Kapitel 9

Sicherung und Wiederherstellung

In diesem Kapitel:

Sicherungen gehören zu den elementaren Aufgaben eines Administrators, solange ich denken kann. Das ist schon ein ziemlich langer Zeitraum, aber tatsächlich gibt es Sicherungen schon sehr viel länger. Auf jedem Computersystem können defekte Festplatten, Serverausfälle, Irrtümer bei der Verwaltung, Softwarebugs, Hardwarefehler und andere Störungen zu Datenverlusten führen. Angesichts dieser Gefahr benötigen Sie Sicherungen, um das beruhigende Gefühl genießen zu können, die verlorenen Daten wiederherstellen zu können, ohne in Schweiß auszubrechen. Die Einführung von Datenbankverfügbarkeitsgruppen und anderen Neuentwicklungen in Exchange Server 2010 erweitert die Palette der Aspekte, die Sie berücksichtigen müssen, wenn Sie ein Sicherungsverfahren aufstellen. Vielleicht gelangen wir eines Tages an einen Punkt, an dem Sicherungen nicht mehr so wichtig sind, wie sie einst waren, vielleicht führen wir Sicherungen irgendwann auf eine andere Art und Weise durch. Außerdem müssen Sie sich über die Wiederherstellung Gedanken machen. Da es bei diesem Thema viel zu besprechen gibt, wollen wir gleich anfangen.

Eine wichtige Grundsatzfrage

Wenn Datenbankverfügbarkeitsgruppen so funktionieren, wie Microsoft es erwartet, und eine stabile Hochverfügbarkeitsumgebung für Exchange schaffen, dann können wir theoretisch die herkömmlichen Ansichten über Sicherung und Wiederherstellung, die seit den ersten Versionen von Exchange vorherrschten, über Bord werfen. Mit Sicherungen haben sich Administratoren vor den Auswirkungen von logischen und physischen Beschädigungen der Datenbanken geschützt, da sie das System damit in den Zustand an einem bestimmten Zeitpunkt zurückversetzen oder Daten wiedergewinnen konnten, wenn einzelne Elemente in Postfächern oder ganze Postfächer versehentlich gelöscht worden waren. Doch Exchange Server 2010 schafft eine ganz neue Situation:

- Datenbanken können über viele Kopien verfügen, sodass ein Fehler auf einem Server die Datenbank nicht unzugänglich macht.
- Dank größerer Postfächer (durch replizierte Datenbanken vor Datenverlusten geschützt), der Aufbewahrung und der Wiederherstellung gelöschter Objekte können Benutzer in vielen Fällen versehentlich entfernte Elemente selbst wiederherstellen.
- Verzögerte Datenbankkopien bieten Schutz gegen die Folgen logischer Beschädigungen.

Die meisten Administratoren werden spontan antworten, dass Sicherungen funktionieren, sodass es keinen Grund gibt, etwas zu ändern. Das klingt vernünftig, aber bedenken Sie, dass Technologie einem ständigen Wandel unterliegt. Die Vorgehensweisen, die gestern angemessen und wirtschaftlich waren, müssen es heute nicht mehr zwangsläufig sein. Exchange Server 2010 ist die erste Version mit Replikation auf mehrere Kopien. Außerdem ist es dank der neuen E/A-Merkmale auch die erste Version, die einen wirkungsvollen Einsatz von SATA-Speicher möglich macht. Die Technik hat sich soweit entwickelt, dass sich auch erschwingliche Festplatten für die Speicherung von Daten eignen, und Netzwerkbandbreite ist billig genug, um eine Replikation über mehrere Standorte hinweg zu erlauben. Wir sind daher an einem Punkt angelangt, an dem wir unsere althergebrachten Verfahrensweisen überprüfen und uns fragen müssen, ob wir unsere Aufgaben nicht auf bessere Weise erfüllen können. Bei dieser Analyse müssen wir die folgenden Faktoren berücksichtigen:

- Die Anforderungen des Gesetzgebers und etwaiger Zertifizierungsprogramme, die Ihr Unternehmen bei der Aufbewahrung von Daten erfüllen muss.
- Die Kosten der Wiederherstellung von herkömmlichen Sicherungen im Vergleich mit dem Aufwand dafür, gelöschte Daten in einem erweiterten Papierkorb oder in Archivpostfächern aufzubewahren. In einer typischen Exchange Server 2007-Umgebung befindet sich die überwiegende

Mehrzahl der Daten in den aktiven Datenbanken und ein geringer Prozentsatz im Papierkorb. Da Sie jetzt sehr große Postfächer bereitstellen, gelöschte Elemente viele Wochen und sogar Monate lang im Papierkorb aufbewahren und Archivpostfächer nutzen können, die in die Clientoberfläche integriert sind, sollte es nicht mehr so häufig erforderlich sein, gelöschte oder offline aufbewahrte Daten wiederherzustellen.

- Die Kosten für die Wiederherstellung einer vollständigen Datenbank von Bandsicherungen (oder VSS-Snapshots oder Klonen) statt von einer passiven Kopie der Datenbank.
- Die Kosten für Bänder, Laufwerke und die interne und externe Aufbewahrung sowie die entsprechenden Kosten für die Aufbewahrung von VSS-Sicherungen. Hier müssen Sie sich u.a. fragen, wie viele Sicherungen Sie brauchen, welches Rotationsverfahren Sie einsetzen usw.
- Die Möglichkeit, Daten auch nach dem Ablauf eines normalen Sicherungszyklus noch zurückgewinnen zu können. Stellen Sie sich vor, in Ihrem Unternehmen wird wegen des Verdachts der sexuellen Nötigung ermittelt, und die Beweise befinden sich in Nachrichten, die sechs Monate zuvor gesendet wurden. Welche Maßnahmen sind erforderlich, um wieder an diese Daten zu kommen?
- Testen und Üben der Maßnahmen, die zur Wiederherstellung nach verschiedenen Arten von ausfällen erforderlich sind, von einem Speicherfehler, der nur eine Datenbank betrifft, bis zum Ausfall von Servern mit mehreren Datenbankkopien. Um die Geschäftsleitung davon zu überzeugen, dass eine Verfahrensänderung möglich ist, müssen Sie vor allen Dingen genau wissen, wie Sie schnell und effektiv den Betrieb wieder aufnehmen und Daten wiederherstellen können.

Brauchen wir noch herkömmliche Sicherungen?

Ist es weiterhin erforderlich, die herkömmlichen täglichen und wöchentlichen Sicherungen von Exchange-Daten ausführen, wenn es eine Datenbankverfügbarkeitsgruppe gibt und von allen wichtigen Postfachdatenbanken mehrere Kopien vorgehalten werden? Viele Unternehmen nehmen täglich vollständige Sicherungen vor, damit sie bei einem Ausfall keine inkrementellen Sicherungen wiederherstellen müssen, was den Wiederherstellungsvorgang vereinfacht. Um den Anforderungen von Zertifizierungsprogrammen zu genügen, werden die Sicherungsbänder gewöhnlich nach einigen Tagen an einen externen Lagerort gebracht, wo sie längere Zeit aufbewahrt werden können. Solche Sicherungszyklen gibt es schon seit den Tagen der ersten Mainframecomputer, doch in einer Zeit, in der die Daten auf mehrere Kopien repliziert werden, stellt sich die Frage, ob dies immer noch die sinnvollste Vorgehensweise ist, um kritische Daten zu schützen und eine Wiederherstellung nach einem katastrophalen Ausfall durchführen, die Datenbanken in den Zustand an einem bestimmten Zeitpunkt zurückversetzen, gesetzliche Anforderungen zur Beweissicherung erfüllen und Benutzerdaten wiedergewinnen zu können.

Aus rechtlichen oder anderen Gründen sind in einigen Umgebungen stets Sicherungen notwendig. Bei den anderen wird es interessant sein zu beobachten, wie sich das Sicherungsverfahren beim Einsatz von Datenbankverfügbarkeitsgruppen ändert. Ich vermute, dass Sicherungen nach wie vor als Sicherheitsnetz verwendet werden, bis sich die Administratoren genügend an die Funktionsweise von Datenbankverfügbarkeitsgruppen gewöhnt haben. Mit der Zeit wird das Vertrauen in diese neue Technik steigen, vor allem nach einem Ausfall, bei dem die Administratoren die Gelegenheit haben zu sehen, wie sie mithilfe von Datenbankverfügbarkeitsgruppen mit dieser Situation fertig werden können. In Zukunft werden wahrscheinlich mehr und mehr Exchange-Umgebungen ohne Sicherungen auskommen und sich ganz auf den Schutz durch Datenbankverfügbarkeitsgruppen verlassen.

Anhand dieser Punkte können Sie eine Kosten-Nutzen-Analyse durchführen, um herauszufinden, ob Ihre Organisation dazu bereit ist, ohne Sicherungen von Exchange-Daten auszukommen (es kann sein, dass Sie für andere Anwendungen nach wie vor herkömmliche Sicherungen benötigen), und wie schnell Sie den Wechsel nach der Bereitstellung von Exchange Server 2010 vollziehen können.

Natürlich müssen Sie alle diese Aspekte im Hinblick auf den Betrieb in Ihrem Unternehmen klären. Ein gutes Beispiel dafür ist der Papierkorb. Er ist in Exchange schon seit etwa zehn Jahren vorhanden und ermöglicht den Benutzern, versehentlich gelöschte Elemente ohne Hilfe eines Administrators wiederherzustellen. Gewöhnlich wird der Papierkorb so eingerichtet, dass er gelöschte Elemente 7 bis 14 Tage lang aufbewahrt, sodass die Benutzer genügend Zeit haben, um zu erkennen, dass sie irrtümlich etwas gelöscht haben, das sie noch brauchen, und es wiederherstellen können, bevor der Informationsspeicher es aus den Datenbanken entfernt. Für besondere Postfächer, z.B. diejenigen für die Geschäftsleitung, werden häufig längere Aufbewahrungszeiten von bis zu sechs Monaten eingerichtet. Die Elemente im Papierkorb werden bei der Berechnung des Kontingents nicht berücksichtigt, sodass der Papierkorb – je nachdem, wie eifrig der Benutzer beim Empfangen, Erstellen und Löschen und E-Mails ist – bis zu 10% der Größe des Postfachs annehmen kann. In manchen Organisationen werden Aufbewahrungszeiten von bis zu zwei Monaten festgelegt, sodass der Papierkorb einen zusätzlichen Speicherplatz von bis zu 25% belegen kann. Diese Mehrbelastung ist jedoch gerechtfertigt, wenn Sie bedenken, dass die Administratoren dadurch viel Zeit sparen, die sie sonst für die Wiederherstellung einzelner Elemente aufbringen müssten. Bei einem Postfach von 1 GB machen 10% 100 MB aus.

Wenn Sie die Postfachgröße auf 10 GB erhöhen, kann der Papierkorb 1 GB umfassen. Ist das noch akzeptabel? Wenn Sie die Daten jeden Tag sichern, dauern Sicherung und Wiederherstellung natürlich deutlich länger. Nutzen Sie dagegen die Datenreplikation, um sich gegen Verluste zu schützen, dann ist 1 GB zusätzlich erforderlicher Speicherplatz kein großes Übel, vor allem da Sie sehr viel Arbeitszeit einsparen, wenn Sie die Sicherungsverfahren einschränken oder ganz aufgeben. Dieses Beispiel zeigt, dass Sie Ihre bisherigen Verfahrensweisen genau unter die Lupe nehmen müssen, um die neuen Technologien und Funktionen nutzen und die Anforderungen Ihrer Organisation kostengünstig erfüllen zu können.

