

## Kapitel 16

# Wiederherstellung im Notfall

### In diesem Kapitel:

Sicherungs- und Wiederherstellungstechnologien	404
Sicherungs- und Wiederherstellungsstrategien	414
Empfohlene Vorgehensweisen	431
Zusammenfassung	432

Sicherung und Wiederherstellung von Exchange Server 2007-Datenbanken sind äußerst wichtige Aspekte der Exchange-Planung und -Konfiguration. Leider übersehen viele Organisationen, welche Bedeutung diesem Gebiet zukommt. Selbst wenn sie regelmäßig Sicherungskopien anlegen, kommt es vor, dass diese nicht ausreichend getestet werden.

Dieses Kapitel dreht sich um das Sichern und Wiederherstellen Ihrer Exchange Server 2007-Datenbanken. Im ersten Teil werden die Exchange-Datenbankarchitektur sowie die verschiedenen Arten der Sicherung und Wiederherstellung ausführlich behandelt. Der zweite Teil erörtert Methoden für die Implementierung üblicher Sicherungs- und Wiederherstellungsverfahren. Außerdem machen Sie sich mit den Werkzeugen vertraut, die oftmals als Hilfe bei der Implementierung und bei der Behebung von Problemen erforderlich sind.

## Sicherungs- und Wiederherstellungstechnologien

In diesem Abschnitt werden die Exchange-Datenbankarchitektur sowie die verschiedenen Arten der Sicherung und Wiederherstellung vorgestellt, die diese Architektur ermöglicht. Dabei kommen einige Merkmale von Exchange Server 2007 zur Sprache, beispielsweise die fortlaufende lokale Replikation (Local Continuous Replication, LCR) und die fortlaufende Clusterreplikation (Clustered Continuous Replication, CCR). Dabei handelt es sich um Protokollversandfunktionen, die implementiert werden, indem auf einem separaten Speicher (bei LCR auf demselben Server, bei CCR dagegen auf einem anderen Clusterknoten) ein Seeding eines Replikats der Datenbank durchgeführt wird und die geschlossenen Transaktionsprotokolle aus der Produktionskopie in das Replikat zurückgespielt werden, um es auf dem aktuellen Stand zu halten.

### Die Exchange-Datenbank

Die Hauptkomponente der Exchange-Postfachserverfunktion ist der Exchange-Informationsspeicher. Kenntnisse über ihn und die zugrunde liegende ESE-Datenbank (Extensible Storage Engine) bilden eine wichtige Voraussetzung, um zu verstehen, wie Sicherungen und Wiederherstellungen in Exchange Server 2007 funktionieren.

---

**HINWEIS**

Die ESE-Datenbank wurde bisher als Jet Blue bezeichnet (ist also eine andere Version als die von Microsoft Office verwendete Datenbank Jet Red).

---

### Grundlegende Architektur

Die von Exchange Server 2007 eingesetzte ESE-Datenbank ist dieselbe Version der B+-Baum-Datenbank, wie sie Exchange Server 2003 SP1 und Active Directory benutzen. Exchange Server 2007 implementiert sie mit einer Reihe von aktualisierten Attributen:

- Die Größe der Protokolldatei sinkt von 5 auf 1 MB.
- Die Seitengröße der Datenbank steigt von 4 auf 8 KB.

Diese Attribute sind erforderlich, um die integrierten Protokollversandfunktionen und ein flacheres E/A-Profil zu unterstützen. Die Protokollversandfähigkeiten (LCR und CCR) benötigen die kleineren Protokolldateien, um die möglichen Datenverluste auf kleinere Blöcke zu begrenzen. Das flachere

E/A-Profil wird durch eine Reihe von Exchange Server 2007-Funktionen erreicht und ermöglicht eine größere Anzahl von Benutzern pro Server als die früheren Versionen. Die Attribute sind wichtig für Konfiguration und Leistung und um Verständnis dafür zu entwickeln, was beim Sichern und Wiederherstellen vor sich geht.

## Transaktionen

Die Datenbanktransaktionen sind ACID-Operationen, d.h., sie sorgen dadurch für Integrität, dass sie atomar (A), konsistent (C), isoliert (I) und dauerhaft (D) sind.

- **Atomar** besagt, dass die Änderung eines Transaktionszustands ganz oder gar nicht stattfindet, was bedeutet, dass die gesamte Transaktion abgeschlossen sein muss, bevor irgendein Teil von ihr als abgeschlossen gelten kann. Atomare Zustandsänderungen umfassen die Neuordnung von Datenbankseiten, Ergänzungen der Postfachordneransicht und die Übertragung von E-Mails. Ohne den atomaren Charakter können vollständige Transaktionen nicht garantiert werden.
- **Konsistent** besagt, dass eine Transaktion eine korrekte Transformation des aktuellen Zustands der Datenbank darstellt. Die Aktionen verletzen als Gruppe keine der Integritätseinschränkungen, die mit dem aktuellen Zustand der Datenbank verknüpft sind. Ohne die Eigenschaft der Konsistenz wäre es möglich, dass während des normalen Betriebs beschädigte E-Mails in die Datenbank gelangen.
- **Isoliert** besagt, dass es für jede Transaktion so scheint, als ob andere entweder vor oder nach ihr ausgeführt würden, aber nicht beides, obwohl die Transaktionen in Wirklichkeit gleichzeitig stattfinden. Ohne diese Eigenschaft könnte ein Objekt als gelesen markiert werden, bevor es dem Postfach zugestellt wird.
- **Dauerhaft** besagt, dass die Änderungen durch eine Transaktion Ausfälle überstehen, sobald sie erfolgreich abgeschlossen ist (also per Commit in die Datenbank übernommen wurde). Dies bedeutet außerdem, dass die gesamte Transaktion zurückgenommen wird, wenn sie nicht in ihrer Gesamtheit abgeschlossen wurde (wenn also kein Commit für sie vorliegt). Ohne Dauerhaftigkeit wäre die Datenbank nach Strom- oder Serverausfall oder anderen inkonsistenten Zuständen nicht bis zur letzten E-Mail wiederherstellbar, die einem Postfach zugestellt wurde.

Die genannten Eigenschaften sind für Sicherungs- und Wiederherstellungsoperationen unverzichtbar. Ohne sie genießt der Exchange-Administrator nicht das Gefühl von Sicherheit, das durch die Seltenheit der Beschädigung von ESE-Datenbanken entsteht. Die Eigenschaften tragen dazu bei, die Einhaltung der folgenden Regeln zu gewährleisten:

- Exchange nimmt alle Änderungen (oder E-Mails) zurück, die nicht vollständig in der Datenbank angekommen sind.
- Exchange schenkt Seiten, die nicht in Ordnung sind, keine Beachtung, um Beschädigungen zu verhindern.
- Exchange akzeptiert keine Operationen, durch die die Datenbank nicht ohne Weiteres konsistent wird.
- Exchange lässt nur die Übernahme jeweils einer Transaktion in die Datenbank zu, obwohl mehrere gleichzeitige Transaktionen erlaubt sind, um die Leistung zu erhöhen.
- Exchange garantiert, dass eine Transaktion innerhalb der Datenbankdatei vollständig wiederherstellbar ist, sobald der Commitvorgang stattgefunden hat.

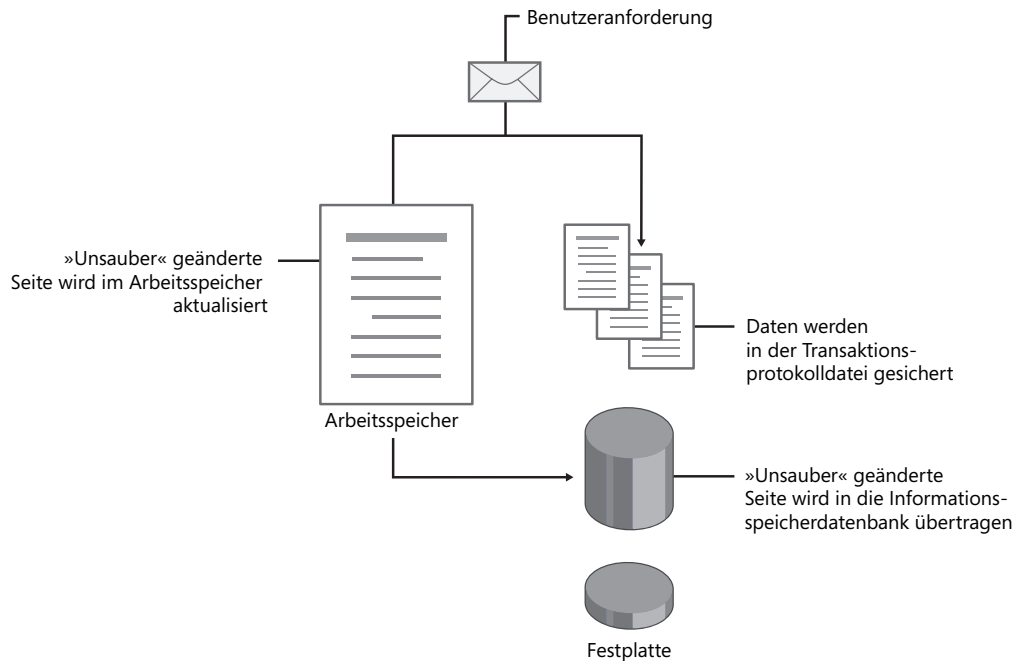
An diese Garantien müssen Sie unbedingt denken, wenn Sie ein Verfahren zum Sichern und Wiederherstellen beurteilen.

## Protokollierung

An welcher Stelle kommen nun all diese Protokolldateien ins Spiel? Das Grundprinzip hinter der ESE-Datenbank lautet, dass das Ablegen im Arbeitsspeicher kostengünstiger ist als das Speichern auf der Festplatte. Das ist seit den Anfängen von Exchange Server der Fall und wurde mit der Umstellung auf eine 64-Bit-Architektur in Exchange Server 2007 sogar noch verstärkt. Wenn Daten zuerst in den Arbeitsspeicher geschrieben und später auf die Festplatte übertragen werden, besteht das Problem darin, dass die im Arbeitsspeicher abgelegten Informationen zustandslos sind. Für Exchange bedeutet dies, dass der Commit und die Wiederherstellbarkeit der E-Mail nicht garantiert sind, solange sie sich im Arbeitsspeicher befindet. Um sicherzustellen, dass die Zustandslosigkeit kein Problem darstellt, wurden die Protokolldateien eingeführt, die dafür sorgen, dass alle Transaktionen aufgezeichnet werden, während sie in den Arbeitsspeicher geschrieben werden. Diese Vorgehensweise wird als *Zweiphasencommit* bezeichnet (siehe Abbildung 16.1).

- Phase 0: Schneller Commit der Transaktion des Benutzers  
Sequenzielles Schreiben der Änderungen an der Seite (Ändern, Löschen, Einfügen)
- Phase 1: Atomare Aktualisierung der Datenbank

Abbildg. 16.1 Zweiphasencommit



Um sich den Vorgang klarzumachen, nehmen Sie an, dass Benutzer 1 eine Nachricht von 2.500 KB (2,4 MB) an Benutzer 2 sendet, einen anderen Benutzer im selben Nachrichtenspeicher:

- Benutzer 1 sendet eine 2.500-KB-Nachricht.
- Im Arbeitsspeicher werden 312,5 8-KB-Seiten belegt.
- 2,44 Protokolldateien werden auf die Festplatte geschrieben.
- Die Nachricht von Benutzer 1 wird in dessen Outlook-Client als GESENDET registriert.

- Benutzer 2 empfängt eine Nachricht mit einem Zeiger auf den Datensatz im Arbeitsspeicher für die 312,5 Seiten, die die Nachricht enthalten.

