen einen Überblick über die Verbesserungsmöglichkeiten der Installation zu gewähren. Der Test prüft TMG auf Herz und Nieren und gibt Ihnen entsprechende Hilfen und Fehlerbehebungsmaßnahmen.

Gehen Sie allen Meldungen nach und stellen Sie sicher, dass Ihnen keine schwerwiegenden Fehler in der Konfiguration unterlaufen sind. Klicken Sie auf den Menüpunkt *Start BPA2Visio*, kann der BPA die Konfiguration von TMG auslesen und automatisch eine Visio-Zeichnung der Konfiguration erstellen. Dazu muss auf dem Rechner, auf dem Sie den TMG-BPA starten, Microsoft Visio 2003/2007/2010 installiert sein. Anschließend öffnet sich automatisch Visio mit der erstellten Zeichnung.

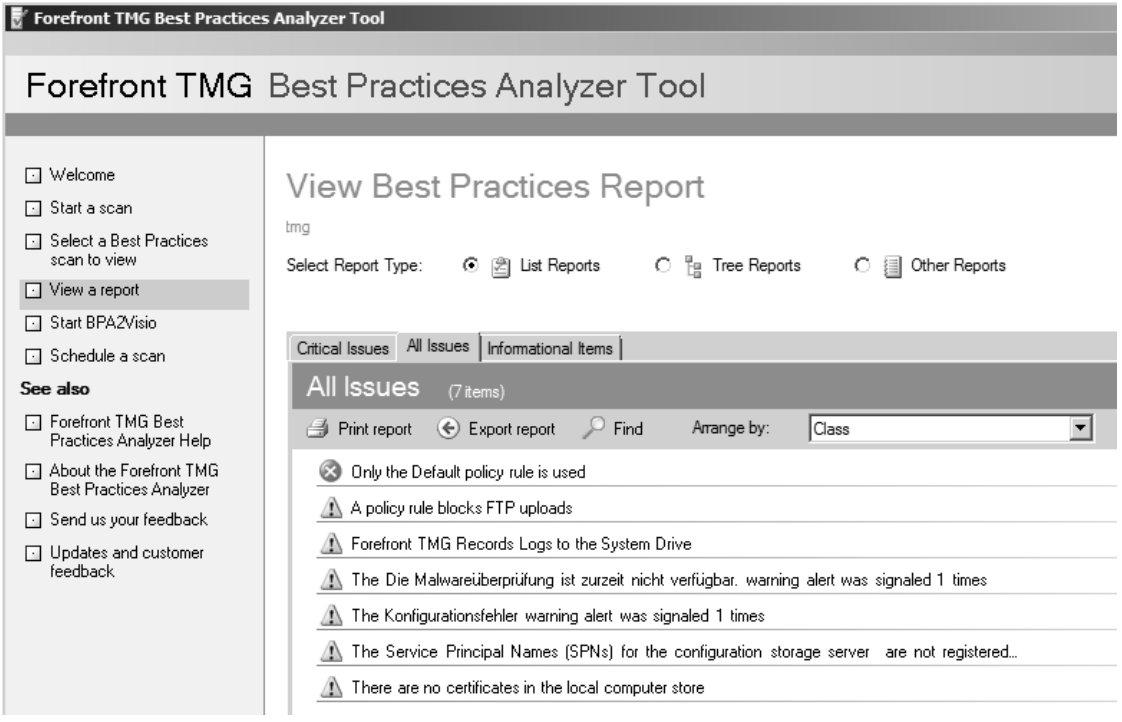

Abbildung 4.32 Anzeigen des Analyseergebnisses der TMG-Installation