Das VSS-Plug-In für Windows Server-Sicherung

Viele Jahre lang konnten Sie in Exchange das Standardprogramm NTBACKUP verwenden, um Datenbanken auf Festplatte oder auf Band zu sichern. Grundlage war die API von ESE (Extensible Storage Engine), die Daten als Stream sicherte und wiederherstellte. Im Gegensatz dazu werden heute VSS-Snapshot-Sicherungen verwendet. Bandsicherungen erfüllten zwar ihren Zweck, doch angesichts immer größerer Datenbanken dauerte es immer länger, um die Sicherungen durchzuführen, selbst mit schnelleren Bändern und ausgefeilten Bandbibliotheken. Als Exchange Server 2007 SP1 auf Windows Server 2008 ausgeführt werden konnte, nahm Microsoft die Möglichkeit heraus, Streaming-Sicherungen von Exchange-Datenbanken durchzuführen, und sah einzig und allein VSS-Sicherungen für Anwendungen vor. Für kleine und mittlere Unternehmen war das ein großes Problem, da gerade sie Streaming-Sicherungen einsetzten. Große Unternehmen verwendeten auch größere Datenbanken und hatten daher gewöhnlich modernere Sicherheitsverfahren mit VSS entwickelt, weshalb sie von diesem Wechsel nicht so stark betroffen waren.

Microsoft reagierte darauf mit dem VSS-Plug-In *WSBExchange.exe* für Windows Server-Sicherung, das zusammen mit der Postfachrolle von Exchange Server 2007 SP2 und Exchange Server 2010 instal-

liert wird. Es gibt einige Unterschiede in der Funktionsweise von Windows Server-Sicherung und NTBACKUP und auch einige Einschränkungen, die Sie bei der Planung von Sicherungen bedenken müssen. Nehmen Sie sich also die Zeit, ein bisschen mit Windows Server-Sicherung herumzuspielen, indem Sie einige Sicherungen und Wiederherstellungen auf einem Testserver durchzuführen. Vor allem müssen Sie die folgenden Punkte beachten:

- Die ursprüngliche Version von Windows Server-Sicherung konnte nur VSS-Sicherungen von kompletten Volumes anlegen. Wenn es neben den Exchange-Datenbanken auch noch andere Daten in dem Volume gibt, werden sie mit in die Sicherung aufgenommen. Außerdem war es nicht möglich, einzelne Datenbanken zu sichern, da alle Datenbanken in dem Volume verarbeitet wurden. Diese Probleme gehören der Vergangenheit an, wenn Sie Windows Server 2008 R2 zusammen mit Exchange Server 2010 SP1 verwenden. In dieser Kombination können Sie einzelne Verzeichnisse auswählen, die Windows Server-Sicherung kopieren soll, z.B. diejenigen, die nur die Exchange-Postfachdatenbanken enthalten.
- Sie haben die Wahl zwischen vollständigen VSS-Sicherungen und VSS-Kopiesicherungen. Der Unterschied liegt darin, dass die Transaktionsprotokolle nach einer vollständigen Sicherung abgeschnitten werden, nicht aber nach einer Kopiesicherung. Erfolgreich heißt in diesem Zusammenhang, dass eine Konsistenzprüfung die Gültigkeit der Datenbank bestätigt hat und dass das gesamte Volume kopiert wurde.
- Um ein Postfach oder eine einzelne Datenbank zurückzugewinnen, stellen Sie sie zunächst in einem anderen Volume von der Sicherung wieder her und verwenden die Dateien dann, um eine Wiederherstellungsdatenbank aufzubauen.
- Remotesicherungen sind nicht möglich. Sie müssen die Sicherung auf dem Server ausführen, auf dem sich die Datenbanken befinden.
- Die Sicherungsdateien können auf einer lokalen Festplatte oder auf einer Netzwerkfreigabe angelegt werden. Eine direkte Sicherung auf Band ist nicht möglich. Wenn Sie Sicherungsbänder benötigen, die Sie auswärts lagern möchten, müssen Sie zunächst eine Sicherung auf Festplatte durchführen und die Sicherungsdateien dann auf Band übertragen.
- Sie können eine Datenbank am ursprünglichen Speicherort wiederherstellen, aber auch auf einer anderen Festplatte. Bei der ersten Möglichkeit werden alle Dateien überschrieben, die sich an dieser Stelle befinden. Alle in einem Volume gesicherten Datenbanken müssen gemeinsam wiederhergestellt werden. Der Vorgang läuft automatisch ab; Sie müssen weder die Bereitstellung der Datenbank aufheben noch die Datenbankeigenschaft *Diese Datenbank kann bei einer Wiederherstellung überschrieben werden* aktivieren, wie es in früheren Versionen von Exchange der Fall war. Dass die Datenbanken jetzt automatisch überschrieben werden, ist schon beängstigend, denn wenn Sie einen Fehler machen, kann das zu unvorhersehbaren Problemen führen. Nehmen wir beispielsweise an, Sie wollen eine Datenbank auf einem logischen Gerät aus einer Sicherung wiederherstellen, denken aber nicht daran, dass es auf diesem logischen Gerät noch zwei weitere, fehlerfreie Datenbanken gibt. Bei einer Wiederherstellung überschreiben Sie alle drei Datenbanken! In diesem Fall tun Sie besser daran, die Datenbank an einem anderen Speicherort wiederherzustellen, sie dort zu überprüfen und die Dateien dann manuell an die richtige Stelle zu kopieren. Eine Datenbank, die Sie an einem anderen Speicherort wiederherstellen, kann Exchange auch bereitstellen und als Wiederherstellungsdatenbank verwenden.
- Bereitstellungspunkte können Sie nur dann verwenden, wenn Sie Exchange Server 2010 auf Windows Server 2008 R2 ausführen. Auf Windows Server 2008 SP2 müssen Sie für die Volumes mit den Exchange-Datenbanken Laufwerksbuchstaben angeben.

Nachdem wir jetzt wissen, wie Windows Server-Sicherung mit Exchange-Datenbanken umgeht, sehen wir uns VSS genauer an.

Exchange und der Volumeschattenkopie-Dienst

Der Volumeschattenkopie-Dienst (Volume ShadowCopy Services, VSS) wurde in Windows Server 2003 eingeführt. Exchange Server 2003 war die erste Version des Messagingprodukts, die VSS für die Sicherung und Wiederherstellung von Datenbanken nutzte, und nach den ersten unvermeidlichen Startschwierigkeiten (aufgrund mangelnder Kenntnisse der Administratoren und einiger Softwarefehler) hat sich die dieser Dienst sowohl in Windows als auch in Exchange nach und nach weiterentwickelt und verbessert. Bei der VSS-Sicherung spielen die drei folgenden Komponenten eine wichtige Rolle:

- Die *Anforderungskomponente* ist eine Sicherungsanwendung wie Backup Exec oder Microsoft System Center Data Protection Manager (DPM).
- Der *Anbieter* ist eine Windows-Komponente, die den Zugang zu einer VSS-Kopie vermittelt.
- Die *Schreibkomponente* ist ein anwendungsspezifisches Bestandteil, das Daten für die Sicherung vorbereitet. Beispielsweise die Exchange-Schreibkomponente ESE anweisen, den Inhalt des Arbeitsspeicher-Caches auf die Festplatte zu schreiben, damit eine vollständige Sicherung durchgeführt werden kann.

Was im Einzelnen geschieht, wenn Sie eine VSS-Sicherung für Exchange durchführen, hängt davon ab, welche Sicherungsanwendung Sie einsetzen. Den Verlauf der Sicherung können Sie beobachten, indem Sie sich die Ereignisse im Anwendungsprotokoll anschauen. Das allgemeine Verfahren läuft wie folgt ab:

- Die Sicherungsanwendung (die Anforderungskomponente) wendet sich an VSS (den Anbieter), um den Zugriff auf eine Exchange-Datenbank anzufordern. In der Benutzeroberfläche der Sicherungsanwendung kann der Administrator angeben, welche Datenbanken er in die Sicherung aufnehmen möchte, und diese Auswahl wird an den Anbieter weitergegeben.
- VSS ruft die Exchange-Schreibkomponente auf und teilt ihr mit, dass eine Sicherung angefordert wurde. Dies ist die Phase *PrepareBackup*, die ESE dazu zwingt, Daten aus dem Arbeitsspeicher auf die Festplatte zu schreiben, das aktuelle Transaktionsprotokoll zu schließen und die Prozesse zu beenden, die Daten in den Cache (Prozess für verzögertes Schreiben) und in die Transaktionsprotokolle schreiben.
- Anschließend weist VSS die Exchange-Schreibkomponente an, die Zieldatenbank »einzufrieren«, um einen festen Zustand für die Sicherung zu erreichen. Während Datenbanken eingefroren sind, akzeptieren sie keine neuen Schreibanforderungen.
- ESE wartet, bis alle Daten aus dem Cache auf die Festplatte geschrieben und die Dienste angehalten sind, und teilt der Anforderungskomponente anschließend mit, dass die Zieldatenbanken eingefroren sind.
- Nachdem alles eingefroren ist, erstellt VSS einen Snapshot und platziert ihn auf einer anderen Festplatte.
- Nach Fertigstellung des Snapshots wird Exchange von VSS wieder »aufgetaut«, sodass die normale Verarbeitung wieder ihren Lauf nehmen kann. Die Prozesse für verzögertes Schreiben und für das Schreiben in die Protokolle werden wieder aufgenommen. Gewöhnlich bemerken die Benutzer die Unterbrechung nicht, vor allem dann, wenn sie Outlook im Exchange-Cache-Modus verwenden.
- Die Sicherungsanwendung führt eine Konsistenzprüfung durch, um sich zu vergewissern, dass sie über fehlerfreie Kopien der Datenbankdateien und Transaktionsprotokolle verfügt. Anschließend entfernt sie die gesicherten Transaktionsprotokolle von der Festplatte.
- Die Sicherungsanwendung meldet die erfolgreiche Durchführung und löst die Verbindung mit VSS.

Nach der Aufnahme des Snapshots wird gewöhnlich ein weiteres Verfahren gestartet, um diesen Snapshot von der Festplatte auf Band zu übertragen, sodass er zur Archivierung oder als Vorsichtsmaßnahme gegen Notfälle an einem externen Standort gelagert werden kann.

Durchführen einer Exchange Server 2010-Sicherung

Die Argumente für die Ansicht, dass man Exchange Server 2010 auch ohne Sicherungen betreiben könne, wenn man genügend Datenbankkopien in einer geschickt entworfenen Datenbankverfügbarkeitsgruppe bereitstellt, haben etwas für sich, doch haben nur wenige Administratoren genug Vertrauen in die Software und Hardware entwickelt, um sich zu dieser Meinung zu bekehren. Zum Glück lassen sich Sicherungen mit Windows Server-Sicherung ohne große Schwierigkeiten erstellen, sofern es keine passiven Datenbanken auf dem Server gibt. Dieses Thema werden wir auch noch angemessen besprechen, aber zunächst einmal gehen wir von dem einfachen Fall einer Sicherung auf einem Server aus, auf dem es nur aktive Datenbanken gibt. Dabei ist es egal, ob es sich um einen eigenständigen Server oder ein Mitglied einer Datenbankverfügbarkeitsgruppe handelt. Datenbanken für öffentliche Ordner können keine Kopien aufweisen und sind daher stets aktiv, sodass sie bei Sicherungen keine Probleme bereiten, sondern einfach mit eingeschlossen werden, wenn sie sich auf dem betreffenden Server befinden.