Zu diesem Zeitpunkt ist die Nachricht gesendet; sie steht im Arbeitsspeicher und wurde sequenziell in eine Protokolldatei geschrieben. Mit der Aufnahme in die Protokolldateien befindet sie sich in einem halb wiederherstellbaren Zustand, weil der letzte Teil (die 0,44 MB) in einer offenen Protokolldatei steht. Außerdem ist sie nicht so gespeichert oder indiziert, dass sie später leicht auffindbar ist. Dazu muss sie in die Datenbank geschrieben werden. Die ESE-Datenbank verfügt über mehrere Methoden, Daten aus dem Arbeitsspeicher in die Datenbank zu übertragen:

- **Anomale Schreibvorgänge** Dies ist die häufigste Vorgehensweise von ESE. In diesem Szenario wurde eine Seite in den Arbeitsspeicher geschrieben, aber in letzter Zeit nicht angefordert. Eine solche Seite wird häufig als unsauber bezeichnet.
- **Schreibvorgänge bei Leerlauf** Schreibvorgänge dieser Art führt ESE am seltensten durch. In dieser Situation passiert auf dem Server nichts anderes und es gibt viele zusätzliche Zyklen, um Daten vom Arbeitsspeicher auf die Festplatte zu verlagern.
- **Rechtzeitige Schreibvorgänge** Sie sind in Exchange Server 2007 häufiger als in früheren Versionen. Hierbei werden Seiten geschrieben, die zwar möglicherweise nicht zum Schreiben bereit, aber für Datenbankseiten bestimmt sind, die einem schreibbereiten Vorgang benachbart sind. Dabei kann es sich um mehrere E-Mails für einen einzigen B+-Baum, zwei Anhänge für eine Anhangstabelle o.Ä. handeln.
- **Normale Schreibvorgänge** Merkwürdigerweise sind sie nicht normal. Sie treten auf, wenn die Prüfpunktiefe ihre Grenze erreicht hat (standardmäßig 20 MB pro Speichergruppe). Diese Situation kommt nur in einem stark belasteten System vor und sollte genau beobachtet werden. Außerdem bringt sie eine Verlangsamung der Sicherung während des Schreibens mit sich, weil sich die Datenbank vor dem Anlegen einer Kopie in einem wiederherstellbaren Zustand befinden muss.
- **Wiederholte Schreibvorgänge** Sie kommen nicht oft vor, denn eine Seite wird nur in Systemen mit hoher Auslastung mehrfach geschrieben. Dies bedeutet, dass sie im Arbeitsspeicher abgelegt und dann mit einer der vier vorstehenden Methoden auf die Festplatte übertragen wurde. Anschließend verschiebt sich der Prüfpunkt über diese Seite hinaus. Wird die Seite wiedergefunden – was voraussetzt, dass ein Benutzer eine Nachricht sofort geändert (bearbeitet, gelöscht o.Ä.) hat –, wird sie als wiederholt geschriebene Seite erkannt.

Sie müssen diese Konzepte unbedingt kennen, um zu verstehen, wie die ACID-Eigenschaften in der Datenbank implementiert werden und wie die verschiedenen Technologien mit dem Charakter der ESE-Datenbank in Konflikt geraten können. Eine Technologie, die Daten im Arbeitsspeicher sichert, ist beispielsweise nicht gut, weil die betreffenden Seiten aktualisiert, gelöscht oder verworfen werden können, bevor sie es überhaupt in die Datenbank schaffen.

## Umlaufprotokollierung

Die *Umlaufprotokollierung* soll den Speicherbedarf für die Transaktionsprotokolle reduzieren, nachdem die aufgezeichneten Transaktionen per Commit in die Datenbank übernommen wurden. Sie wird für Produktions-Mailsysteme im Allgemeinen nicht empfohlen. In ESE-Implementierungen, bei denen die Wiederherstellbarkeit einer einzelnen Datenbank nicht absolut erforderlich ist (beispielsweise für Active Directory oder die Exchange-Funktion des Hub-Transport-servers) wird sie wegen der Art, wie sie die Protokolldateien nach dem Commit behandelt, standardmäßig eingesetzt. Bei aktiver Umlaufprotokollierung werden die Protokolle nach der Übernahme in die Datenbank aus dem System gelöscht, was dazu führt, dass sich immer nur wenige Protokolle auf dem System befinden. Es bedeutet außerdem, dass Sie während einer Wiederherstellung keinen Rollforward der

Datenbank durchführen können, weil bei einer vollständigen Sicherung die Protokolle nicht gesichert werden. Glücklicherweise ist die Umlaufprotokollierung außer auf Edge- und Hub-Transport-Servern standardmäßig deaktiviert. Diese Serverfunktionen enthalten weitgehend kurzlebige Daten und erfordern es in den meisten Fällen nicht, dass Sicherungen von ihnen angelegt werden.

## Prüfsummen

Die *Prüfsumme* (auch Nachrichten-Hash genannt) ist ein String, der berechnet und dann jeder Seite der Datenbank hinzugefügt wird, um die Integrität der Seite zu dokumentieren. Dabei garantiert sie die Integrität nicht selbst. Statt dessen gewährleistet die Neuberechnung der Summe beim Einlesen der Seite in den Arbeitsspeicher, dass die aus der Datenbank gelesenen Daten mit denen identisch sind, die in die Datenbank geschrieben wurden.

Wenn eine Seite in den Arbeitsspeicher geladen wird, wird die Prüfsumme berechnet und die Seitennummer überprüft. Stimmt die Prüfsumme nicht mit der überein, die beim Speichern in der Datenbank auf der Seite abgelegt wurde, können Sie sicher sein, dass die Seite beschädigt oder verfälscht ist. ESE ignoriert oder korrigiert einfache Fehler durch *umgekippte Bits*, also solche, bei denen ein einzelnes Bit als 1 anstatt als 0 geschrieben wird. Der Fehler wird ignoriert, wenn er in Verbindung mit einer manuellen Prüfung der Summe festgestellt wird (zum Beispiel bei einer Sicherung durch den Volumenschattenkopie-Dienst [Volume Shadow Copy Service, VSS]).

Beachten Sie, dass ESE den Schaden an der Seite nicht verursacht, sondern nur meldet. In fast allen Fällen ist die Beschädigung der Datenbank das Ergebnis der Fehlfunktion eines Hardwaregeräts oder Gerätetreibers. ESE kann keine Beschädigungen auf Seitenebene verursachen. Sie treten auf, wenn die Daten auf die Festplatte geschrieben werden, und sind auf Ihre Hardware oder Ihre Gerätetreiber zurückzuführen. Deshalb müssen Sie unbedingt dafür sorgen, dass Ihre gesamte Firmware und Ihre Gerätetreiber über die neuesten Patches und Aktualisierungen verfügen und die gesamte Hardware die WHQL-Tests bestanden hat. Der Microsoft-Kundendienst wird zusammen mit Ihrem Hardwarehersteller alle Probleme lösen, die möglicherweise zwischen Ihrer Hardware und Ihrer Exchange Server 2007-Datenbank bestehen.

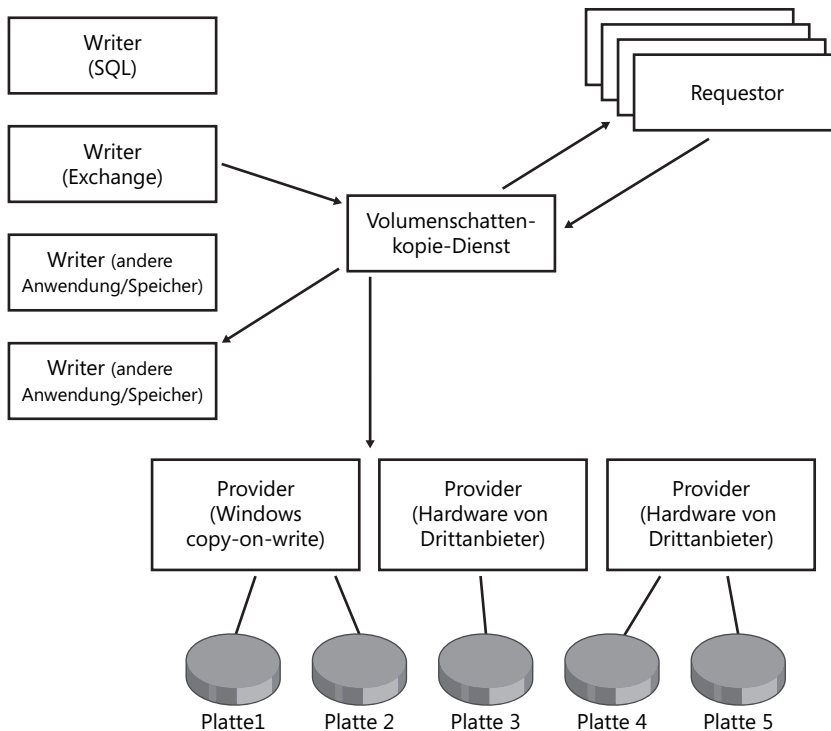
## Der Volumenschattenkopie-Dienst

Der Volumenschattenkopie-Dienst (VSS) ist eine übliche Methode, die zum Sichern und Wiederherstellen von Exchange Server 2007 eingesetzt wird. Alle Sicherungen auf VSS-Basis werden als Online-sicherungen betrachtet, weil sie voraussetzen, dass während des Vorgangs der Exchange-Informationsspeicher läuft. Sie stützen sich in hohem Maß auf den Virtual Disk Service (VDS) und das Windows-VSS-Framework. Dieses Framework beruht auf folgenden Voraussetzungen:

- Windows stellt ein Framework bereit, das regelt, wie Anwendungen gesichert werden. Dies ist möglich, weil es alle Komponenten versteht, die unter dem Betriebssystem ausgeführt werden.
- Anwendungen stellen Writer bereit, die regeln, wann die Anwendung zum Anlegen einer Sicherungskopie bereit ist. Dies ist möglich, weil der Writer die Anwendung versteht.
- Microsoft und Drittanbieter stellen Requestoren bereit, die mit einer Anwendung für die Gesamt-sicherung zusammenarbeiten. Dies ist möglich, weil der Requestor versteht, wie die Sicherungsanwendung funktioniert, und weiß, welche Daten sie benötigt, um erfolgreich zu sein.
- Microsoft und Drittanbieter stellen Hard- und Software bereit, die verstehen, wie Speicherarrays synchronisiert und die Volumens anschließend aufgeteilt werden können.

Aus diesen vier Komponenten ergibt sich schließlich eine Lösung, in der ein Requestor Windows auffordert, eine Umgebung einzurichten, in der ein VSS-Snapshot erstellt werden kann. Anschließend fordert er den Writer der Anwendung auf, einen Snapshot der Anwendung einzurichten. Der Writer fordert seinerseits den Provider auf, auf der Grundlage irgendeiner von ihm unterstützten Technologie einen Snapshot einzurichten. Sind alle Puzzleteile zusammengefügt, teilt der Writer dem Requestor mit, zu welchem Zeitpunkt die Anwendung seiner Entscheidung nach für einen Snapshot bereit ist. Für Exchange bedeutet dies, dass der aktuelle Vorgang, mit dem Seiten auf die Festplatte geschrieben wurden, abgeschlossen ist und in der Datenbank keine neuen Transaktionen gestartet wurden. Diese Pause in der Aktivität darf nur zehn Sekunden dauern, während der Provider seinen Snapshot der Daten anfertigt. Ist der Snapshot abgeschlossen, informiert der Requestor den Writer, dass alles gut gelaufen ist und die Transaktionsverarbeitung wieder aufgenommen werden kann. Zu diesem Zeitpunkt hat der Provider eine Kopie der Datenbank und der Protokolldateien erhalten. Dann arbeitet der Provider mit dem Requestor zusammen, um sicherzustellen, dass die Datenbank auf Konsistenz geprüft wird und die Protokolle auf dem Produktionsdatenträger abgeschnitten werden. Damit Sie sich dies besser vorstellen können, zeigt Abbildung 16.2 ein Diagramm dieses Vorgangs.

Abbildg. 16.2 Das VSS-Framework (Volumenschattenkopie-Dienst)



## Unterstützte Typen von VSS-Sicherungen

Die verfügbaren Requestoren unterscheiden sich in ihrer Funktionalität und darin, welche VSS-Funktionen sie unterstützen. Das VSS-Framework unterstützt beispielsweise alle Standardsicherungsmethoden: vollständige, differenzielle, inkrementelle und Kopiesicherung; die meisten Anbieter implementieren jedoch nur die vollständige und die differenzielle Sicherung. Dieser Abschnitt beschreibt, was bei den einzelnen Typen geschieht.

### Vollständige Sicherung

Der Datenträger oder die Datei mit der Datenbank wird mithilfe von Hard- oder Software auf einen anderen Speicherort gespiegelt.

1. Der Exchange-Writer informiert den Requestor, wann er für einen Snapshot bereit ist.
2. Der Requestor hat zehn Sekunden, um den Snapshot aufzunehmen. Dies umfasst das Spiegeln der verbleibenden Blöcke in der Datenbank oder auf dem Datenträger, die nicht synchron sind, und das Trennen der Beziehung.
3. Anschließend ist der Requestor dafür zuständig, die Spiegelung an einem anderen Ort bereitzustellen, um eine Prüfsumme der Datenbank zu bilden. Dies geschieht mithilfe einer Prüfsummen-API oder mit dem Befehl `eseutil.exe /k`. Je nach Größe der Datenbank kann dieser Vorgang langwierig sein und das Speicherteilsystem mit einer Folge von sequenziellen Lesevorgängen in Anspruch nehmen. Er kann gedrosselt werden, um die Beanspruchung zu verringern, muss jedoch abgeschlossen sein, bevor die Protokolldateien abgeschnitten werden können.

### Inkrementelle Sicherung

Der Datenträger oder die Datei mit dem Protokoll wird mithilfe von Hard- oder Software auf einen anderen Speicherort gespiegelt.

1. Der Exchange-Writer informiert den Requestor, wann er für einen Snapshot bereit ist.
2. Der Requestor hat zehn Sekunden, um den Snapshot aufzunehmen. Dies umfasst das Spiegeln der verbleibenden Protokolldatei oder der Blöcke auf dem Datenträger der Protokolldatei, die nicht synchron sind, und das Trennen der Beziehung.
3. Die Datenbankdateien bleiben unberührt und werden erst bei der nächsten vollständigen Sicherung berücksichtigt. Jede inkrementelle Sicherung, die angelegt wird, enthält also sämtliche Protokolldateien seit der letzten vollständigen oder inkrementellen Sicherung. Für die Wiederherstellung werden nur die letzte vollständige und die letzte inkrementelle Sicherung benötigt.

### Differenzielle Sicherung

Der Datenträger oder die Datei mit dem Protokoll wird mithilfe von Hard- oder Software auf einen anderen Speicherort gespiegelt.

1. Der Exchange-Writer informiert den Requestor, wann er für einen Snapshot bereit ist.
2. Der Requestor hat zehn Sekunden, um den Snapshot aufzunehmen. Dies umfasst das Spiegeln der verbleibenden Protokolldatei oder der Blöcke auf dem Datenträger der Protokolldatei, die nicht synchron sind, und das Trennen der Beziehung.

Der Unterschied besteht darin, dass bei der differenziellen Sicherung die seit der letzten Sicherung angelegten Protokolldateien nicht abgeschnitten werden. Jede differenzielle Sicherung, die angelegt wird, enthält also nur die Protokolldateien seit der letzten vollständigen oder inkrementellen Sicherung. Für die Wiederherstellung werden die letzte vollständige und alle folgenden differenziellen Sicherungen benötigt.

### Kopiesicherung

Die Kopiesicherung läuft ähnlich ab wie eine vollständige. Der Unterschied besteht darin, dass die Protokolldateien nicht abgeschnitten werden.



## Die Exchange-Streamingsicherung-API

Die Exchange-Streamingsicherung-API gibt es seit Exchange Server 5.5. Sie wurde leicht aktualisiert, blieb aber weitgehend unverändert, um die Sicherungsanwendungen zu unterstützen, die sie nutzen. Die mit ihrer Hilfe angelegten Sicherungen werden als Streamingsicherungen bezeichnet. Es handelt sich ebenfalls um Onlinesicherungen, weil sie voraussetzen, dass der Exchange-Informationsspeicher läuft. In Exchange Server 2007 benötigte die ausgereifte Streaming-API keinerlei Aktualisierungen. Um sie einzusetzen, starten Sie einfach die Sicherungsanwendung. Diese informiert ESE, dass sie in einen Sicherungsmodus wechselt, woraufhin für jede betroffene Datenbank eine Patchdatei (PAT) angelegt wird (vorausgesetzt, es handelt sich um eine vollständige Sicherung). Während einer vollständigen Onlinesicherung steht die Datenbank für Geschäftsvorgänge zur Verfügung, und Transaktionen können in die Datenbanken aufgenommen werden. Wenn eine Transaktion eine geteilte Operation über die Sicherungsgrenze (die Stelle in der EDB-Datei, die besagt, was bereits gesichert wurde und was noch nicht) hinaus veranlasst, wird die Seite, die vor der Grenze liegt, in der PAT-Datei festgehalten. Für jede Datenbank in der Sicherung wird eine eigene PAT-Datei verwendet, etwa **Priv1.pat** oder **Pub1.pat**. Diese Dateien kommen nur während einer Sicherung oder Wiederherstellung vor. Bei differenziellen oder inkrementellen Sicherungen gibt es keine PAT-Dateien.

Wenn ESE in einen Sicherungsmodus wechselt, wird eine neue Protokolldatei geöffnet. Heißt die aktuelle Protokolldatei beispielsweise **Edb.log**, wird sie geschlossen und in die letzte Generation umbenannt, und eine neue Datei mit dem Namen **Edb.log** wird geöffnet. Dies ist der Augenblick, in dem ESE die Protokolldateien abschneiden kann, nachdem die Sicherung abgeschlossen ist.

Zu Beginn fordert die Sicherungsanwendung ESE auf, die Seiten einzulesen und in eine Reihenfolge zu bringen. Anschließend werden die Seiten in Blöcke zu 64 KB (8 Seiten) unterteilt und in den Arbeitsspeicher geladen. Dann prüft ESE die Prüfsummen der einzelnen Seiten, um die Integrität der Daten sicherzustellen. Stimmt die errechnete Prüfsumme einer Seite nicht mit der beim Schreiben auf die Festplatte aufgezeichneten überein, untersucht der Informationsspeicher, ob es sich um einen Fehler durch ein einzelnes umgekipptes Bit handelt (ob also ein Bit 1 ist, wenn es 0 sein müsste, oder umgekehrt). In diesem Fall wird versucht, den Fehler zu korrigieren. Andernfalls wird der Sicherungsvorgang angehalten und eine Fehlermeldung in die Ereignisprotokolle aufgenommen. Die Sicherungsanwendung verhindert auf diese Weise, dass beschädigte Daten aufgezeichnet werden.

Außerdem nimmt die Sicherungs-API diese Gelegenheit wahr, um die Seiten zu bereinigen, wenn das Flag »Gelöschte Seiten eliminieren« gesetzt ist. Dies geschieht nur bei einer Online-Streamingsicherung, und erst nachdem die Originaldaten in den anderen Speicher verschoben wurden, überschreibt die Streaming-API Seiten, die keine Verweise von anderen Seiten enthalten (beispielsweise Indizes und Mailobjekte), mit einer Reihe alphanumerischer Zeichen. Das Schöne daran ist, dass Sie nach einer erfolgreichen Onlinesicherung Ihrer Exchange-Datenbanken mithilfe des Exchange-Agents von Ihrem Softwareanbieter sicher sein können, dass die Datenbank auf Ihrer Plattenbibliothek oder Ihrem Band vollkommene Integrität aufweist, weil die Gesamtheit der Seiten in den Arbeitsspeicher eingelesen, die Prüfsumme berechnet und die Datenbank dann auf Platte oder Band kopiert wurde. Es ist auch etwas anderes als eine VSS-Sicherung, bei der die Prüfsummen der einzelnen Seiten nicht überprüft werden. Als Administrator sollten Sie dies bei der Planung eines Verfahrens für die Sicherung bedenken.

Nachdem die Sicherung erfolgreich abgeschlossen ist und alle Seiten gelesen wurden, kopiert die Sicherungs-API die Protokolle und die Patchdateien in den Sicherungssatz. Anschließend werden die Protokolldateien an dem Punkt abgeschnitten oder gelöscht, an dem die neue Generation zu Beginn der Sicherung eingesetzt hat. Der Sicherungssatz wird geschlossen, ESE wechselt in den Normalmodus und die Sicherung ist fertig.

Eine inkrementelle oder differenzielle Sicherung betrifft nur die Protokolldateien. Es werden keine Operationen ausgeführt, die Patchdateien, Prüfsummen oder das sequenzielle Einlesen von Seiten umfassen.

Zur Erinnerung noch einmal die Schritte einer vollständigen Sicherung:

1. Die Sicherung startet, ein Synchronisierungspunkt wird fixiert und eine leere Patchdatei angelegt.
2. Die Datei **Edb.log** bekommt ohne Rücksicht darauf, ob sie voll ist oder nicht, die nächste Protokollnummer und es wird eine neue Datei mit dem Namen **Edb.log** angelegt.
3. Die Sicherung für die aktuelle Speichergruppe beginnt.
4. Für jede zu sichernde Datenbank in der Speichergruppe wird eine PAT-Datei angelegt, in die der Datenbankheader geschrieben wird.
5. Während der Sicherung werden geteilte Operationen, die über die Sicherungsgrenze hinausgehen, in der PAT-Datei abgelegt.
6. Während der Sicherung kopiert Windows Server 2003 Backup immer 64 KB Daten auf einmal. Zusätzliche Transaktionen werden wie üblich erstellt und gespeichert. Die Prüfsummen der einzelnen Seiten werden berechnet und mit den jeweils aufgezeichneten verglichen, um die Integrität der Daten zu gewährleisten.
7. Sieht die Konfiguration der Datenbank vor, dass gelöschte Seiten überschrieben werden, so erfolgt dies sie mit einer Reihe alphanumerischer Zeichen.
8. Das während der Sicherung verwendete Protokoll (ab dem Prüfpunkt) und die Patchdateien werden auf Festplatte oder Band kopiert.
9. Sieht die Konfiguration der Datenbank vor, dass gelöschte Seiten überschrieben werden, so werden die überschriebenen Seiten auf der Festplatte abgelegt.
10. Die alten Protokolle auf der Festplatte werden gelöscht.
11. Die alten Patchdateien auf der Festplatte werden gelöscht.
12. Die Sicherung ist abgeschlossen.

## Unterstützte Typen von Streamingsicherungen

Die Streamingsicherungsprogramme können Exchange-Datenbanken mit einer Reihe von Standardmethoden sichern. Windows Backup nutzt sämtliche Funktionen und kann bei einem Wiederherstellungsverfahren eingesetzt werden. Andere Anwendungen fügen weitere anbieterspezifische Funktionen hinzu. Dieser Abschnitt beschreibt, was bei den einzelnen Ereignissen geschieht.

### Vollständige Sicherungen

1. Die Sicherungsanwendung startet und informiert ESE über die Sicherung; für jede betroffene Datenbank wird eine Patchdatei angelegt. Eine neue Protokollgeneration wird eröffnet, um eingehende Datenbankanforderungen entgegenzunehmen.
2. Die Sicherungsanwendung liest die Datenbankdatei seitenweise in den Arbeitsspeicher ein. Dabei wird die Prüfsumme verifiziert und das Flag »Gelöschte Seiten eliminieren« geprüft.
3. Gibt es nicht korrigierbare Fehler vom Typ -1018 oder -1022, hält die Datenbank auf den betreffenden Seiten an, sodass die Sicherung nicht fortgesetzt wird.
4. Sind Seiten bei gesetztem Flag »Gelöschte Seiten eliminieren« zum Löschen markiert, werden sie mit einer Reihe alphanumerischer Zeichen überschrieben und auf der Festplatte abgelegt.
5. Nachdem die gesamte Datenbank die Schritte 1 bis 4 durchlaufen hat, werden die Datenbank, die Patchdatei und die Protokolle auf das Sicherungsmedium kopiert, die Protokolle bis zu der in Schritt 1 begonnenen Generation abgeschnitten und der Datenbankheader unter der Überschrift »Sicherung abgeschlossen« mit einem aktuellen Zeitstempel aktualisiert.