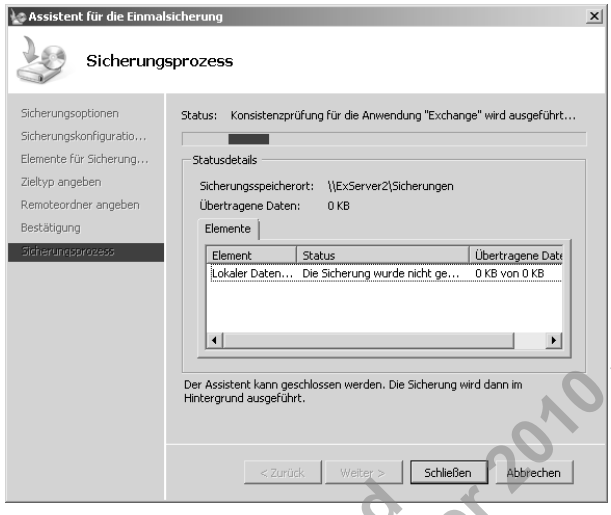
Windows Server-Sicherung weist einen Assistenten auf, mit dem Sie in mehreren Schritten einen Sicherungsauftrag erstellen und damit eine Reihe von Optionen auswählen können. Sobald die Sicherungsanwendung mit der Verarbeitung der Datenbanken beginnt, brauchen Sie sie nicht mehr geöffnet zu halten. Wenn Sie den Assistenten schließen, läuft sie bis zum Abschluss des Vorgangs im Hintergrund. Um sich zu vergewissern, dass die Sicherung erfolgreich verlaufen ist, können Sie später im Ereignisprotokoll oder in Windows Server-Sicherung nachsehen.

1. Starten Sie Windows Server-Sicherung und wählen Sie die Option, um zum jetzigen Zeitpunkt eine Sicherung vorzunehmen (*Einmalsicherung*).
2. Wählen Sie *Unterschiedliche Optionen*, um angeben zu können, welche Volumes Sie sichern möchten, und dann *Benutzerdefiniert*, um die gewünschten Volumes festzulegen. Denken Sie daran, dass sämtliche Datenbanken in diesen Volumes in die Sicherung aufgenommen werden. Wenn sich Datenbanken und Transaktionsprotokolle in unterschiedlichen Volumes befinden, müssen Sie dafür sorgen, dass alle relevanten Informationen in die Sicherung eingeschlossen werden.
3. Klicken Sie auf *Erweiterte Einstellungen* und wählen Sie dann *Vollständige VSS-Sicherung* aus, damit die Transaktionsprotokolle nach der erfolgeichen Sicherung abgeschnitten werden.
4. Wählen Sie das Ziel für die Sicherung aus. Dabei kann es sich um einen lokalen Datenträger, aber auch um eine Netzwerkfreigabe handeln. Natürlich erfolgt der Vorgang auf einer lokalen Festplatte schneller. Windows Server-Sicherung überprüft, ob Sie die erforderlichen Berechtigungen haben, um auf das ausgewählte Ziel zu schreiben. Sorgen Sie dafür, dass am Ziel genügend freier Speicherplatz vorhanden ist. Windows Server-Sicherung schreibt auch einen Satz von XML-Dateien mit Metadaten über die Sicherung und die VHD-Dateien (Virtual Hard Disk, virtuelle Festplatte) für jedes Volume an diese Stelle.
5. Überprüfen Sie die Sicherungsoptionen, die Sie gewählt haben, und fahren Sie mit dem Vorgang fort.

   Windows Server-Sicherung richtet die erforderlichen Dateien und Ordner am Sicherungsziel ein.

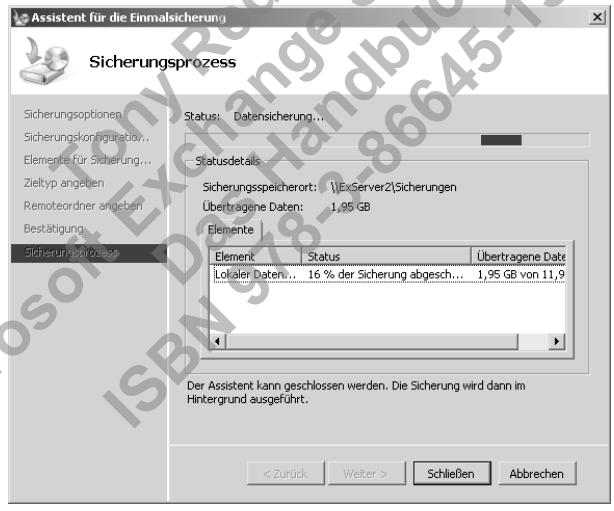
Anschließend fordert Windows Server-Sicherung von Exchange eine Konsistenzprüfung der Datenbanken an, um sicherzustellen, dass sie sich als Sicherungsdaten eignen (siehe Abbildung 9.1). Dabei wird jede Datenbank einzeln überprüft. Wenn eine den Test nicht besteht, verzeichnet Windows Server-Sicherung das Problem im Anwendungsprotokoll, fährt aber mit dem Verfahren fort. Die Datenbanken und Transaktionsprotokolle werden in die Sicherung aufgenommen, können aber nicht zur Wiederherstellung verwendet werden.

Abbildg. 9.1 Windows Server-Sicherung führt eine Exchange-Konsistenzprüfung durch.



Windows Server-Sicherung kopiert die Volumes zum festgelegten Ziel (siehe Abbildung 9.2).

Abbildg. 9.2 Windows Server-Sicherung kopiert Exchange-Daten.



Nachdem alle Volumes verarbeitet sind, beendet Windows Server-Sicherung den Vorgang und aktualisiert den Sicherungsverlauf auf dem lokalen Server.

Die einzelnen Schritte des Sicherungsvorgangs können Sie nachverfolgen, indem Sie die im Anwendungsprotokoll verzeichneten Ereignisse untersuchen. Tabelle 9.1 zeigt eine beispielhafte Abfolge von Ereignissen, wie sie bei einer Sicherung auf einem Server auftreten können, der Mitglied einer Datenbankverfügbarkeitsgruppe ist und mehrere Datenbanken beherbergt. Von diesen Datenbanken kann es auch noch weitere Kopien auf anderen Servern geben. Ist die Umlaufprotokollierung aktiviert, kann Exchange die Transaktionsprotokolle möglicherweise nicht abschneiden. Das gilt vor allem dann, wenn die Sicherung zu einem Zeitpunkt geringer Benutzeraktivität erfolgt, in der keine Transaktionsprotokolle erstellt wird. Ist ein Abschneiden der Transaktionsprotokolle nicht erforderlich, wird Ereignis 9827 gemeldet. Ohne Umlaufprotokollierung schneidet Exchange die Transaktionsprotokolle nach einer erfolgreichen vollständigen Sicherung ab und zeichnet Ereignis 9780 auf.

HINWEIS Bei einigen dieser Schritte werden mehrere Ereignisse mit derselben Kennung aufgezeichnet. Beispielsweise wird Ereignis 2001 für jede einzelne Datenbank protokolliert, die ESE zur Vorbereitung auf die Sicherung einfriert.

Tabelle 9.1 Sicherungsereignisse

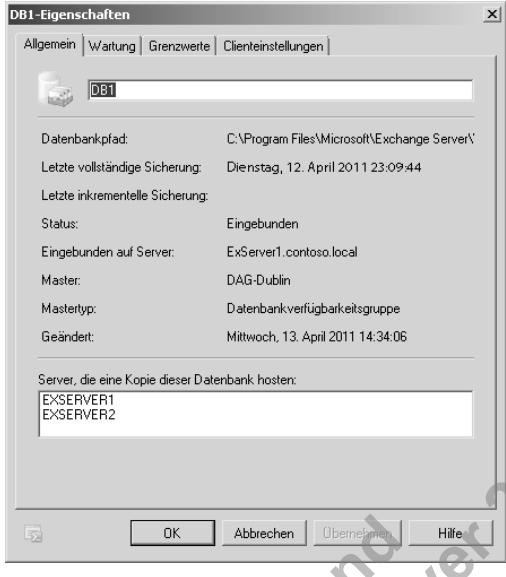
Ereigniskennung	Quelle	Ereignis
9606	MSExchangeIS	Die VSS-Schreibkomponente wird zur Verarbeitung der Datenbanken vorbereitet.
2005	ESE	Der Schattenkopiedienst wird gestartet. ESE erstellt eine Instanz und erlaubt ihm den Zugriff auf die Datenbanken.
9811	MSExchangeIS	Das Datenbankmodul die auf dem Server bereitgestellten Datenbanken auf die Sicherung vor.
2001	ESE	ESE friert die einzelnen Datenbanken ein.
9610	MSExchangeIS	Das Einfrieren war erfolgreich.
2003	ESE	Der Einfriervorgang wird beendet.
9612	MSExchangeIS	Die Datenbanken wurden erfolgreich aufgetaut.
3156	MSExchangeIS	Die Datenbanken werden für die ESE-Instanz bereitgestellt, die die Sicherung durchführt.
224 oder 225	ESE	ESE gibt an, wie das Abschneiden der Protokolle verlief. Ereignis 224 wird gemeldet, wenn Protokolle abgeschnitten werden (wobei die Namen der abgeschnitten Protokolldateien vermerkt werden). Ist kein Abschneiden erforderlich, wird Ereignis 225 aufgezeichnet.
9827 oder 9780	MSExchangeIS	Beide Ereignisse zeigen an, dass die Sicherung erfolgreich verlief. Ereignis 9827 wird gemeldet, wenn keine Transaktionsprotokolle abgeschnitten wurden, anderenfalls wird Ereignis 9780 aufgezeichnet.
2006	ESE	ESE bestätigt, dass die vollständige Sicherung erfolgreich verlaufen ist.
9618	MSExchangeIS	Die VSS-Schreibkomponente von Exchange wird geschlossen.
9648	MSExchangeIS	Das Sicherungsprogramm wird geschlossen.

Nach einer erfolgreichen vollständigen Sicherung schneidet Windows Server-Sicherung die Transaktionsprotokolle für die Datenbanken ab und aktualisiert in den Datenbankeigenschaften das

Datum der letzten guten Sicherung. Dieses Datum können Sie einsehen, indem Sie die Datenbank in der Exchange-Verwaltungskonsole markieren und ihre Eigenschaften aufrufen (siehe Abbidlung 9.3) oder indem Sie mit dem folgenden Befehl den Sicherungsstatus des Servers abrufen:

```
Get-MailboxDatabase -Server 'ServerName' -Status | Select Name, LastFullBackup
```

Abbildg. 9.3 In den Datenbankeigenschaften wird das Datum der letzten erfolgreichen Sicherung angezeigt.



Sie können auch nach allen Postfachdatenbanken in der Organisaton suchen, die noch nie gesichert wurden. Hierbei ist der Parameter *-Status* wichtig, da Sie Exchange damit zwingen, Informationen über Sicherungszeitpunkte auszugeben. Ohne *-Status* würden alle Datenbanken aufgelistet, da Exchange dann kein Sicherungsdatum sieht und daher überall NULL-Werte annimmt.

```
Get-MailboxDatabase -Status | Where {$_.LastFullBackup -eq $Null} | Select Name
```

Befindet sich auf dem Server auch eine Datenbank für öffentliche Ordner, müssen Sie dafür einen eigenen Befehl geben:

```
Get-PublicFolderDatabase -Status | Where {$_.LastFullBackup -eq $Null} | Select Name
```

Insidertipp: Andere Sicherungsprodukte

Anspruchsvollere Sicherungsprodukte wie Microsoft System Center DPM, Symantec Backup Exec oder HP Data Protector weichen in Einzelheiten von dem hier vorgestellten Vorgang ab, Funktionsprinzip und allgemeiner Ablauf aber sind identisch. Alle wichtigen Sicherungsprodukte sind jetzt so aktualisiert worden, dass sie auch für Exchange Server 2010 verwendet werden können und in der Lage sind, Sicherungen der aktiven und passiven Datenbanken in Datenbankverfügbarkeitsgruppen vorzunehmen. Trotzdem sollten Sie den Anbieter Ihres Sicherungsprodukts fragen, ob besondere Maßnahmen erforderlich sind, um sicherzustellen, dass Sie zuverlässige Sicherungen anlegen, aus denen Sie Ihre Daten bei Bedarf wiederherstellen können.

Schwierigkeiten bei der Sicherung aufgrund passiver Datenbankkopien

Das Exchange-Plug-In für Windows Server-Sicherung ermöglicht Onlinesicherungen von Postfachdatenbanken, eignet sich aber nicht zum Sichern der Datenbankkopien in einer Datenbankverfügbarkeitsgruppe. Zwar kann dieses Programm auch einen Mitgliedserver einer solchen Gruppe sichern, aber nur, wenn alle Datenbankkopien auf ihm aktiv sind. Sind auch passive Datenbanken vorhanden, werden die Daten zwar kopiert, bestehen aber die Konsistenzprüfung nicht, weshalb die Sicherung nicht zur Wiederherstellung herangezogen werden kann. Der Grund dafür liegt darin, dass der Informationsspeicher die passiven Datenbanken nicht auf solche Weise bereitstellt wie die aktiven. Nur der Exchange-Replikationsdienst greift auf diese Datenbanken zu, um die von den Servern mit den aktiven Kopien übertragenen Transaktionsprotokolle einzuspielen. Es ist also eine zweite VSS-Schreibkomponente erforderlich, die es Windows Server-Sicherung erlaubt, über den Exchange-Replikationsdienst auf die passiven Datenbanken zuzugreifen.

TIPP Es ist durchaus möglich, dass Windows Server-Sicherung mit der Zeit verbessert wird und auch mit den Schwierigkeiten fertig wird, die sich durch das Vorhandensein von aktiven und passiven Datenbankkopien in einer Verfügbarkeitsgruppe stellen. Daher sollten Sie vor dem Einrichten eines Sicherheitsverfahrens in Ihrer Produktionsumgebung Tests mit den neuesten Softwareversionen durchführen. Die hier beschriebenen Erfahrungen gehen auf Exchange Server 2010 SP1 und Windows Server 2008 R2 zurück.

Da auf Mitgliedservern einer Datenbankverfügbarkeitsgruppe in der Produktion wahrscheinlich sowohl aktive als auch passive Kopien vorhanden sind, wird in solchen Umgebungen gewöhnlich ein anspruchsvolleres Sicherungsprodukt bereitgestellt, z.B. Microsoft System Center DPM. Wenn Sie nicht dazu bereit sind, Geld für zusätzliche Software auszugeben, können Sie auch ein Verfahren entwickeln, bei dem Sie die aktiven Datenbanken so zwischen den Servern umschalten, dass sie mit Windows Server-Sicherung kopiert werden können. Dabei schalten Sie alle Datenbanken auf einem Server aktiv, sodass er keine passiven Kopien mehr enthält, wenn Sie mit der Sicherung beginnen. Das ist zwar möglich, aber offensichtlich mit viel Handarbeit verbunden, ganz zu schweigen von der Fehleranfälligkeit und den möglichen Betriebsstörungen für die Benutzer. Besser ist es, die bittere Pille zu schlucken und in Sicherungssoftware zu investieren, die mit sämtlichen möglichen Konstellationen in einer Datenbankverfügbarkeitsgruppe fertig wird bis hin zu der Möglichkeit, Datenbanken für öffentliche Ordner, aktive und passive Postfachdatenbankkopien alle zusammen zu sichern. Fragen Sie den Hersteller Ihres derzeitigen Sicherungsprodukts, ob dessen aktuelle Version für den Einsatz in Datenbankverfügbarkeitsgruppen geeignet ist, und welche Tipps er Ihnen zu einer möglichst rationellen Vorgehensweise für die Sicherung und Wiederherstellung in solchen Gruppen geben kann.

Insidertipp: Passive Datenbankkopien zur Entlastung des aktiven Servers

Es kann wünschenswert sein, Sicherungen der passiven Datenbankkopien vorzunehmen, um den aktiven Server zu entlassen. In manchen Umgebungen werden passive Kopien auf einem eigens dafür vorgesehenen Server gesammelt, der nur zu Verwaltungszwecken da ist. Sicherungen werden dann ausschließlich auf diesem Server vorgenommen. Je nach Anzahl der passiven Kopien, die auf die Server in der Datenbankverfügbarkeitsgruppe verteilt werden müssen, kann es aber auch sein, dass diese Vorgehensweise nicht möglich ist.

Wie wir bei der Beschreibung von Windows Server-Sicherung schon gesehen haben, werden die Transaktionsprotokolle nach der erfolgreichen vollständigen Sicherung einer aktiven Datenbank abgeschnitten oder gelöscht. Der Replikationsdienst auf dem Server mit der aktiven Kopie setzt sich dazu mit dem Informationsspeicher in Verbindung, um ihm den aktuellen Sicherungsstatus mitzuteilen. Der Informationsspeicher erkennt, dass eine erfolgreiche Sicherung erfolgt ist, und aktualisiert seinerseits den Header der Datenbank mit dem Sicherungsstatus, der Uhrzeit und dem Datum usw. Zusammen mit anderen Datenbankaktualisierungen werden die Headerdaten an alle Server mit Kopien repliziert. Der Code in *Eseback.dll* berechnet dann, welche Transaktionsprotokolle nach der Sicherung nicht mehr benötigt werden, und entfernt sie von dem Server, auf dem die Sicherung stattgefunden hat. Dieser Löschvorgang wird an den Replikationsdienst auf den Servern mit den Kopien gemeldet, sodass die dortigen Replikationsdienste auf ihren Servern die gleichen Protokolle abschneiden können.

Wiederherstellung in einer Wiederherstellungsdatenbank

Wenn Sie eine Datenbankverfügbarkeitsgruppe betreiben und darin ein Server oder ein Speicher ausfällt, sollten Sie in der Lage sein, zu einer Datenbankkopie umzuschalten, sodass die Benutzer weiterhin auf ihre Daten zugreifen können, während Sie das Problem beheben. Der große Vorteil von Datenbankverfügbarkeitsgruppen lässt sich in einem kurzen Satz ausdrücken: Der Betrieb geht auch bei einem Server- oder Speicherausfall weiter. Voraussetzung dafür ist natürlich, dass Sie über genügend Datenbankkopien verfügen und dass der Ausfall nicht sämtliche Kopien betrifft. Wenn jedoch ein Speicherfehler auftritt, ohne dass Sie auf eine Datenbankverfügbarkeitsgruppe zurückgreifen können, müssen Sie eine Wiederherstellung von einer Sicherung durchführen.

Insidertipp: Die ungeschminkte Wahrheit über die Wiederherstellung gelöschter Elemente

Selbst wenn Sie eine Datenbankverfügbarkeitsgruppe haben, kann es immer noch sein, dass Sie auf eine Sicherung zurückgreifen müssen, um Daten wiederzugewinnen, die auf andere Weise nicht mehr zugänglich sind. Die verlängerten Aufbewahrungszeiten für gelöschte Objekte helfen zwar, die Arbeit auf die Benutzer abzuwälzen, die ein Element versehentlich aus ihrem Postfach gelöscht haben und jetzt feststellen, dass sie es doch wieder brauchen, aber laut Murphys Gesetz denken die meisten Administratoren erst dann daran, die Standardaufbewahrungszeit für gelöschte Objekte von 14 Tagen zu verlängern, nachdem sich ein Benutzer gemeldet hat, der ein wichtiges Element vor 15 Tagen gelöscht hat. Möglicherweise können Sie solche Ansinnen auf Wiederherstellung aufgrund der hohen Kosten und des damit verbundenen Arbeitsaufwands ablehnen, aber wahrscheinlich müssen Sie den Vorgang doch durchführen, vor allem, wenn der Benutzer, der Sie darum bittet, ein Mitglied der Geschäftsführung ist.

Mit Windows Server-Sicherung können Sie Exchange Server 2010-Datenbanken an demselben Speicherort wiederherstellen, an dem sie gesichert wurden, aber auch an einem anderen. In beiden Fällen werden sämtliche Datenbanken und Transaktionsprotokolle eines ganzen Volumes wiederhergestellt. Die Wiederherstellung am selben Ort ist die Möglichkeit, die Sie wählen, wenn Sie eine Festplatte ersetzen müssen und Sie alle ihre Inhalte auf den Zustand an demselben Zeitpunkt zurückversetzen möchten. Wollen Sie dagegen nur die Daten in einen oder mehreren einzelnen Postfächern des Sicherungssatzes wiederherstellen, wählen Sie einen anderen Speicherort. Bei diesem Vorgang wird die Wiederherstellungsdatenbank genutzt, die Nachfolgerin der in Exchange Server 2003 und 2007 ver-

wendeten Speichergruppe für die Wiederherstellung. Dabei handelt es sich um eine Datenbank, die von einer Sicherung an einem Speicherort wiederhergestellt wurde, an dem Exchange auf sie zugreifen kann. Die Postfächer in der Wiederherstellungsdatenbank sind in getrenntem Zustand, da sie keine Verbindung zu Benutzerkonten in Active Directory haben, allerdings können Sie Verbindung mit diesen Postfächern aufnehmen, um Daten abzurufen und in reguläre Datenbanken zu verschieben, wo sie den Benutzern zur Verfügung stehen.

HINWEIS Es ist nicht möglich, eine Datenbank für öffentliche Ordner in einer Wiederherstellungsdatenbank wiederherzustellen. Letzteres gibt es nur für Postfachdatenbanken.

Durchführen der Wiederherstellung

Um die Wiederherstellung durchführen zu können, müssen Sie die Antworten auf die folgenden Fragen kennen:

- Wo ist der Sicherungssatz gespeichert?
- Welches Datum hat die Sicherung, die Sie wiederherstellen wollen?
- An welchem Speicherort soll die Wiederherstellung erfolgen?
- Was möchten Sie anschließend mit der wiederhergestellten Datenbank tun?

Wenn Sie einen Plan haben, in dem alle diese Fragen beantwortet werden, beginnen Sie damit, dass Sie Windows Server-Sicherung starten und darin auf den Speicherort verweisen, an dem sich der Sicherungssatz befindet. Das kann ein Ort auf demselben Speicher sein, aber auch ein Remoteordner. Wählen Sie die Dateien aus, die Sie wiederherstellen möchten. Abbildung 9.4 zeigt das entsprechende Dialogfeld. In diesem Fall stehen drei einzelne Datenbanken zur Wiederherstellung zur Verfügung, wobei eine markiert ist (nämlich *DB3*).