**Inkrementell**

1. Die Sicherungsanwendung startet und informiert ESE über die Sicherung. Eine neue Protokollgeneration wird eröffnet, um eingehende Datenbankanforderungen entgegenzunehmen.
2. Die Anwendung liest die Protokolldateien auf der Festplatte und kopiert sie auf das Sicherungsmedium.
3. Nachdem sämtliche Protokolle bis zu der in Schritt 1 begonnenen Generation kopiert sind, werden die Protokolle abgeschnitten, und die Sicherung ist abgeschlossen.

**Differenziell**

1. Die Sicherungsanwendung startet und informiert ESE über die Sicherung. Eine neue Protokollgeneration wird eröffnet, um eingehende Datenbankanforderungen entgegenzunehmen.
2. Die Anwendung liest die Protokolldateien auf der Festplatte und kopiert sie auf das Sicherungsmedium.
3. Nachdem sämtliche Protokolle bis zu der in Schritt 1 begonnenen Generation kopiert sind, ist die Sicherung abgeschlossen.

**Kopie**

Eine Kopiesicherung läuft ähnlich ab wie eine vollständige Sicherung. Sie unterscheidet sich dadurch, dass die Protokolldateien nicht abgeschnitten werden.

**Der Wiederherstellungsvorgang**

Bevor Sie mit dem Wiederherstellen beginnen, müssen Sie die Bereitstellung der Datenbanken aufheben, um sie für die Benutzer unzugänglich zu machen. Dazu können Sie die Exchange-Verwaltungskonsole oder die Exchange-Verwaltungsshell benutzen.

Zu Beginn einer Wiederherstellungsoperation informiert der Speicher ESE, dass der Vorgang beginnt, sodass ESE in den Wiederherstellungsmodus wechselt. Der Sicherungs-Agent kopiert die Datenbank direkt vom Band in den Zielpfad. Die zugehörigen Protokoll- und Patchdateien werden an einen von Ihnen festgelegten temporären Ort auf dem Server kopiert, sodass sie nicht am selben Ort gespeichert werden wie aktuelle Dateien in der Produktionsumgebung. Würden Sie den Produktionspfad als temporären Pfad wählen, könnten Sie Protokolldateien überschreiben, was zu einer logischen Beschädigung der aktuellen Produktionsdatenbank führt. Achten Sie also darauf, dass der temporäre Pfad nicht Ihr Produktionspfad ist.

Nachdem die Protokoll- und Patchdateien am temporären Ort wiederhergestellt sind, muss zum Wiederherstellen der Datenbank eine neue Speichergruppe angelegt werden. Danach wird die Datenbank vom Band an den temporären Ort (und in die Wiederherstellungsspeichergruppe) kopiert. Anschließend kopiert das Modul für die Datenbankwiederherstellung die Daten der Patchdatei und die Protokolldateien vom Band in die Datenbank.

ESE verarbeitet die aktuellen Protokolle, was Sie an den Zeitpunkt der Datenbanksicherung zurückbringt (vorausgesetzt, alle Transaktionsprotokolle seit der letzten erfolgreichen Onlinesicherung bis zum Auftreten des Notfalls sind verfügbar). Danach führt ESE eine gewisse Bereinigung durch, indem es Protokoll- und Patchdateien aus dem temporären Pfad sowie die Speicherinstanz zum Wiederherstellen löscht. Anschließend werden die Speichergruppe und auch Ihre Datenbank für die Produktionsumgebung bereitgestellt.

## Andere Exchange Server-Komponenten

Außer der Exchange-Datenbank müssen einige weitere Komponenten in die Sicherungsplanung einbezogen werden. Einige davon kommen bei mehreren Serverfunktionen vor und lassen sich auf ähnliche Weise sichern und wiederherstellen. Eine Sicherung des Systemzustands ist beispielsweise für alle Serverfunktionen sinnvoll. Andere gibt es nur bei bestimmten Serverfunktionen, sodass die Sicherung nur dort sinnvoll ist. In Tabelle 16.1 können Sie nachlesen, welche Exchange Server-Komponenten gesichert werden sollten.

**Tabelle 16.1** Weitere zu sichernde Serverkomponenten

Serverfunktion	Zu sichernde Daten	Ort/Methode
Postfach	Datenbank und Protokolle für Postfach und öffentliche Ordner Inhaltsindex Systemeinstellungen	Streaming- oder VSS-Sicherung Keine Sicherung erforderlich, Index bei Wiederherstellung neu anlegen Sicherung des Systemzustands
Hub-Transport	Systemeinstellungen	Sicherung des Systemzustands
Clientzugriff	Konfiguration des Clientzugriffs (IMAP-Einstellungen, Verfügbarkeitsdienste usw.) Exchange ActiveSync-Konfiguration Webdienste-Konfiguration AutoErmittlungsdienst-Konfiguration Systemeinstellungen	\\ClientAccess\*. * Sicherung des Systemzustands
Edge-Transport	ADAM-Anpassungen Systemeinstellungen	Clone Config (ExportEdgeConfig.ps1) Sicherung des Systemzustands

Weitere Informationen finden Sie auf der Microsoft-Website unter der Adresse <http://technet.microsoft.com/en-us/library/bb124780.aspx>.

## Sicherungs- und Wiederherstellungsstrategien

Ihre Wiederherstellungsstrategie bestimmt Ihre Sicherungsstrategie; sie können nicht unabhängig voneinander geplant werden. Überlegen Sie bei der Auswahl des günstigsten Sicherungsverfahrens für Ihre Umgebung zuerst, wie und wo die Wiederherstellung erfolgt. Dieser erste Schritt führt Ihre Planung auf einen Weg, der besser zu Ihrer Umgebung und den Gesamterfordernissen passt, als wenn Sie zuerst über die Sicherung nachdenken.

Wie muss die Datenbanksicherung zum Beispiel im Fall der Wiederherstellung zur Verfügung stehen? Sie kann als Datei auf Band vorliegen, die sich an einen Produktionsort kopieren lässt. Sie kann als Festplatte vorliegen, die an einen Produktionsort gespiegelt werden kann. Sie kann in Form mehrerer Dateien auf einer Festplatte oder auf mehreren Festplatten vorliegen. Es kommt darauf an, sich zu überlegen, welche Art der Wiederherstellung für die meisten vorstellbaren Situationen sinnvoll ist.

Sie müssen für ausreichend Speicherplatz sorgen, um sowohl die Datenbank als auch die Protokolldateien wiederherstellen zu können. Legen Sie innerhalb einer Woche 2.000 Protokolldateien an, müssen Sie im Notfall 2 GB Daten wiederherstellen. Wenn Sie das zur Größe Ihrer Datenbanken addieren, werden Sie verstehen, warum Sie Ihre Wiederherstellungsstrategie in Verbindung mit der Sicherungsstrategie planen müssen.

Neben den technischen Überlegungen zum Sichern und Wiederherstellen spielen auch Serviceverträge über Sicherungs- und Wiederherstellungszeiten sowie die Verfügbarkeit des Mailsystems eine wichtige Funktion. Bei der Planung der Wiederherstellungsmethoden müssen diese geschäftlichen Anforderungen zwingend berücksichtigt werden. Die Verträge müssen den Bedarf aller Benutzer des Exchange-Systems erfüllen. Dazu zählen einzelne Nutzer, Anwendungen und Geschäftsprozesse. Angesichts dieses umfangreichen Benutzerspektrums in der Exchange-Umgebung lassen sich nur schwer Vereinbarungen treffen, und die Komplexität des Systems nimmt zu. Sehen Sie sich als anhaltspunkt die Werteskala für Serviceverträge in Tabelle 6.2 an.

**Tabelle 16.2** Werteskala für Serviceverträge

Vertrag	Standard-Höchstwert*	Premium- Höchstwert*	Tatsächlich beobachtet
Verfügbarkeit des Exchange-Dienstes	99,999% Montag – Freitag 7–18 Uhr	99,999% Montag – Sonntag 0–24 Uhr	99,99875%
Verfügbarkeit des Mobildienstes	99,999% Montag – Freitag 7–18 Uhr	99,999% Montag – Sonntag 0–24 Uhr	99,997%
Verfügbarkeit der Anwendungsweiterleitung	99,999% Montag – Freitag 7–18 Uhr	99,999% Montag – Sonntag 0–24 Uhr	100%
Verfügbarkeit des Outlook-Clients	99,999% Montag – Freitag 7–18 Uhr	99,999% Montag – Sonntag 0–24 Uhr	100%
Verfügbarkeit von Outlook Web Access	99,999% Geschäftszeit	99,999% Montag – Sonntag 0–24 Uhr	99,98%
Wiederherstellen eines einzelnen Postfachs	4 Stunden	1 Stunde	2 Stunden
Wiederherstellen einer Postfachdatenbank	4 Stunden	1 Stunde	2 Stunden
Wiederherstellen eines Postfachservers	5 Stunden	2 Stunden	7 Stunden
Aufspüren von Daten (E-Discovery) einem einzelnen Postfach	5 Tage	2 Tage	3 Tage
Wiederherstellen eines Postfachobjekts	1 Woche	1 Woche	5 Tage
* Standard ist definiert pro Benutzer für alle, die den Standardpreis bezahlen			
** Premium ist definiert pro Benutzer für alle, die für besseren Service mehr als den Standardpreis bezahlen			

Durch eine Analyse der Anforderungen an Wiederherstellung und Verfügbarkeit lässt sich leicht ermitteln, welche technische Architektur erforderlich ist. Einen kritischen Bereich bildet die Festlegung der Größe von Postfächern und Datenbanken. Beachten Sie, dass die Wiederherstellung eines einzelnen Postfachs und die Wiederherstellung einer Postfachdatenbank getrennt aufgeführt sind. Das ist normal und auf die Größe des Postfachs und die Anzahl der Benutzer einer einzelnen Postfachdatenbank zurückzuführen. Es gibt mehrere Methoden, die Exchange-Konfiguration so einzusetzen, dass sie verschiedene Serviceverträge erfüllt. Meistens werden die Größe der Postfächer und die Anzahl der Benutzer pro Datenbank verwendet. Diese beiden Komponenten definieren die Datenbankgröße und die damit verbundenen Sicherungs- und Wiederherstellungszeiten pro Server. Sehen Sie sich zum Beispiel die durchschnittliche Wiederherstellungszeit eines Servers an. Nehmen wir mehrere Server mit jeweils fünf Datenbanken (pro Speichergruppe eine), 100 Benutzern pro Datenbank und einer Postfachbegrenzung von 400 MB an, dann umfasst jede Datenbank etwa 47 GB. Kommt es darauf an,

wie lange die Wiederherstellung des gesamten Servers dauert, stellen die Reduzierung der Benutzeranzahl pro Server oder der Postfachgröße pro Benutzer gute Möglichkeiten dar. In beiden Fällen müssen Sie eine Defragmentierung außerhalb des laufenden Betriebs durchführen, um die physische Größe der Datenbank zu verringern. Steht dagegen die Anzahl der Server im Mittelpunkt, kann eine Konsolidierung vorgenommen werden, die alle Benutzer auf einem einzigen Server unterbringt, indem Sie die Anzahl der Speichergruppen und Datenbanken für den einzelnen Server erhöhen. Dadurch verlängert sich die Zeit für die Wiederherstellung des Servers, aber die Zeit für die Wiederherstellung einer einzelnen Postfachdatenbank bleibt dieselbe. Dies ist eine wesentliche Grundlage für die Planung der Servergröße.

Weitere Informationen zur Speicherplanung finden Sie unter der Adresse <http://technet.microsoft.com/en-us/library/c5a9c0ed-e43e-4bc7-99fe-7d1a9cb967f8.aspx>.