Abbildg. 9.4 Auswählen der wiederherzustellenden Datenbankdateien

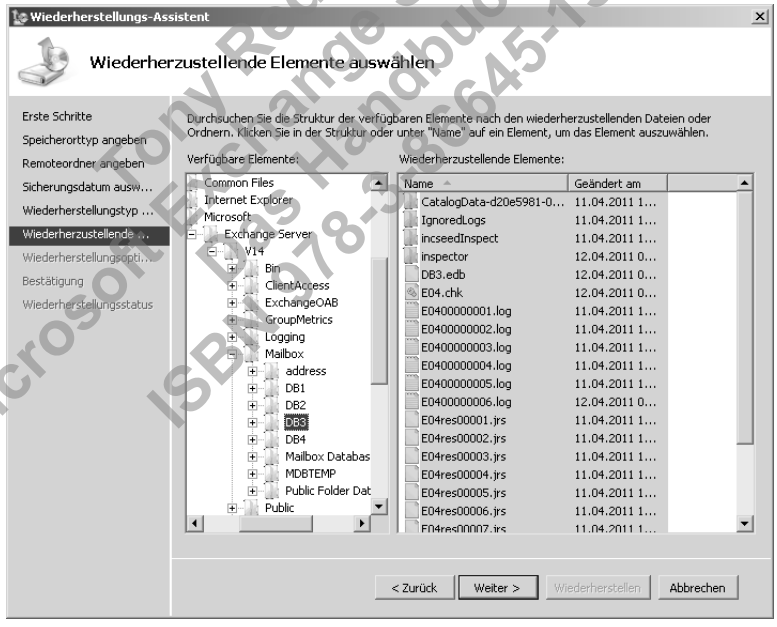
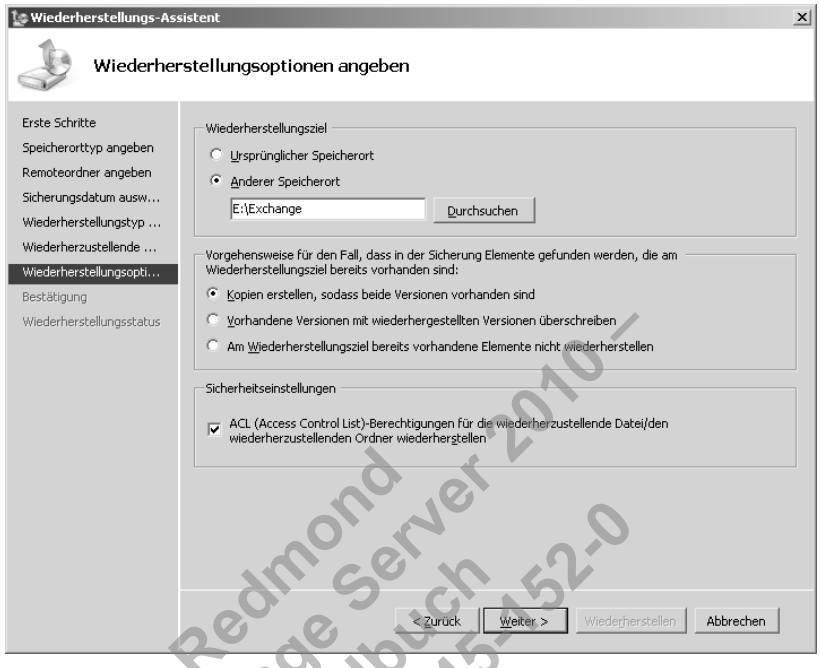


Abbildung 9.5 zeigt den nächsten Schritt, in dem Sie den Speicherort für die Wiederherstellung auswählen (der Ordner muss bereits vorhanden sein, und Sie müssen für ausreichend Platz auf der Festplatte gesorgt haben) und die Parameter bestätigen, um fortfahren zu können. Wenn Sie Datenbanken an ihrem ursprünglichen Speicherort wiederherstellen, hebt Exchange automatisch die Bereitstellung der Datenbanken auf, die sich zurzeit dort befinden, führt die Wiederherstellung durch und stellt dann die wiederhergestellten Datenbanken bereit, um sie online zu bringen. Dabei werden auch alle erforderlichen Transaktionsprotokolle eingespielt.

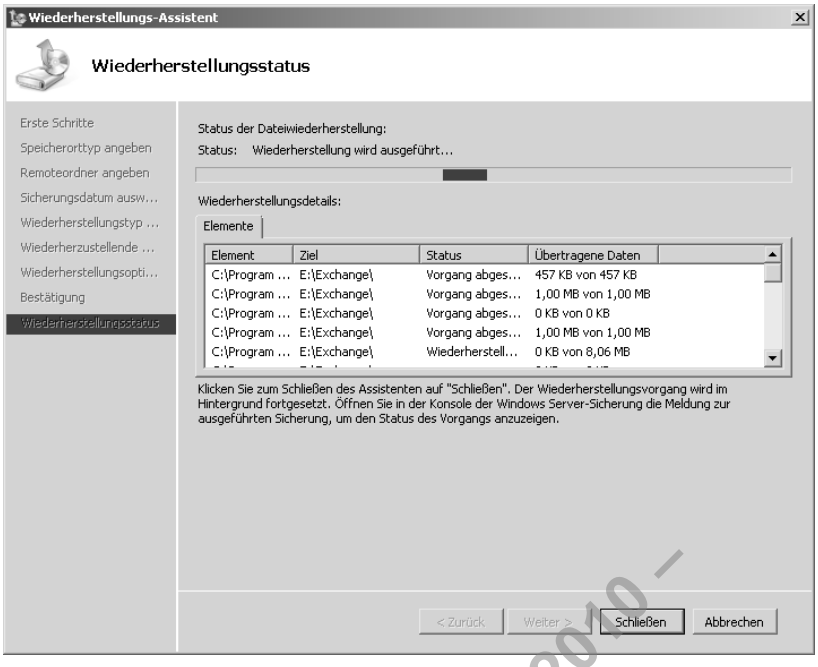
Abbildg. 9.5 Festlegen der Parameter für die Wiederherstellung



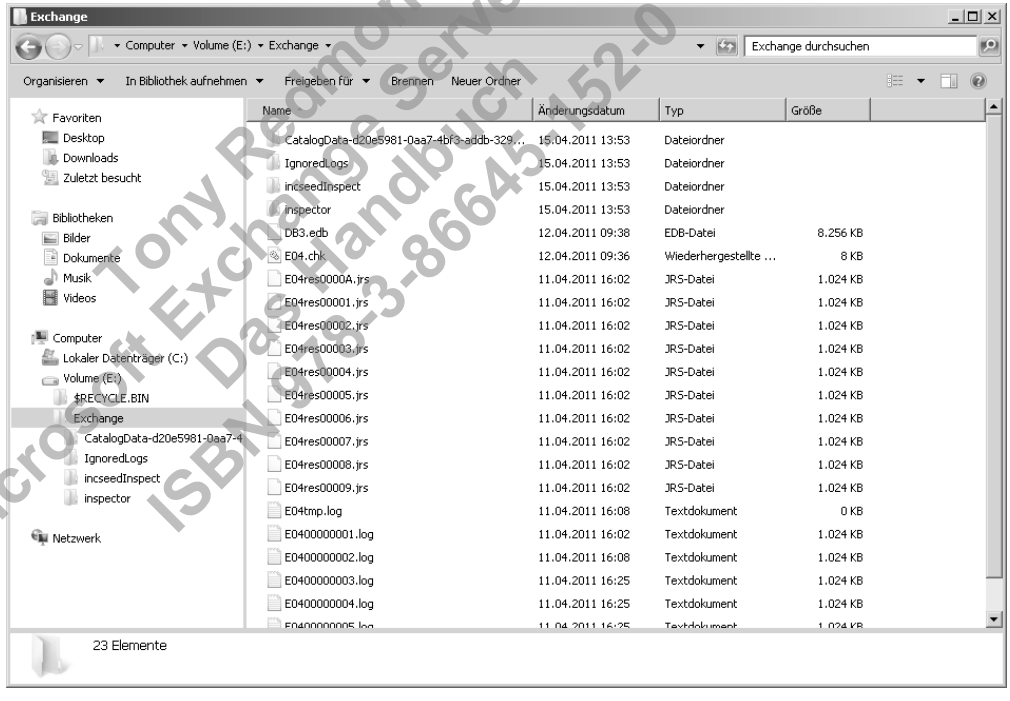
Die Wiederherstellung der Datenbanken erfolgt meistens schneller als die ursprüngliche Sicherung, da Sie gewöhnlich nur einen Teil der Daten aus dem gesamten Volume in der Sicherung wiederherstellen müssen. Abbildung 9.6 zeigt, dass mehrere Dateien wiederhergestellt wurden und dass Windows Server-Sicherung zurzeit die Datenbankdatei *DB3* verarbeitet. Wie viel Zeit für eine Wiederherstellung erforderlich ist, hängt von der Geschwindigkeit des Speicherteilsystems, von der Serverbelastung durch andere Tätigkeiten und der Größe der Datenbanken ab. Allerdings können Sie davon ausgehen, dass eine Wiederherstellung von einer Festplatte selbst auf dem langsamstem Server mit über 300 MB pro Minute erfolgt.

Nach der Wiederherstellung finden Sie die Datenbanken, Transaktionsprotokolle und Prüfpunktdateien am Wiederherstellungsspeicherort. Wie Sie in Abbildung 9.7 sehen, sind alle Datenbankdateien und Katalogordner für den Inhaltsindex an Ort und Stelle.

Abbildg. 9.6 Wiederherstellen der Dateien einer Exchange-Datenbank



Abbildg. 9.7 Datenbankdateien nach der Wiederherstellung



Insidertipp: Sinnvolle Verwendung der Option »Diese Datenbank kann bei einer Wiederherstellung überschrieben werden«

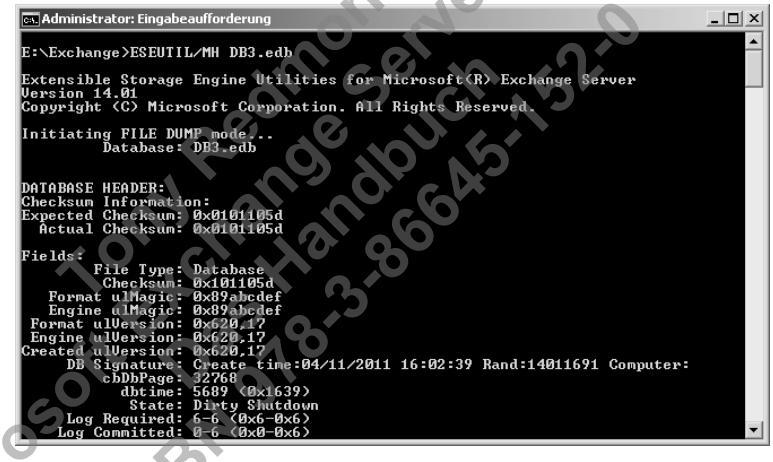
Es gibt noch einen kleinen Umstand, den Sie beachten sollten: Wenn Sie die Datenbankeigenschaften anzeigen, sehen Sie auch eine Option, die Exchange erlaubt, die Datenbank während einer Wiederherstellung zu überschreiben. Wenn Sie Windows Server-Sicherung verwenden, ist diese Einstellung jedoch ohne Bedeutung, da die Sicherungen und Wiederherstellungen volumeweise durchgeführt werden. Bei der Wiederherstellung hebt das Exchange-Plug-In für Windows Server-Sicherung die Bereitstellung der Kopie auf, die sich am Zielort befindet, sodass sie überschrieben werden kann. Die Option *Diese Datenbank kann bei einer Wiederherstellung überschrieben werden* ist jedoch für andere Sicherungsprodukte von Bedeutung, bei denen eine genauere Auswahl der wiederherzustellenden Objekte möglich ist.

Überprüfen der wiederhergestellten Datenbank

Die erforderlichen Dateien befinden sich jetzt auf der Festplatte, aber in Exchange können wir noch keine Verbindung mit der Datenbank aufnehmen, um Daten abzurufen. Als Erstes müssen wir überprüfen, ob sich die Datenbank in einem Zustand befindet, in dem sie als Wiederherstellungsdatenbank auf einem Server bereitgestellt werden kann. Dazu führen wir ESEUTIL aus, um die Datenbankheader zu überprüfen. In unserem Fall wollen wir uns den Header von *DB3.edb* genauer aussehen, weshalb der Befehl wie folgt lautet:

```
ESEUTIL/MH DB3.edb
```

Abbildg. 9.8 Überprüfen des Datenbankheaders mit ESEUTIL nach der Wiederherstellung

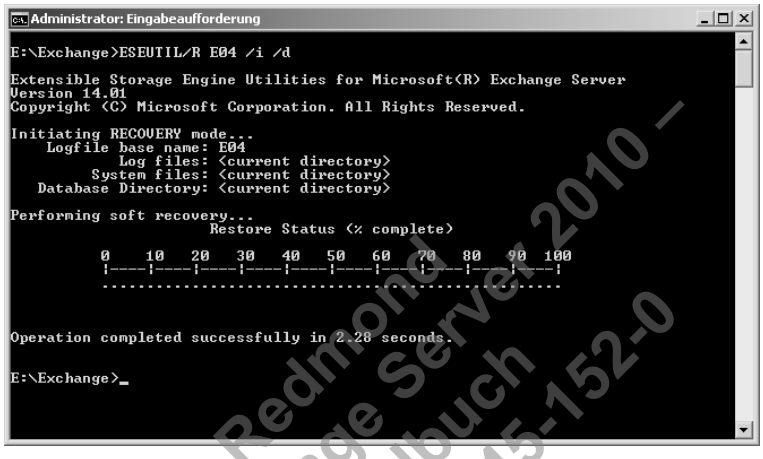


In der Ausgabe von ESEUTIL, die Sie in Abbildung 9.8 sehen, wird als Datenbankstatus *Dirty Shutdown* (mit modifizierten Seiten heruntergefahren) angegeben. In diesem Zustand weigert sich Exchange, eine Datenbank bereitzustellen, weshalb wir erneut ESEUTIL ausführen müssen, um alle ausstehenden Transaktionen einzuspielen, die sich in den wiederhergestellten Transaktionsprotokollen befinden, und die Datenbank damit auf einen aktuelleren Stand zu bringen. Dazu führen wir folgenden Befehl aus:

```
ESEUTIL /R E04 /i /d
```

Dank der Option */R* wird ESEUTIL im Wiederherstellungsmodus (*R* für »recovery«) ausgeführt. *E03* ist das Transaktionsprotokollpräfix für die Datenbank, die wir wiederherstellen möchten, wie wir anhand des letzten Transaktionsprotokolls oder er letzten Prüfpunktdatei ablesen können. In Abbildung 9.7 ist als Prüfpunktdatei *E04.chk* aufgeführt, weshalb *E04* das korrekte Präfix sein muss. Die Option */i* sorgt dafür, dass ESEUTIL das Fehlen von Dateien ignoriert, und mit */d* wird der Pfad für die Transaktionsprotokolle angegeben. Da wir uns bereits in dem Verzeichnis mit den wiederhergestellten Datenbank- und Protokolldateien befinden, brauchen wir diese Wert nicht anzugeben. ESEUTIL liest zunächst die Prüfpunktdatei, um herauszufinden, welche Transaktionen mit Commit in die Datenbank übernommen wurden, und gibt dann die ausstehenden Transaktionsprotokolle wieder, um ihre Daten in die Datenbank einzuspielen (siehe Abbildung 9.9). Wenn nicht gerade Tausende von Transaktionsprotokollen zu verarbeiten sind, läuft dieser Vorgang recht zügig ab. Datenbanken mit Umlaufprotokollierung, die durch die Mitgliedschaft in Verfügbarkeitsgruppen gegen Datenverluste geschützt sind, weisen gewöhnlich weit weniger Transaktionsprotokolle auf als andere.

Abbildg. 9.9 ESEUTIL aktualisiert die wiederhergestellte Datenbank durch die Daten aus den Transaktionsprotokollen.



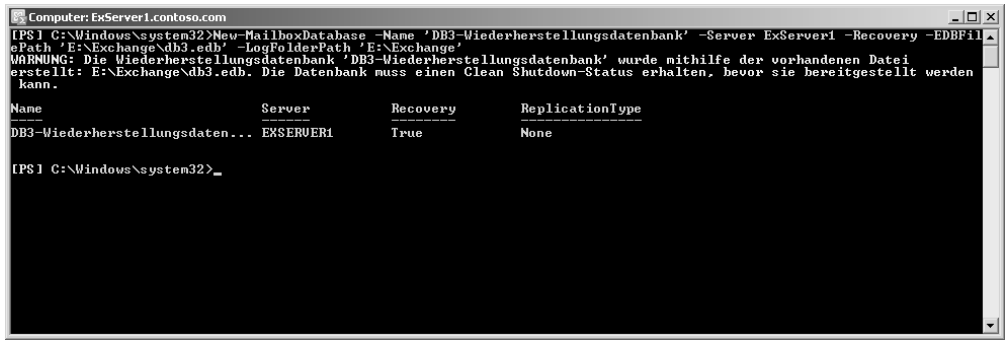
Nachdem das Programm ESEUTIL die Wiederherstellung der Datenbank abgeschlossen hat, können wir es mit der Option */MH* erneut ausführen, um uns zu vergewissern, dass sich die Datenbank jetzt im Zustand *Clean Shutdown* (sauber heruntergefahren) befindet.

Bereitstellen einer Wiederherstellungsdatenbank

Die Datenbank ist jetzt wiederhergestellt und validiert, aber in Exchange immer noch nicht zugänglich. Dazu müssen wir einen Zeiger auf die Datenbank erstellen und sie als Wiederherstellungsdatenbank kennzeichnen, was aber nur in der Exchange-Verwaltungsshell möglich ist. Als Erstes erstellen wir mit *New-MailboxDatabase* den Zeiger (und zwar in den Exchange-Konfigurationsdaten von Active Directory) auf die wiederhergestellte Datenbank. Der Trick besteht darin, den Parameter *-Recovery* zu verwenden, damit Exchange weiß, dass diese Datenbank für Wiederherstellungszwecke verwendet wird:

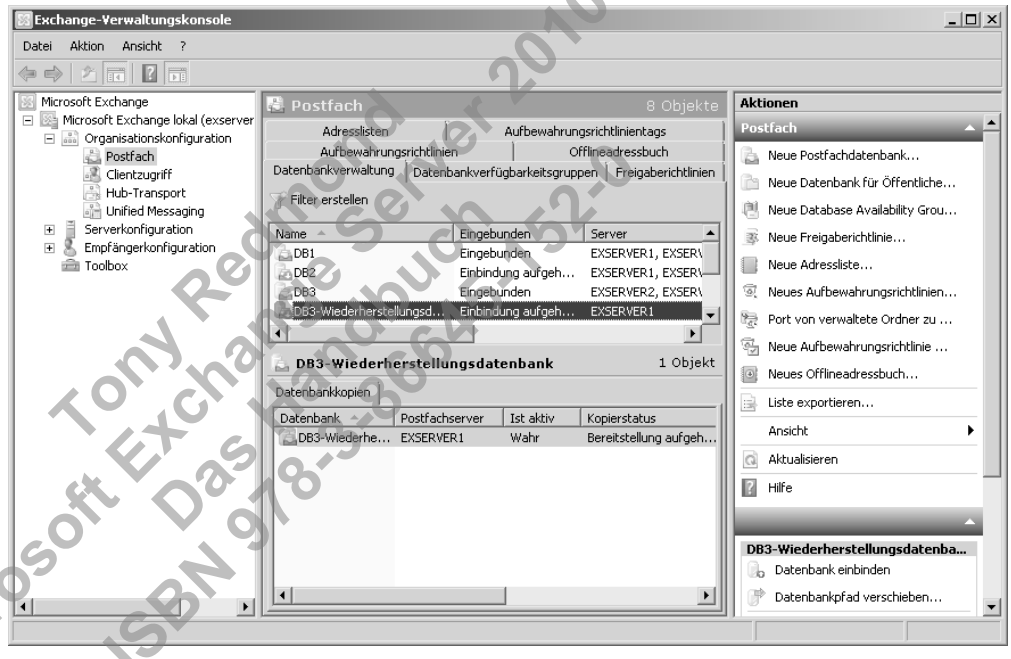
```
New-MailboxDatabase -Name 'DB3 Rec overy Database' -Server ExServer1 -Recovery -EDBFilePath
'E:\Exchange\db3.edb' -LogFolderPath 'E:\Exchange'
```

Abbildg. 9.10 Bekanntmachen der wiederhergestellten Datenbank in Exchange



Wie Sie in Abbildung 9.10 erkennen können, teilte Ihnen Exchange mit, dass Sie die wiederhergestellte Datenbank nur dann bereitstellen können, wenn Sie sich im Zustand *Clean Shutdown* befindet. Dafür haben wir schon mit ESEUTIL gesorgt, weshalb wir hier einfach fortfahren können. In der Exchange-Verwaltungskonsole wird die Wiederherstellungsdatenbank jetzt angezeigt, sodass wir sie genauso wie jede andere Datenbank verwalten können (siehe Abbildung 9.11).

Abbildg. 9.11 Anzeige der Wiederherstellungsdatenbank in der Exchange-Verwaltungskonsole



Als nächsten Schritt müssen wir die Datenbank bereitstellen, was wir sowohl in der Verwaltungskonsole als auch in der Verwaltungsshell tun können. Versuchen wir es in der Shell:

```
Mount-Database -Identity 'DB3 Recovery Database'
```

HINWEIS Wenn Sie versuchen, eine Datenbank bereitzustellen, bei der einige Dateien fehlen, warnt Sie Exchange, bietet Ihnen aber an, eine neue Datenbank anzulegen und diese bereitzustellen. Wenn Sie das zulassen, haben Sie eine wunderschöne neue und vollständig leere Datenbank, was manchmal durchaus in Ihrem Sinne sein kann (z.B. bei einer Dial-Tone-Wiederherstellung), aber nicht, wenn Sie einen kompletten Satz von Datenbank- und Protokolldateien wiederherstellen wollten.