### Die Wiederherstellungsmöglichkeiten testen

Regelmäßiges Testen der Wiederherstellung von Sicherungen löst für Organisationen drei wichtige Probleme. Das erste ist, dass das technische Personal die erforderliche Vertrautheit mit den Wiederherstellungstechniken und -fähigkeiten behält, die normalerweise nur im Notfall eingesetzt werden. Das zweite ist die vollständige Überprüfung der Systemsicherung, das dritte das Erkennen von Problemen im Sicherungsverfahren, die sonst nur bei einem echten Notfall ans Licht kämen.

Alle drei Probleme werden mit einer einzigen Wiederherstellung in regelmäßigem Turnus abgedeckt. Es wird empfohlen, mindestens einmal pro Quartal eine vollständige Wiederherstellung zu testen. Dabei können jedes Mal andere Mitarbeiter eingesetzt oder andere Dienste getestet werden (zum Beispiel einmal die Wiederherstellung eines Postfachs und das nächste Mal ein Cluster-Failover). Auf diese Weise stören die Wiederherstellungstests weder andere Projekte noch den täglichen Betrieb, bleiben aber trotzdem ein wichtiger Bestandteil der regelmäßigen Aktivitäten.

Am häufigsten wird der Postfachserver wiederhergestellt. Er bildet die Kernkomponente von Exchange Server 2007 und ist der wichtigste Server, der bei einem Ausfall eines Standorts oder der Hauptplatine eines einzelnen Servers wiederhergestellt werden muss. Aus diesem Grund spielen Sie beim Testen dieser Art von Wiederherstellung ein häufiges Szenario durch.

Es gibt zwei allgemein empfohlene Methoden für die Wiederherstellung von Exchange Server 2007. Die erste stellt alle Datenbanken eines ausgefallenen Servers auf einem ähnlichen Server wieder her, die zweite benutzt dazu die verbleibenden Postfachserver der Umgebung. Die erste Option ähnelt den Wiederherstellungstechniken früherer Exchange Server-Versionen, während die zweite mit Exchange Server 2007 neu eingeführt wurde. Die erste Möglichkeit wird vorgeschrieben; doch ihre Techniken sind auch bei der zweiten anwendbar.

Ein Merkmal von Exchange Server 2007, die so genannte Datenbankportabilität, ermöglicht das Portieren von Exchange Server 2007-Datenbanken zwischen Exchange Server-Computern derselben Exchange-Organisation. Damit lässt sich eine Exchange-Datenbank in der Speichergruppe 1 mit dem Namen **DB1** auf einem Server **Exch1** heruntergefahren (oder anderweitig konsistent machen), in die Speichergruppe 2 auf dem Server **Exch2** verlegen und ohne weitere Aktionen oder Modifikationen bereitstellen. Damit dies funktioniert, müssen Sie zunächst in der Speichergruppe 2 auf dem Server **Exch2** eine Platzhalterdatenbank anlegen und die Option **Diese Datenbank kann bei einer Wiederherstellung überschrieben werden** aktivieren. ►

### Die Wiederherstellungsmöglichkeiten testen

Um eine vollständige Serverwiederherstellung zu testen und den Postfachinhalt zu validieren, sollte auf einem freien Server in einer Laborumgebung eine neue Active Directory-Gesamtstruktur installiert werden. Dabei kann es sich um einen virtuellen Server, eine Arbeitsstation oder einen anderen Rechner mit geringer Leistungsfähigkeit handeln. Mit der neuen Active Directory-Gesamtstruktur muss ein Exchange Server-Computer installiert werden, und zwar in einer Exchange-Organisation mit demselben oder einem anderen Namen. Der Exchange Server-Computer selbst kann ebenfalls einen beliebigen Namen haben. Nachdem der neue Server installiert und ähnlich wie der Produktionsserver konfiguriert wurde, müssen die Speichergruppen und Platzhalterdatenbanken angelegt werden. Nun müssen die Datenbanken vom Produktionsserver mit einem der Verfahren wiederhergestellt werden, die Ihre Sicherungsstrategie zulässt. Denken Sie daran, dass es jetzt darauf ankommt, echte Wiederherstellungsprozeduren einzusetzen. Anschließend sollten die Datenbanken bereitgestellt werden, und dann können Postfächer mit ihnen verbunden werden, um deren Inhalt zu überprüfen. Geschieht dies nicht in einer Labor-, sondern in der Produktionsumgebung, sollten Sie dafür sorgen, dass die Testpostfächer nicht mit den Benutzerpostfächern, sondern mit den wiederhergestellten Postfächern verbunden werden.

In einem echten Notfall oder in einer Exchange-Testorganisation, die verfügbar bleibt, ist die Umleitung der Active Directory-Benutzereinstellungen auf die wiederhergestellten Datenbanken einfach. Führen Sie einfach in der Exchange-Verwaltungsshell den folgenden Befehl aus:

```
move-mailbox -configurationonly -targetdatabase <Name_der_neuen_Datenbank>
```

Ohne zu wissen, dass Ihre Sicherungen funktionieren, können Sie keine Wiederherstellung durchführen. Überzeugen Sie sich jeden Tag davon, dass Ihre Sicherungsaufgaben abgeschlossen sind, und testen Sie vierteljährlich eine Wiederherstellung. Der Verzicht auf die Überprüfung der Sicherungen ist ein häufiger Fehler, weil man sich nur zu leicht darauf verlässt, dass die Sicherungsbänder ausgetauscht und die Daten korrekt gesichert werden. Beziehen Sie die Überprüfung der Sicherungsprotokolle und die Durchführung einer Wiederherstellung in Ihre regelmäßigen Routinemaßnahmen ein, um zu gewährleisten, dass die Wiederherstellung funktioniert.

#### HINWEIS

Die Überprüfung der Sicherungen muss nicht schwierig sein; sie lässt sich durch ein automatisches System wie den Systems Center Operations Manager von Microsoft oder durch eigene Skripte überwachen, die die Ereignisprotokolle auf Sicherungserfolgseignisse analysieren. Es ist wichtig, nicht nur auf Ereignisse für das Scheitern der Sicherung, sondern auch auf solche für ihren Erfolg zu achten, damit Sie wissen, dass eine Sicherung, bei der kein Fehler gemeldet wird, nicht zu lange gedauert hat.

Außerdem ist es wichtig, die Wiederherstellungsprozeduren für andere Funktionen als Postfachdatenbanken und -server zu testen. Dabei handelt es sich häufig um einen Neuaufbau, doch in anderen Fällen ist es ein komplexer Vorgang. Weitere Informationen darüber finden Sie unter der Adresse <http://technet.microsoft.com/en-us/library/aa998890.aspx>.

## Einen Exchange-Postfachserver wiederherstellen

Die vollständige Wiederherstellung eines Exchange-Postfachservers zu planen kann ein langwieriger Vorgang sein, weil er der wichtigste Server einer Exchange-Infrastruktur ist. Er bildet die Existenzgrundlage für alle anderen Komponenten. Bedenken Sie bei der Auswahl des Wiederherstellungsverfahrens folgende Faktoren:

1. **Der Active Directory-Ort für die Wiederherstellung** Sind der Active Directory-Standort und alle vorher dort vorhandenen Active Directory-Objekte intakt?
2. **Die unterstützende Active Directory-Infrastruktur** Sind die Serverfunktionen Clientzugriff und Hub-Transport an dem Standort vorhanden, an dem der Postfachserver wiederhergestellt wird? Kann der wiederhergestellte Postfachserver mit den Unified Messaging-, Edge-, Share-Point- oder Rechteverwaltungsdiensten interagieren, falls sie genutzt werden?
3. **Der wiederherzustellende Server** Handelt es sich um einen Postfachclusterver, einen eigenständigen Server oder einen eigenständigen Server, der als Cluster mit nur einem Knoten fungiert?

Die häufigsten Wiederherstellungsstrategien für den Postfachserver als Ganzes sind die vollständige Wiederherstellung und der Neuaufbau der Exchange-Anwendung. Sie werden üblicherweise bei betriebsbereiten Standby-Servern eingesetzt, wobei der erste Schritt die Verwendung eines Dial-Tone-Servers ist.

### Vollständige Serverwiederherstellung

Vollständige Serverwiederherstellungen werden durchgeführt, wenn zusätzlich zu einer Sicherung der Windows-Serverdaten eine Sicherung der Exchange-Datenbanken unterhalten wird. Die Serverdaten werden bei Exchange-Installationen nicht oft verwendet, weil Exchange sich während des Betriebs nicht besonders stark auf den Systemzustand des Windows-Servers stützt. Dieser Wiederherstellungsvorgang umfasst folgende Schritte:

1. Beschaffen von Ersatzhardware mit Komponenten, die den ursprünglichen Hardwarekomponenten des Servers entsprechen. Dazu können RAID-Controller, Netzwerkkarten usw. gehören.
2. Neuerstellen des Windows-Servers mit der Version, dem Service Pack und den Treiberversionen des ursprünglichen Servers
3. Wiederherstellen des Systemzustands und der Dateisystemsicherung auf dem Windows-Server
4. Neuinstallieren von Exchange Server mit den Service Packs
5. Wiederherstellen der Exchange Server 2007-Datenbanken

Nach Abschluss dieses Vorgangs können die Benutzer ohne Neuinstallation auf ihre Postfächer zugreifen. Eine Datenbankwiederherstellung ist nicht erforderlich, und es ist davon auszugehen, dass der Server so lange funktioniert, wie es die Komponenten erlauben. Bei dieser Vorgehensweise müssen die weiter vorn erörterten Überlegungen zu Active Directory und Exchange berücksichtigt werden. Das gilt nicht, wenn Exchange Server 2007 auf dem Active Directory-Server untergebracht und mit den Funktionen Hub-Transport und Clientzugriff kombiniert ist. In diesem Fall werden im Verlauf der skizzierten Schritte sämtliche Komponenten wiederhergestellt.

Diese Lösung ist zuverlässig; sie ist jedoch kostspielig und bringt ein hohes Maß an Verwaltungsaufwand mit sich. Dafür zu sorgen, dass genau dieselben Komponenten verfügbar sind, setzt normalerweise voraus, dass sie bereitgehalten werden, da Hardwarekomponenten einen kürzeren Lebenszyklus aufweisen als Software. Einen Windows Server 2003-Computer neu zu erstellen und wiederherzustellen erfordert mehr Zeit, als lediglich den Server neu zu erstellen und die Anwendungen neu zu installieren. Aufgrund dieser Einschränkungen lässt sich diese Möglichkeit in Situationen, in denen E-Mail auch nur die geringste Bedeutung hat, nur schwer umsetzen.



Die Lösung wird durch den Wiederherstellungspunkt und die Wiederherstellungszeit eingeschränkt, die sie bietet (Recovery Point Objective, RPO bzw. Recovery Time Objective, RTO). Das erste Ziel lässt sich durch Technologien von Drittanbietern erhöhen, die die Datenbank auf den Wiederherstellungsstandort replizieren. Am häufigsten werden dabei die Daten per VSS-Kopie oder Protokollversand über das Netzwerk übertragen oder die veränderten Spuren auf die Festplatten repliziert. Die Wiederherstellungszeit ist sehr hoch, was zum einen an der großen Menge Arbeit liegt, die zur Vorbereitung der Umgebung geleistet werden muss, und zum anderen daran, dass die Wiederherstellung der Daten aus den Sicherungen sehr lange dauert.

## Neuerstellung der Exchange-Anwendung

Die Neuerstellung der Exchange-Anwendung umfasst neben der eigentlichen Neuerstellung auch die darauf folgende Wiederherstellung der Daten. Um die Exchange-Anwendung auf einem Server wiederherzustellen, kann sie einfach von Anfang an auf einem neuen Windows Server-Computer oder mithilfe der Befehlszeilenoption **/m:RecoverServer** bzw. **/RecoverCMS** auf einem Standbyserver installiert werden. Bevor der Administrator die einzelnen Schritte durchführt, muss er wissen, welche Art von Exchange Server-Computer neu installiert werden soll. Für einen Clusterserver gilt die zweite Option, für einen Server, der nicht zu einem Cluster gehört, die erste.