Beim Bereitstellen der Datenbank werden eine neue Prüfpunktdatei und ein neuer Satz von Transaktionsprotokollen angelegt, um alle Änderungen zu erfassen, die an der Datenbank vorgenommen werden, während sie sich im Wiederherstellungsmodus befindet. Da die Datenbank jetzt bereitsteht, können wir mit einigen der Cmdlets für Postfachdatenbanken auf sie zugreifen. Beispielsweise können wir wie folgt die Namen der enthaltenen Postfächer und die Anzahl der darin befindlichen Elemente herausfinden:

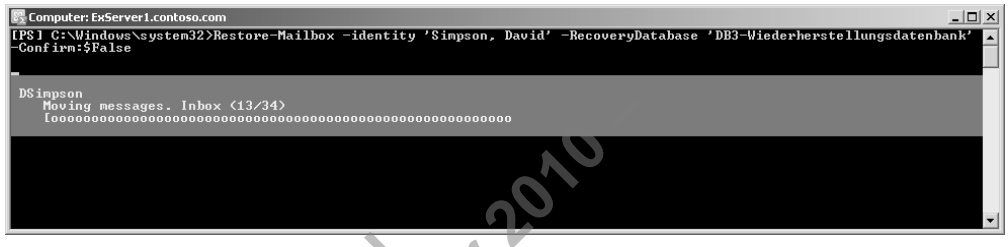
```
Get-MailboxStatistics -Database 'DB3 Recovery Database' | Select DisplayName, ItemCount |
Format-Table -AutoSize

DisplayName                                        ItemCount
-----------                                        ---------
Pelton, David (HQ)                                    74
Shen, Alan                                            41
Shah, Niraj (China HQ)                                37
Online Archive - Redmond, Tony                       126
Camelbeke, Geert                                      11
Akers, Kim                                           100
Online Archive - Akers, Kim                            7
Smits, Guntars                                        31
Redmond, Conor (IT)                                   43
Shen, Paul (China HQ)                                 39
Peled, Yael (IT)                                      26
Solovay, Andrew                                       30
Galway Conference Room                                17
Parker, Darren                                        20
Redmond, Tony                                       1053
Simpson, David (Sales)                                39
Pais, Wilson                                          21
SystemMailbox{3ef66f70-347f-4b1e-97ad-73e9ff908d0e}    1
```


Diese Informationen sind nützlich, da wir daran ablesen können, was sich in der Datenbank befindet. Allerdings können wir keine Cmdlets wie *Get-Mailbox* einsetzen, um Informationen über einzelne Postfächer in der Wiederherstellungsdatenbank abzurufen. Stattdessen müssen wir *Restore-Mailbox* verwenden, um die Postfächer in eine Onlinedatenbank zu verschieben, in der die Benutzer Zugriff auf die wiederhergestellten Daten haben.

Wiederherstellen der Postfachdaten

Restore-Mailbox und das in SP1 neu eingeführte *New-MailboxRestoreRequest* sind bemerkenswerte Cmdlets, die Sie auf verschiedene Weisen einsetzen können, um ein Postfach aus einer Wiederherstellungsdatenbank mit einem Zielpostfach in einer anderen Datenbank zusammenzuführen. Das Zielpostfach muss mit einem Benutzerkonto verbunden sein, allerdings können Sie Daten aus einem Postfach in der Wiederherstellungsdatenbank in ein Postfach mit einem anderen Namen in der Zieldatenbank verschieben. Zusammenführen heißt, dass die Nachrichten, die bereits im Zielpostfach vorhanden sind, nicht überschrieben werden. Der Vorgang ist nicht destruktiv, sondern ergänzt nur. Wie viel Zeit erforderlich ist, um ein Postfach zu untersuchen und die Elemente wiederherzustellen, hängt von der Anzahl der enthaltenen Objekte, der Serverkonfiguration und der Systemlast ab, aber Sie können damit rechnen, dass mehrere hundert Elemente pro Minute verarbeitet werden. Exchange hält Sie während des Vorgangs über den Fortschritt auf dem Laufenden, wie Sie in Abbildung 9.12 sehen.

Abbildg. 9.12 Wiederherstellen der Elemente in einem Postfach



Mit *Restore-Mailbox* haben Sie unter anderem folgende Möglichkeiten:

- Wiederherstellung der Daten aller Postfächer aus der Wiederherstellungsdatenbank in einer Onlinedatenbank. Der folgende Befehl ruft eine Liste der Postfächer in der Datenbank *DB3* ab und stellt alle Postfächer wieder her, die in der Wiederherstellungsdatenbank *DB3 Recovery Database* zu finden sind:

```
Get-Mailbox -Database 'DB3' | Restore-Mailbox -RecoveryDatabase 'DB3 Recovery Database'
```

- Wiederherstellung der Daten ausgewählter Postfächer aus der Wiederherstellungsdatenbank in einer Onlinedatenbank. Der folgende Beispielbefehl stellt den kompletten Inhalt des Postfachs für den Benutzer *Simpson, David (Sales)* aus der Wiederherstellungsdatenbank wieder her. Mit *-Confirm: $False* verhindern wir, dass Exchange uns um Bestätigung bittet, um fortzufahren, da wir davon ausgehen, dass wir wissen, was wir hier tun.

```
Restore-Mailbox -Identity 'Simpson, David (Sales)' -RecoveryDatabase 'DB3 Recovery
Database' -Confirm:$False
```

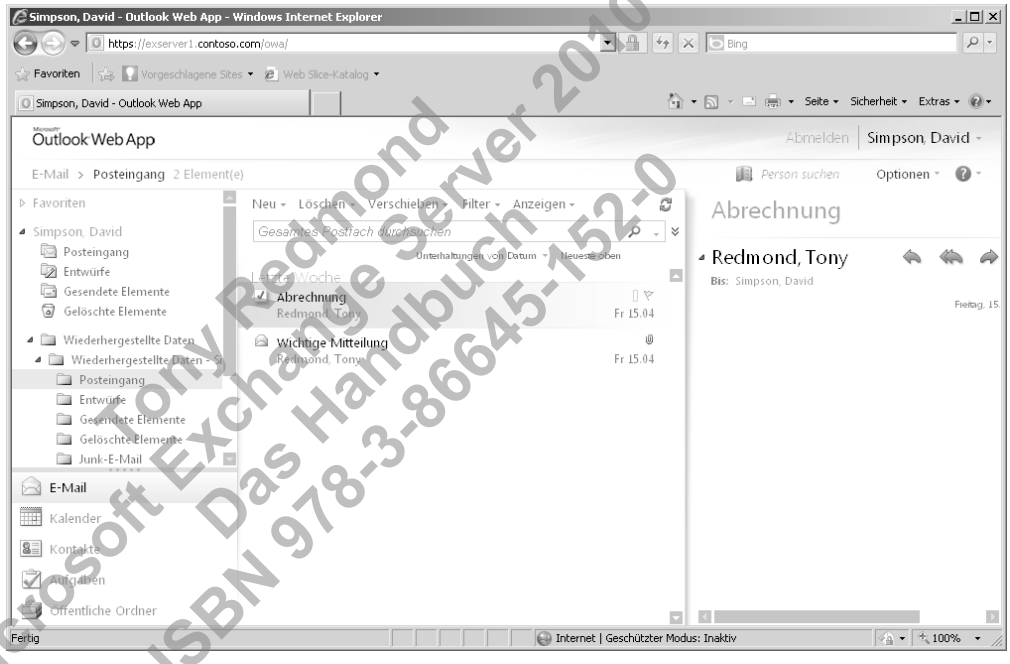
- Wiederherstellung ausgewählter Daten einzelner Postfächer aus der Wiederherstellungsdatenbank in einer Onlinedatenbank. Nehmen wir beispielsweise an, Kim Akers teilt uns mit, dass sie mehrere Elemente gelöscht hat, die sie nicht mehr aus dem Papierkorb zurückgewinnen kann, aber nur an dem Element *Confidential* interessiert ist, das aus dem Posteingang entfernt wurde. Dieses eine Element können Sie mit folgendem Befehl wiederherstellen:

```
Restore-Mailbox -Identity 'Akers, Kim' -RecoveryDatabase 'DB3 Recovery Database'
-IncludeFolders '\Inbox' -SubjectKeywords 'Confidential' -Confirm:$False
```

- Wiederherstellung ausgewählter Daten in einem neuen Ordner eines anderen Postfachs. Das ist eine nützliche Technik, um Informationen aus einer Sicherung wiederzugewinnen, die für eine Untersuchung benötigt werden, wenn sich die Daten nicht durch eine Discoverysuche finden lassen, da sie bereits abgelaufen sind und aus der Datenbank entfernt wurden. Im folgenden Beispiel suchen wir nach Informationen über ein Projekt namens »Athena« im Postfach von Kim Akes und exportieren alle gefundenen Elemente in den Wiederherstellungsordner im Postfach der Untersuchungsbeamten. Bei diesem Beispiel sind vor allem zwei Dinge bemerkenswert. Erstens sorgt der Parameter *-ContentKeywords* dafür, dass Exchange im Inhalt der Elemente und in den Anhängen sucht, was den Vorgang stark verlangsamen kann, wenn viele umfangreiche Anhänge zu durchsuchen sind. Zweitens können Sie zwar für den Parameter *-Identiy* jeden der üblichen Bezeichner für das Quellpostfach angeben (Alias, Name usw.), doch müssen Sie für den Parameter *-RecoveryMailbox* den Postfachnamen verwenden. Als Ergebnis der Suche wird ein Satz von Ordnern unter dem in dem Befehl angegebenen Stammordner ausgegeben. Außerdem werden der Name des Quellpostfachs sowie Datum und Uhrzeit der Wiederherstellung vermerkt. Abbildung 9.13 zeigt, wie die wiederhergestellten Elemente im Zielpostfach erscheinen.

```
Restore-Mailbox -Identity 'Legal Investigators' -RecoveryDatabas 'DB3 Recovery
Database'-SubjectKeywords 'Athena' -ContentKeywords 'Athena' -TargetFolder 'Recovered
Data' -RecoveryMailbox 'Akers, Kim' -Confirm:$False
```

Abbildg. 9.13 Wiederhergestellte Elemente in einem Zielpostfach



In allen Fällen erstellt Exchange zwei Protokolldateien mit Einzelheiten der von *Restore-Mailbox* durchgeführten Operationen, eine im Text- und eine im XML-Format. Beide Protokolle werden im Verzeichnis *\Logging\MigrationLogs* des Exchange-Stammverzeichnisses auf dem Server gespeichert, auf dem die Wiederherstellung stattfand. Das folgende Beispiel zeigt eine leicht bearbeitete Version der Textprotokolldatei:

```
[05/28/2010 11:39:19.0431] [0] Processing object "contoso.com/Exchange
Users/Simpson, David (Sales)".
[05/28/2010 11:39:19.0478] [0] Searching objects "DB3" of type "MailboxDatabase"
  under the root "$null".
[05/28/2010 11:39:19.0509] [0] Searching objects "b9f054d2-896f-4207-a9e0-db1ef3120c52"
  of type "MailboxStatistics" under the root "DB3 Recovery Database".
[05/28/2010 11:39:20.0274] [0] [DSimpson] The operation has started.
[05/28/2010 11:39:20.0274] [0] [DSimpson] Approving object.
[05/28/2010 11:39:20.0431] [0] [DSimpson] Opening source mailbox.
[05/28/2010 11:39:20.0446] [0] [DSimpson] Trying to open mailbox by GUID:
   szServerLegacyDN: /o=contoso/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=EXSERVER1
   pguidMdb: {533F6963-BB02-493A-92CD-CE1783155B75}
   pguidMailbox: {B9F054D2-896F-4207-A9E0-DB1EF3120C52}
   szServer: EXSERVER1.contoso.com
[05/28/2010 11:39:20.0446] [0] [DSimpson] Open mailbox succeeded.
[05/28/2010 11:39:20.0446] [0] [DSimpson] Opening destination mailbox.
[05/28/2010 11:39:20.0446] [0] [DSimpson] Trying to open mailbox by GUID:
   szServerLegacyDN: /o=contoso/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=EXSERVER2
   pguidMdb: {3EF66F70-347F-4B1E-97AD-73E9FF908D0E}
   pguidMailbox: {B9F054D2-896F-4207-A9E0-DB1EF3120C52}
   szServer: EXSERVER2.contoso.com
[05/28/2010 11:39:20.0446] [0] [DSimpson] Open mailbox succeeded.
[05/28/2010 11:39:20.0446] [0] [DSimpson] Moving messages.
[05/28/2010 11:39:20.0446] [0] [DSimpson] Recovering messages.
[05/28/2010 11:39:20.0446] [0] [DSimpson] Merging messages.
[05/28/2010 11:40:27.0259] [0] [DSimpson] 0 items couldn't be moved to the target mailbox.
[05/28/2010 11:40:27.0259] [0] [DSimpson] Messages moved. Closing connections.
[05/28/2010 11:40:27.0337] [0] [DSimpson] The operation has finished.
```

In Exchange Server 2010 SP1 können Sie auch das Cmdlet *New-MailboxRestoreRequest* verwenden, um Postfachdaten aus getrennten Postfächern oder aus Postfächern in Wiederherstellungsdatenbanken wiederherzustellen. Dabei wird das asynchrone Anforderungsmodell genutzt, das auch beim Verschieben, Importieren und Exportieren von Postfächern durch den Postfachreplikationsdienst zum Einsatz kommt. Dieses neue Cmdlet wurde nötig, da es in SP1 möglich sein muss, Daten aus einem Postfach wiederherzustellen, das bei einem Verschiebungsvorgang nur »weich« gelöscht wurde. Außerdem können Sie mit ihm Daten aus Archivpostfächern wiedergewinnen. Aufgrund der asynchronen Vorgehensweise des Postfachreplikationsdienstes müssen Sie nicht auf die Wiederherstellung der Daten warten. Führen Sie einfach den Befehl aus, um eine Wiederherstellungsanforderung zu erstellen, und kümmern Sie sich dann um andere Dinge, während die Anforderung bearbeitet wird.

Im folgenden Beispiel erstellen wir mit *New-MailboxRestoreRequest* eine Wiederherstellungsanforderung, um Daten aus dem Posteingangsordner im Postfach *Akers, Kim* der Datenbank *DB3 Recovery Database* zu lesen und in den Ordner für wiederhergestellte Elemente im Postfach *Legal Investigators* zu schreiben:

```
New-MailboxRestoreRequest -TargetMailbox 'Legal Investigators' -SourceDatabase 'DB3
RecoveryDatabase' -SourceStoreMailbox 'Akers, Kim' -BadItemLimit 5 -TargetRootFolder
'Recovered Items' -SourceRootFolder 'Inbox' -Name 'Legal Recovery Ref 104'
```

Das Ergebnis ist der Wiederherstellungsauftrag *'Legal Investigators'\Legal Recovery Ref 104*, der in die Warteschlange des Postfachreplikationsdienstes gestellt wird. Den Fortschritt können Sie mithilfe des Cmdlets *Get-MailboxRestoreRequest* überprüfen:

```
Get-MailboxRestoreRequest -Identity 'Legal Investigators'\Legal Recovery Ref 104'
```

Sobald der Auftrag abgeschlossen ist, können Sie sich das Ergebnis mit *Get-MailboxRestoreRequest-Statistics* ansehen:

```
Get-MailboxRestoreRequestStatistics -Identity 'Legal Investigators'\Legal Recovery Ref 104'
| Format-List
Name                          : Legal Recovery Ref 104
Status                        : Completed
StatusDetail                  : Completed
SyncStage                     : SyncFinished
Flags                         : IntraOrg, Pull
RequestStyle                  : IntraOrg
Direction                     : Pull
Protect                       : False
Suspend                       : False
SourceExchangeGuid            : d8f7a889-b430-4791-ad8c-360310f74b1c
SourceRootFolder              : Inbox
SourceVersion                 : Version 14.1 (Build 218.5)
SourceDatabase                : DB3 Recovery Database
MailboxRestoreFlags           : Disabled, Recovery
TargetAlias                   : LegalInvestigators
TargetIsArchive               : False
TargetExchangeGuid            : 73d598ff-a7ce-4542-8740-b6509424f139
TargetRootFolder              : Recovered Data
TargetVersion                 : Version 14.1 (Build 218.5)
TargetDatabase                : DB3
TargetMailboxIdentity         : contoso.com/Exchange Users/Legal Investigators
IncludeFolders                : {}
ExcludeFolders                : {}
ExcludeDumpster               : False
ConflictResolutionOption      : KeepSourceItem
AssociatedMessagesCopyOption : DoNotCopy
BadItemLimit                  : 5
BadItemsEncountered           : 0
QueuedTimestamp               : 6/3/2010 10:08:16 PM
StartTimestamp                : 6/3/2010 10:08:20 PM
```

```
LastUpdateTimestamp          : 6/3/2010 10:08:26 PM
CompletionTimestamp          : 6/3/2010 10:08:26 PM
TotalQueuedDuration          : 00:00:04
TotalInProgressDuration      : 00:00:05
MRSServerName                : ExServer1.contoso.com
EstimatedTransferSize        : 2.414 MB (2,531,099 bytes)
EstimatedTransferItemCount   : 62
BytesTransferred             : 2.881 MB (3,020,719 bytes)
ItemsTransferred             : 62
PercentComplete              : 100
```

Insidertipp: Aufräumen nach der Wiederherstellung

Es wäre unklug, eine Wiederherstellungsdatenbank an Ort und Stelle zu belassen, während sie mit Exchange verbunden ist oder während ihre Dateien auf der Festplatte zugänglich sind, sodass ein skrupelloser Administrator, der über die entsprechenden Berechtigungen verfügt, darauf zugreifen und sich den Inhalt der Postfächer darin ansehen kann. Nachdem Sie die erforderlichen Wiederherstellungsvorgänge ausgeführt haben, sollten Sie die Wiederherstellungsdatenbank daher entfernen und ihre Dateien von der Festplatte löschen.

Gehen Sie dazu folgendermaßen vor:

1. Heben Sie die Bereitstellung der Wiederherstellungsdatenbank auf.

```
Dismount-Database -Identity 'Sales Recovery Database' -Confirm:$False
```

2. Entfernen Sie die Wiederherstellungsdatenbank aus Exchange (mit der Exchange-Verwaltungskonsole oder -Verwaltungsshell).

```
Remove-MailboxDatabase -Identity 'Sales Recovery Database' -Confirm:$False
```

3. Löschen Sie die Datenbankdateien aus dem Wiederherstellungsspeicherort.

New-MailboxRestoreRequest ist kein genaues Äquivalent zu *Restore-Mailbox*, denn ihm fehlen einige der Betreff- und Inhaltsfiltermöglichkeiten, die es möglich machen, bestimmte Daten aus einer Wiederherstellungsdatenbank herauszufischen. Mit den beiden Cmdlets können Sie sich entscheiden, ob Sie interaktiv oder im Hintergrund arbeiten wollen. Es ist jedoch wahrscheinlich, dass Microsoft die fehlenden Funktionen schließlich zu *New-MailboxRestoreRequest* hinzufügt, sodass *Restore-Mailbox* aufgegeben werden kann.

Vollständige Serversicherungen

Der neue Schwerpunkt auf der Mobilität von Datenbanken und die Aufhebung der engen Bindung zwischen Datenbanken und Postfachservern hat auch Auswirkungen auf Sicherungen:

- Die Sicherungen werden volumeweise vorgenommen. Alle Datenbanken und Transaktionsprotokolle, die es in einem Volume gibt, werden in die Sicherung aufgenommen.

- Die Sicherungen dienen dazu, Datenbanken nach einem Festplatten- oder Serverausfall wiederherzustellen. Bei einem Serverausfall können Sie die Exchange-Konfigurationsdaten aus Active Directory wiedergewinnen, indem Sie das Exchange-Setupprogramm im Wiederherstellungsmodus ausführen (siehe Kapitel 2, »Installation von Microsoft Exchange Server 2010«). Anschließend müssen Sie dann in mehreren separaten Schritten die Daten auf dem Server wiederherstellen. Nur einer dieser Schritte betrifft jedoch die Wiederherstellung von Datenbanken.
- Es gibt keinen »Systemstatus«, der in den Exchange-Sicherungen aufgezeichnet wird. Um auch die Windows-Konfiguration eines Servers zu sichern, müssen Sie zusätzliche Maßnahmen ergreifen. Auch für die anderen auf dem Exchange Server-Computer installierten Anwendungen müssen Sie eigene Sicherungsverfahren durchführen.
- Was Exchange angeht, müssen die Sicherungen von Exchange Server-Computern, die nicht die Postfachrolle ausführen, lediglich die Konfigurationsdaten umfassen, die nicht in Active Directory festgehalten werden. Wenn Sie beispielsweise einige der *OWA.asp*-Dateien anpassen, müssen Sie Kopien davon anlegen, da diese Dateien bei der Wiederherstellung eines Clientzugriffsservers nicht berücksichtigt werden. Das Gleiche gilt auch für die Transportkonfigurationsdateien auf einem Hub-Transport-Server.

HINWEIS Die offensichtliche Schwierigkeit, vor die Administratoren durch die Änderungen in Exchange Server 2010 und die neue Vorgehensweise von Windows Server-Sicherung gestellt werden, ist die Tatsache, dass es keine vorgefertigte Komplettlösung gibt, um einen gesamten Server mit einer einzigen, allumfassenden Operation zu sichern. Die Wiederherstellung eines Postfachservers mit Exchange Server 2010 erfordert daher eine andere Planung als bei den vorhergehenden Versionen.

Wenn Konfigurationsdateien auf Hub-Transport- und Clientzugriffsservern geändert werden, so geschieht dies gewöhnlich nur einmalig. Die Konfigurationsdateien bleiben dann bis zur nächsten Softwareaktualisierung unberührt, weshalb es nicht notwendig ist, sie regelmäßig zu sichern. Allerdings müssen Sie eine Kopie aller geänderten Exchange-Konfigurationsdateien und jeglicher anderer manuell bearbeiteter Dateien erstellen und an einem sicheren Platz aufbewahren, um im Fall einer Serverwiederherstellung leicht darauf zugreifen können. Außerdem müssen Sie alle Änderungen, die Sie an Exchange-Dateien vornehmen, sorgfältig dokumentieren, damit auch andere Administratoren die Gründe für die Änderungen kennen und beurteilen können, ob es nach der Installation einer neuen Version, eines Service Packs oder einer Rollupaktualisierung nötig ist, diese Änderung erneut anzuwenden.

Clients

Nachdem die Hardware eingerichtet ist und Exchange reibungslos läuft, können wir uns jetzt darum kümmern, wie die Clients die Infrastruktur ausnutzen. Wenden wir unseren Blick daher Outlook, Outlook Web App und den anderen Clients zu, die Verbindung mit Exchange aufnehmen können.