Um **/m:RecoverServer** einzusetzen, unternehmen Sie Folgendes:

1. Setzen Sie mit **Active Directory-Benutzer und -Computer** das Computerkonto für den Server zurück, der wiederhergestellt werden soll.
2. Überprüfen Sie, ob alle Servernamen, Datenträgerkonfigurationen und Verzeichnispfade dieselben sind wie auf dem alten Server.
3. Wechseln Sie an der Befehlszeile in das Exchange Server-Quellverzeichnis und geben Sie den folgenden Befehl:

```
Setup.exe /m:RecoverServer
```

An diesem Punkt fragt das Exchange-Setupprogramm Active Directory nach den Konfigurationsdaten für den Server, den Sie wiederherzustellen versuchen. Die zuvor installierten Serverfunktionen und Datenspeicherorte werden zum Konfigurieren der Installation von Exchange Server verwendet. Es sollte nicht erforderlich sein, dass die Benutzer Daten ändern, und die Administratoren sollten keine Benutzerkonfigurationen verschieben müssen.

Um **/RecoverCMS** einzusetzen, gehen sie wie folgt vor:

1. Setzen Sie mit **Active Directory-Benutzer und -Computer** das Computerkonto für den Server zurück, der wiederhergestellt werden soll.
2. Überprüfen Sie, ob alle Servernamen, Datenträgerkonfigurationen und Verzeichnispfade dieselben sind wie auf dem alten Server.
3. Erstellen Sie den Clusterserver mit derselben Konfiguration wie im alten Cluster. Einzelkopiecluster können nicht als Cluster mit fortlaufender Clusterreplikation wiederhergestellt werden und umgekehrt.
4. Installieren Sie die Funktion des passiven Exchange Server-Postfachservers auf dem Knoten des Clusters, in dem die Wiederherstellung erfolgt.
5. Wechseln Sie an der Befehlszeile in das Exchange Server-Quellverzeichnis und geben Sie den folgenden Befehl:

```
Setup.exe /RecoverCMS /CMSName:<CMSName> CMSIPAddress:<CMSIPAddress>
```

6. Wenn Sie einen Einzelkopiecluster mit mehreren Exchange-Postfachclusterversern wiederherstellen, wiederholen Sie die Schritte 4 und 5, bis alle auf aktiven Knoten installiert sind.
7. Stellen Sie die Exchange-Postfachdatenbanken wieder her. Dazu können Sie eine Sicherungskopie oder eine Replikation auf Festplatten- oder Protokollversandbasis verwenden.
8. Installieren Sie im Cluster einen oder mehrere passive Knoten.

Jetzt ist der Exchange-Postfachclusterverser installiert und betriebsbereit. Es sollte nicht erforderlich sein, dass die Benutzer Daten ändern, und die Administratoren sollten keine Benutzerkonfigurationen verschieben müssen.

Bei beiden Wiederherstellungsverfahren für Exchange müssen die Überlegungen zu Active Directory und Exchange beachtet werden. Auf einem Exchange-Clusterverser können keine anderen Exchange-Funktionen untergebracht werden, was voraussetzt, dass diese am Standort bereits vorhanden sind. Sie sollten bereits neu erstellt oder vorhanden sein oder sich als nächster Punkt auf der Liste der neu zu erstellenden Elemente befinden.

Es handelt sich um zuverlässige Lösungen; der Kosten- und Verwaltungsaufwand kann je nach Konfiguration unterschiedlich ausfallen. Die verwendeten Server müssen nicht genau gleich sein, auch wenn sie für Einzelkopiecluster den WHQL-Standard erfüllen müssen. Der Exchange-Postfachclusterverser muss denselben Namen tragen wie der vorherige; die Servernamen, die IP-Adressen usw. brauchen jedoch nicht übereinzustimmen. Die Wiederherstellung benötigt wesentlich weniger Zeit als das manuelle Neuerstellen der Konfiguration einschließlich der Überprüfung, ob die Konfiguration korrekt eingegeben wurde.

Die Lösung ist auf den Wiederherstellungspunkt und die Wiederherstellungszeit beschränkt, die sie bietet. Das erste Ziel lässt sich durch Technologien von Drittanbietern erhöhen, die die Datenbank auf den Wiederherstellungsstandort replizieren. Am häufigsten werden dabei die Daten per VSS-Kopie oder Protokollversand über das Netzwerk übertragen oder die veränderten Spuren auf die Festplatten repliziert. Die Wiederherstellungszeit ist immer noch länger als bei einer Strategie mit hoher Verfügbarkeit, weil immer noch eine gewisse Menge Arbeit erforderlich ist. Sie ist aber kürzer als bei einer Wiederherstellungsstrategie, weil während des Vorgangs ein größerer Teil der Daten verwendet wird, die bereits vorliegen und benötigt werden, damit die Anwendung läuft.

## Dial-Tone-Server

Dial-Tone-Server ähneln Dial-Tone-Datenbanken; es sind einfach leere Konfigurationen, die bei dem Versuch eingesetzt werden, den Dienst für die Benutzer wiederherzustellen. Sie erfüllen keine der Anforderungen an einen Cluster-, Bereitschafts- oder Hochverfügbarkeitsdienst, weil die Messagingdaten bei einer Dial-Tone-Wiederherstellung nicht unmittelbar verfügbar sind. Die grundlegende E-Mail-Funktionalität wird sofort aktiviert; E-Mail-Daten, Regeln, Kalenderdaten, Einstellungen für Unified Messaging, Konfigurationen für Mobilgeräte usw. werden jedoch nicht wiederhergestellt. Der Vorteil dieser Lösung besteht darin, dass die Benutzer in eingeschränktem Umfang arbeiten können, bis der Rest der Daten wiederhergestellt oder neu angelegt worden ist.

Um eine Dial-Tone-Wiederherstellung zu implementieren, führen Sie folgende Schritte durch:

1. Installieren Sie einen vollständigen Exchange-Postfachserver und legen Sie alle erforderlichen Speicherguppen, Datenbanken und sonstigen Umgebungskonfigurationen an.
2. Handelt es sich um eine Dial-Tone-Datenbank, legen Sie Speicherguppen und Datenbanken auf vorhandenen Servern an, die von der Geschäftsführung für die Verwendung bei einer Dial-Tone-Wiederherstellung vorgesehen wurden.

3. Wenn eine Dial-Tone-Wiederherstellung erforderlich ist – beispielsweise, wenn Server oder Standort ausgefallen sind –, verwenden Sie das Commandlet **Move-Mailbox-ConfigurationOnly** und verweisen alle Postfächer, die verschoben werden müssen, auf die Dial-Tone-Datenbanken.
4. Wenn die Messagingdaten verfügbar werden, können sie entweder auf dem Dial-Tone-Server wiederhergestellt und in die Postfächer importiert oder auf einem Exchange-Ersatzserver vorbereitet werden, sodass die Benutzer auf die Ersatzhardware verschoben werden können.

Diese Lösung hat eine sehr kurze Wiederherstellungszeit für den Dienst und einen nahen Wiederherstellungspunkt; die Wiederherstellungszeit für die Daten ist normalerweise länger. Dies bietet Vorteile für Organisationen, die für Geschäftsprozesse auf E-Mail-Dienste angewiesen sind, aber für die Verarbeitung dieser Geschäftsfunktionen keine Verlaufsdaten benötigen.

## Eine Exchange-Postfachdatenbank wiederherstellen

Die Wiederherstellung einer Exchange Server 2007-Postfachdatenbank ist üblicherweise komplexer als die Wiederherstellung des Postfachservers selbst. Sie kann einfache Werkzeuge wie Exchange Disaster Recovery Analyzer oder komplexe wie Exchange ESE Utility oder Information Store Integrity benötigen.

Manchmal muss die Datenbank in irgendeiner Form wiederhergestellt werden, auch wenn keine saubere Sicherung einer Postfachdatenbank zu bekommen ist. Exchange Server 2007 hat den Wiederherstellungsvorgang durch die Portierbarkeit der Datenbank in weiten Teilen vereinfacht. Diese integrierte Funktion ermöglicht es, die Datenbank unabhängig vom Servernamen auf einen Server zu verschieben und dort bereitzustellen. Das ist insofern für Wiederherstellungsverfahren wichtig, als sich eine Datenbank fast überall unterbringen und benutzen lässt, sobald sie sich in einem konsistenten Zustand befindet und bereitstellbar ist.

Der Kniff besteht darin, die Datenbank konsistent zu machen. Dafür gibt es mehrere Methoden. Stellen Sie bei der Wiederherstellung Ihrer Datenbank fest, dass sie beschädigt ist oder sich nicht bereitstellen lässt, ist es günstig, in den Disaster Recovery Analyzer in der Toolbox zu wechseln und ihn für die Datenbank auszuführen. Dieser Assistent führt Sie durch die Suche nach der Datenbank und die Verwendung von **Eseutil.exe** im Wiederherstellungsmodus, um zu versuchen, die Datenbank bereitstellbar zu machen.

Bleibt dieser Versuch erfolglos, haben Sie zwei Möglichkeiten. Sie können eine weiche Wiederherstellung der Datenbank mit **Eseutil.exe** und der Option **/r** durchführen oder **Isinteg.exe -fix** starten, um alle Fehler zu beheben, die aus der Sicht der Anwendung auf den Datenbankseiten zu finden sind.

## Ein einzelnes Exchange-Postfach wiederherstellen

Bisher ging es um Ereignisse, bei denen Ihr Standort, Ihr Server oder Ihre Datenbank ausgefallen waren. In diesen Fällen wurden ganze Server wieder arbeitsfähig gemacht und Postfachdatenbanken wiederhergestellt. Die häufigste Wiederherstellungssituation, die Exchange-Administratoren erleben, ist die Wiederherstellung von Postfächern. Ein Fehler eines einzelnen Postfachs ist wahrscheinlicher als einer auf Datenbank- oder Serverebene. Deshalb bilden die Möglichkeiten zur Wiederherstellung eines einzelnen Postfachs einen entscheidenden Bestandteil Ihrer Gesamtplanung.

In Exchange Server 2007 ist es relativ einfach, ein einzelnes Postfach wiederherzustellen: Sobald die Datenbank in einer Speichergruppe für die Wiederherstellung (Recovery Storage Group, RSG) auf ihre Wiederherstellung wartet, brauchen Sie eigentlich nur noch den folgenden Befehl auszuführen:

```
Restore-mailbox -identity <Anzeigename> -RSGDatabase <RSG\Postfachdatenbank>
```

Dies ist die einfachste Methode. Sie stellt die Postfachdaten in dem mit dem angegebenen Anzeigenamen verknüpften Postfach wieder her. Das ist gut und sinnvoll. Wahrscheinlich ist dies die häufigste Vorgehensweise für die Wiederherstellung gelöschter Postfächer; es gibt jedoch noch andere Möglichkeiten.

Hat ein Mitarbeiter die Firma verlassen und möchte sein früherer Vorgesetzter den Zustand von dessen Postfachs vor dem Ausscheiden einsehen, wird eine alte Sicherung der Postfachdatenbank in der RSG wiederhergestellt. Dann müssen Sie das Postfach des Mitarbeiters mit folgendem Befehl in das des Vorgesetzten verschieben:

```
Restore-Mailbox -RSGMailbox 'Ex-Employee Name' -  
RSGDatabase 'RSG\Mailbox Database' -id 'Manager Mailbox' -TargetFolder 'Ex-  
Employee's OldEmail'
```

Es ist wichtig, die Möglichkeit vorzusehen, eine einzelne Datenbank in einer RSG wiederherzustellen, sonst lässt sich ein einzelnes Postfach nur mit Werkzeugen von Drittanbietern wiederherstellen.

### Aus der Praxis: Die Aufbewahrung gelöschter Objekte planen

Die aufgezeigten Wiederherstellungsverfahren sind großartig; erfahrene Administratoren wissen jedoch sehr genau, dass E-Mails sehr leicht versehentlich gelöscht werden, was Benutzer und Administratoren vor Probleme stellt. Die Möglichkeit, gelöschte E-Mails schnell wiederherzustellen, ist normalerweise von größter Bedeutung; ohne richtige Planung kann es zu anstrengenden Situationen kommen. Ich habe solche Fälle mehrfach erlebt. Eine leitender Mitarbeiterin arbeitete noch spät an einem Vorschlag oder einem Projekt, und ich war natürlich noch damit beschäftigt, Patches für den Server zu aktualisieren. Plötzlich geht eine Sofortnachricht von der leitenden Angestellten auf, in der sie nach einer Möglichkeit fragt, eins ihrer E-Mail-Objekte wiederherzustellen. Ich ließ alles fallen, was ich gerade tat, um auf ihre Anfrage zu reagieren (es war sowieso schon spät, und das konnte einen guten Eindruck machen). Nach kurzer Diskussion über das Messagingprogramm entdeckte ich, dass sie im Verlauf des Abends in mehreren E-Mails ihrer Mitarbeiter nachgelesen hatte, um einen Bericht für ihren Chef zu erstellen. Um an die Mails zu kommen, öffnete und schloss sie sie mit der vertrauten Tastenkombination. Am Ende der Arbeit druckte sie den Bericht aus und las ihn noch einmal, wobei sie einen Fehler in den Daten bemerkte. Sie kehrte zum Posteingang zurück, um die E-Mail mit der Korrektur zu suchen, und entdeckte, dass sie weg war. Sie durchsuchte den Ordner und den Ordner **Gelöscht**, aber ohne Erfolg.

Nach einigen Tests auf meinem eigenen Client fand ich heraus, dass die verwendete Tastenkombination für eine andere Anwendung galt; den E-Mail-Client unserer Firma veranlasste sie jedoch, das E-Mail-Objekt dauerhaft zu löschen. Damals war ich froh, dass unsere Richtlinie für die Aufbewahrung gelöschter Objekte noch den Standardwert 14 Tage benutzte. Ich konnte zuversichtlich antworten, dass ich alle Objekte wiederherstellen könne, die sie brauchte, um die Arbeit des Abends abzuschließen, ohne Datenbanken oder Objekte von der Exchange-Verwaltungsshell aus wiederherstellen zu müssen. ►

**Aus der Praxis: Die Aufbewahrung gelöschter Objekte planen**

Es ist wichtig, ein angemessenes Verfahren für die Aufbewahrung gelöschter Objekte zu planen und dafür zu sorgen, dass die in der festgelegten Zeit anfallende Menge im vorgesehenen Platz für die Datenbank untergebracht werden kann. Eine allgemeine Faustregel gibt für die 14-tägige Aufbewahrung 10 Prozent der Datenbankgröße an. Sollte die Frist überschritten sein und müssen Sie bestimmte Objekte aus einer Datenbankwiederherstellung entnehmen, verwenden Sie den Befehl **RestoreMailbox**. Dazu stellen Sie die Datenbank einfach in einer RSG wieder her, führen das Commandlet aus und geben an, welche Nachrichten in welchem Produktionspostfach wiederhergestellt werden sollen.

## Einen Exchange-Postfachserver sichern

Nachdem Sie jetzt wissen, was erforderlich ist, um Exchange Server-Computer wiederherzustellen, haben wir genügend Vorwissen, um uns mit dem Sichern zu befassen. Es gibt mehrere Methoden, die beiden bereits erörterten Technologien zu implementieren, um sie an die Wiederherstellungsverfahren anzupassen – die Technologien der streaming- und der VSS-basierten vollständigen, differenziellen, inkrementellen oder Kopiesicherung, verbunden damit, dass bestimmte Informationen in Active Directory oder einer transportablen Serverkopie verfügbar sind.

Bei Serversicherungen sorgen Sie dafür, dass der Systemzustand, die Registrierung und die Anwendungen, die die Serverinstallation unterstützen, in der Sicherungsdefinition enthalten sind. Diese Sicherungen brauchen nicht jede Nacht angefertigt zu werden, sollten jedoch vor und nach allen Patchvorgängen und Softwareaktualisierungen durchgeführt werden.

Bei der Neuerstellung von Servern sorgen Sie für eine gründliche Dokumentierung. Dabei haben Sie die Wahl zwischen einer sorgfältig verfassten Konfigurationsdokumentation, einer automatisierten Standardinstallation für Exchange Server-Computer und einem Konfigurationsmanagementsystem von einem Drittanbieter. In allen Fällen sollte das Sichern einfach sein und bei jedem Erstellen eines neuen Servers getestet werden.

Bei der Serverwiederherstellung bietet Exchange Server mehrere Möglichkeiten. Benutzen Sie die Informationen aus Active Directory, muss das Betriebssystem in einem Zustand neu erstellt werden, der Exchange unterstützt, aber nicht unbedingt in dem, den es vorher hatte. Damit entfällt die Notwendigkeit, eine Sicherung oder Kopie des Systems zu unterhalten. Die Wiederherstellung kann auch von einem Speicherbereichsnetzwerk (Storage Area Network, SAN) aus erfolgen. Dabei werden im Speicherarray des Netzwerks logische Einheitennummern (Logical Unit Number, LUN) unterhalten, die beim Ausfall eines physischen Servers wiederverwendet werden können. Der Server selbst muss wie im ersten Fall mit der vorherigen Konfiguration neu erstellt werden (einschließlich HBAs, Treiber, SAN-Verbindungen usw.); die Daten werden jedoch nicht aus einer Sicherung wiederhergestellt. Der Server wird dann einfach an das SAN angeschlossen, bekommt Zugriff auf die LUNs und wird eingeschaltet. Diese Situation gibt Ihnen auch die Flexibilität, Start-LUNs des Betriebssystems auf andere Speicherarrays oder andere Volumes im Speicherarray zu replizieren.

## Eine Exchange-Postfachdatenbank sichern

Das Sichern einer Exchange-Postfachdatenbank kann schwer zu planen sein. Die Datenbank wird im Lauf des Tages für vieles genutzt, was nicht zu Sicherungszwecken unterbrochen werden sollte. Benutzerzugriff, Neuaufbau von Inhaltsindizes und Onlinewartung kommen dabei am häufigsten

vor. Die Sicherung sollte für eine Zeit geplant werden, in der sie nicht damit in Konflikt gerät und trotzdem jede Nacht erledigt wird.

Häufig kommen die beiden folgenden Methoden zum Einsatz; sie sind umfangreich getestet und erfüllen sinnvolle Ziele hinsichtlich Wiederherstellungspunkt und -zeit:

- Wöchentlich eine vollständige und täglich eine inkrementelle Sicherung
- Täglich eine vollständige Sicherung

---

**HINWEIS** Als Alternative zu diesen Technologien ermöglichen einige Drittanbieter durch benutzerdefinierte Plattenspiegelung und/oder Dateisystemtreiber Sicherungen, die weder auf VSS noch auf Streaming basieren. Um vor einer Implementierung in der Produktion die Unterstützungsfähigkeit und die technische Zuverlässigkeit sicherzustellen, ist eine sorgfältige Bewertung dieser Technologien von Drittanbietern erforderlich. Microsoft unterstützt sie häufig nicht, sodass der Primärsupport den Drittanbietern überlassen bleibt.

---

## Wöchentliche und tägliche Sicherungen kombinieren

Die erste Methode ist eine wöchentliche vollständige und eine tägliche inkrementelle Sicherung. Sie kann auf Streaming- oder VSS-Basis erfolgen. Wegen der Geschwindigkeit der inkrementellen Sicherungen fällt die Sicherungsdauer normalerweise geringer aus. Bei einem kleineren Zeitfenster können die Datenbanken größer sein, was wiederum größere Postfächer ermöglicht, während die Benutzer immer noch zusammenbleiben können. Dies spielt in vielen Umgebungen eine Rolle, sodass diese Methode populär geworden ist. Außerdem stört das kleinere Zeitfenster die wichtige Onlinewartung nicht, die einmal wöchentlich stattfinden und nicht mit dem Neuaufbau von Indizes oder der allgemeinen Benutzeraktivität in Konflikt geraten soll. Die genannten Eigenschaften sind für Sicherungen günstig; die Methode weist jedoch auch Nachteile auf.

Am deutlichsten ist die Anzahl der Sicherungen, die für eine vollständige Wiederherstellung einge spielt werden müssen. Außerdem kann sich die mögliche Beschädigung einer inkrementellen Sicherung schädlich auf den Vorgang der Gesamtsicherung auswirken; die ausschließliche Verwendung vollständiger Sicherungen würde dagegen eine Wiederherstellung aus einer der jüngsten Sicherungen ermöglichen.

## Tägliche vollständige Sicherungen

Die zweite Methode ist die der täglichen vollständigen Sicherung. Sie kann auf Streaming- oder VSS-Basis erfolgen. Wegen der betroffenen Datenmengen führt diese Vorgehensweise zu längeren Sicherungszeiten pro Nacht. Durch Plattenspiegelung können bei VSS-Sicherungen die Dauer und die Belastung der Hosts erheblich reduziert werden. Wenn Sie keine dieser Lösungen einsetzen können, reicht auch ein Software-VSS-Provider oder ein Streamingsicherungsprogramm aus. Unabhängig von der verwendeten Technologie sollten Sie ein größeres Zeitfenster einplanen, um zu gewährleisten, dass die Sicherung erfolgreich abgeschlossen werden kann. Häufig werden Probleme wie langwierige Konsistenzprüfungen, Fehler bei der Bereitstellung von Medien und Ausfälle mitten in der Sicherung nicht bedacht, sodass das Zeitfenster überschritten wird.

Bei der Planung einer vollständigen Sicherung auf VSS-Basis ist Folgendes zu bedenken:

- Die Zeit für eine Konsistenzprüfung
- Die Zeit für die Synchronisierung der VSS-Medien mit den Produktionsspindeln
- Das Verhalten bei Fehlern bei der Bereitstellung von Medien wie Festplatten und Bändern

- Das Verhalten bei Fehlern mitten im Sicherungsvorgang wie dem Beendigungszustand der Festplatte

Bei der Planung einer vollständigen Sicherung auf Streamingbasis ist ebenfalls einiges zu bedenken:

- Die Belastung für den Host bei Aktivierung des Flags »Gelöschte Objekte eliminieren«
- Die Zeit für eine vollständige Sicherung
- Das Verhalten bei Fehlern bei der Bereitstellung von Medien wie Festplatten und Bändern
- Das Verhalten bei Fehlern mitten im Sicherungsvorgang wie dem Beendigungszustand der Festplatte

All dies müssen Sie berücksichtigen und einplanen, um einen reibungslosen Ablauf Ihrer Sicherungen zu gewährleisten. Viel zu häufig werden diese Aspekte übersehen, und die Erledigung von Sicherungen wird zur langwierigen Aufgabe, die niemals abgeschlossen wird. Daraus können Sicherungen entstehen, die nicht vollständig sind oder sich bei einem Ausfall nicht wiederherstellen lassen.

## Ein einzelnes Exchange-Postfach sichern

Das Sichern einzelner Exchange-Postfächer ist das einfachste Thema, das in diesem Kapitel angesprochen wird. Um es einfach auszudrücken: Microsoft unterstützt diese Funktion von sich aus nicht. Die beiden Sicherungstechnologien, Streaming und VSS, ermöglichen nur das vollständige Sichern und Wiederherstellen von Datenbanken, was jedoch nicht bedeutet, dass das Sichern eines einzelnen Postfachs unmöglich ist. Für Exchange Server kann ein Drittanbieter ein Sicherungsprogramm erstellen, das jedes Postfach einzeln sichert. Dies geschieht üblicherweise mithilfe der MAPI-Schnittstelle genau so, wie sich ein Outlook-Client bei einem Postfach anmeldet und dann in der Lage ist, alle darin befindlichen Objekte zu lesen. Dies wurde schon für frühere Versionen angeboten, aber die Hersteller haben diese Fähigkeit häufig hinzugefügt und wieder weggelassen. Einige haben diese Strategie als Sicherung auf Objektebene implementiert, sodass sich einzelne Nachrichten aus einer echten Sicherungsdatei wiederherstellen lassen.

Diese Anwendungen von Drittanbietern können Ihre Umgebung erheblich verbessern, aber Leistung und Zeitvorgaben dieser Lösungen bringen einige ernsthafte Probleme mit sich. Wenn Sie vorhaben, eine davon einzusetzen, sollten Sie ernsthaft erwägen, die betreffende Sicherung vom Produktions-exemplar der Datenbank auf ein Replikat zu verlagern, das durch fortlaufende Cluster- oder lokale Replikation oder eine andere Replikationstechnologie entstanden sein kann; wichtig ist nur, dass die Sicherung keine Zeit auf dem Produktionsdatenträger in Anspruch nimmt.

Eine Alternative zu einer Sicherungslösung auf Postfachebene kann eine Anwendung bilden, die ein ausgelagertes Verfahren zum Sichern und Wiederherstellen eines Postfachs ermöglicht, bei der eine vollständige Sicherung und Wiederherstellung der Datenbank über die Wiederherstellungsspeichergruppe benutzt wird. Dieses Verfahren beeinträchtigt die Leistung des Produktionssystems nicht im selben Maß wie eine Sicherungslösung auf Postfachebene.

## Für Beschädigungen vorausplanen

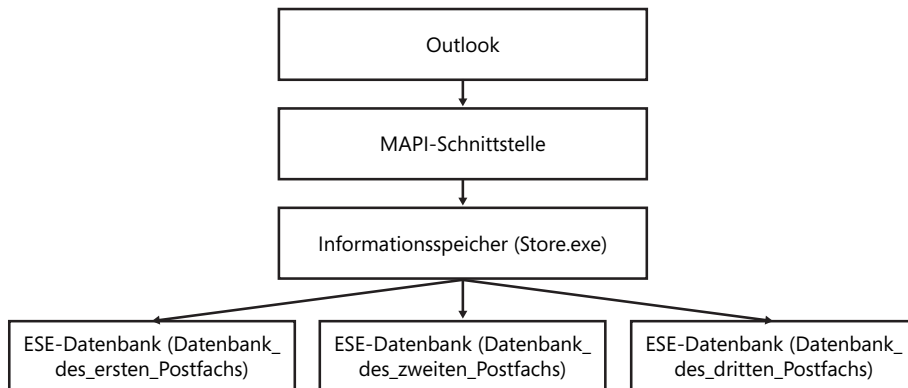
Beschädigungen sind unvermeidlich. Irgendwann erleidet eine Datenbank, die unter Ihrer Kontrolle steht, einen Schaden. Darauf sollten Sie sich einrichten und Vorkehrungen treffen, die Tools und Prozeduren beherrschen und die nötige Ruhe entwickeln, die erforderlich ist, um mit dieser kritischen Situation fertig zu werden.

Mit folgenden Tools sollten Sie sich auskennen:

- Eseutil
- Isinteg
- MfcMAPI

Dann sind Sie in der Lage, das Datenbankmodul ESE zu bedienen (Eseutil), Fehler in der Informationsspeicherschicht zu finden und zu beheben (Isinteg) und mit dem Protokoll MAPI in bestimmte Postfächer zu schauen (MfcMAPI). Sie müssen den grundlegenden Unterschied zwischen den drei Komponenten kennen, um zu verstehen, wo ein Problem jeweils liegen kann. In Abbildung 16.3 sehen Sie unten die Datenbankinstanzen (ESE); dort sind die Daten gespeichert. Der Informationsspeicher liegt darüber; es handelt sich um einen einzelnen Prozess, der den Zugriff auf die einzelnen Datenbanken verwaltet und steuert, wie die Informationen in und aus den Datenbanken gelangen. Die MAPI-Schnittstelle bildet die Verbindung zum Informationsspeicher; sie bestimmt, wie Outlook-Clients den Informationsspeicher und schließlich die Datenbank sehen und mit ihnen kommunizieren. Outlook benutzt die Schnittstelle zur Kommunikation mit Exchange. Sie sehen, dass jedes Werkzeug Einfluss auf einen anderen Teil des Stacks nehmen kann: **Eseutil.exe** kann direkt mit der ESE-Datenbank interagieren, **Isinteg.exe** mit den Datenbanken im Kontext des Informationsspeichers und **MfcMAPI.exe** auf dieselbe Weise wie Outlook (jedoch ohne irgendwelche Einschränkungen) über die MAPI-Schnittstelle mit dem Informationsspeicher.

Abbildg. 16.3 Schichten zwischen Outlook und der Datenbank



## Sicherungsstrategien umsetzen

Die drei wichtigsten Anforderungen, die beim Umsetzen der beschriebenen Verfahren zu bedenken sind, betreffen Wiederherstellungspunkt bzw. -zeit, die finanzielle Seite und die Umgebung. Sie definieren, wie die Verfahren implementiert werden und wie sie arbeiten.

Am häufigsten werden Wiederherstellungspunkt und Wiederherstellungszeit diskutiert. Das erste Ziel ist der Zeitpunkt, auf dessen Zustand das System wiederhergestellt werden soll. Wenn Sie das System einmal wöchentlich mittwochs um zehn Uhr sichern, heißt Ihr Ziel für den Rest der Woche Mittwoch zehn Uhr, weil dies der einzige Zeitpunkt ist, für den eine Wiederherstellung möglich ist. Das zweite bezeichnet die gewünschte Dauer der Wiederherstellung des Systems. Wenn Ihre Sicherungsmethode Ihnen erlaubt, ein USB-Kabel einzustecken, auf eine Schaltfläche zu klicken und zehn Minuten zu warten, bis das System vollständig wiederhergestellt ist, beträgt Ihre Sicherungsdauer etwa elf Minu-



ten (unter der Voraussetzung, dass die Arbeit mit Kabel und Schaltfläche etwa eine Minute dauert). Häufig werden diese beiden Ziele kombiniert. Systeme mit dem Ziel eines möglichst nahen Wiederherstellungspunkts haben normalerweise auch das Ziel einer kurzen Wiederherstellungszeit und umgekehrt. Das Problem liegt darin, dass der finanzielle Aufwand üblicherweise ebenfalls gemeinsam steigt oder sinkt: Szenarien mit nahem Wiederherstellungspunkt und kurzer Wiederherstellungszeit kosten im Allgemeinen mehr, solche mit fernem Wiederherstellungspunkt und langer Wiederherstellungszeitziel weniger.

Damit kommen wir zur zweiten wichtigen Anforderung: dem finanziellen Aufwand. Diese Überlegung ist wichtig und hat wahrscheinlich erheblichen Einfluss darauf, welche Verfahren eingesetzt werden. Ein geografisch weit verteilter Cluster mit replizierten Speicherarrays weist zum Beispiel die anspruchsvollsten Ziele für Wiederherstellungspunkt und Wiederherstellungszeit für E-Mail-Datenbankumgebungen auf und stellt normalerweise eine teure Lösung dar. Ein verschlüsseltes Sicherungsband, das per Post an den wiederherzustellenden Standort geschickt wird, wo es auf neuen Servern eingespielt wird, erfüllt dagegen nur sehr geringe Ansprüche an Wiederherstellungspunkt und Wiederherstellungszeit und stellt ungefähr die billigste Lösung dar, die Sie bekommen können.

Die Überlegungen zur Umgebung bilden die dritte wesentliche Anforderung. Sie erfordert ein hohes Maß an Planung. Dazu gehört, welche Serverfunktionen auf den wiederherzustellenden Servern eingerichtet sind, an welchem Active Directory-Standort der Server wiederhergestellt wird und welche Infrastruktur zwischen den beiden Standorten besteht. Ist auf dem Server nur die Funktion des Postfachservers eingerichtet, kommt möglicherweise eine Clusterlösung in Frage; allerdings müssen an dem Active Directory-Standort, an dem der Postfachserver wiederhergestellt werden soll, bereits der Clientzugriffs- und der Hub-Transportserver vorhanden sein. Ist die einzige Netzwerkverbindung zwischen den beiden Standorten eine E1-Leitung mit hoher Latenz, stellen Festplatten- oder fortlaufende Clusterreplikation möglicherweise keine praktikablen Lösungen dar, um Kopien der Postfachdatenbank an den Wiederherstellungsort zu transportieren.

Der nächste Abschnitt zeigt häufige Szenarien, in denen die genannten Anforderungen bei der Entwicklung von Verfahren zur Wiederherstellbarkeit von Diensten und Daten berücksichtigt wurden. Sie erfüllen bestimmte konkrete Anforderungen und dienen nur zur Veranschaulichung.

## Fortlaufende Clusterreplikation mit VSS

Das erste Szenario zeigt die fortlaufende Clusterreplikation (Clustered Continuous Replication, CCR) mit Sicherungen durch den Volumenschattenkopie-Dienst (Volume Shadow Copy Service, VSS). Es kombiniert die neue CCR-Technologie mit dem VSS-Standardframework. Die Verwendung von CCR und VSS in Ihrer Umgebung bietet gegenüber anderen Lösungen für die Datenreplikation einige Vorteile, die in erster Linie die Kosten, die Unterstützung und die Zeit bis zum Neustart betreffen. Sie in einem Szenario zu verknüpfen bedeutet, dass Ihre Umgebung aus folgender Hardware besteht:

- Ein Cluster mit dem Microsoft-Clusterdienst, der aus zwei Exchange Server 2007-Postfachservern und einem Quorumgerät besteht.
  - Die Exchange Server 2007-Postfachserver brauchen nicht die gleiche Hardware aufzuweisen, aber Sie sollten einplanen, dass Sie die Produktionslast jederzeit auf einem der beiden Systeme ausführen können.
  - Das Quorumgerät kann ein beliebiges unterstütztes Quorumgerät in einem Microsoft-Cluster sein, zum Beispiel eine Quorumfestplatte, ein Quorumserver in einem MNS-Cluster (Majority Node Set) oder ein Dateifreigabenzeuge in einem MNS-Cluster.

- Ein Server zur Durchführung von Sicherungen, der auch als Host des Dateifreigabenzeugen für Ihren MNS-Cluster dienen kann. Dieser Server kann über 32- oder 64-Bit-Hardware verfügen und braucht nicht den übrigen Serverkonfigurationen zu entsprechen. Der VSS-Requestor befindet sich auf dem Server, der für die Sicherungen zuständig ist. Benutzt der Server ein freigegebenes Speicherarray, werden auf dem Sicherungsserver Festplattenreplikate bereitgestellt, um Prüfsummen zu verifizieren.

Dieses Szenario wird normalerweise so eingerichtet, dass der Cluster auf jedem Knoten betrieben werden kann und zur Wartung des Servers oder bei (geplanten oder ungeplanten) Notfällen ein Failover auf jeden Knoten möglich ist. Der Sicherungsserver kann über das Netzwerk mit beiden Knoten kommunizieren und ist in der Lage, mit dem verwendeten VSS-Provider zu sprechen. Der Zeitplan für die Sicherungen ist in erster Linie von der Menge der Daten in den einzelnen CCR-Gruppen und dem zulässigen Zeitfenster für die Sicherung in der Organisation abhängig. Am häufigsten ist ein Szenario, in dem vollständige Sicherungen am Wochenende in einem erweiterten Zeitfenster und differenzielle Sicherungen während der Woche in einem kleineren Zeitfenster stattfinden.

Beim Implementieren eines derartigen Szenarios sind zwei wichtige Aspekte zu bedenken:

- Welche Menge an Datenverlust kann Ihre Umgebung verkraften (Wiederherstellungspunkt)?
- Innerhalb welcher Zeit muss Ihre Umgebung neu gestartet werden (Wiederherstellungszeit)?

Bei einem geplanten Failover gewährleistet die fortlaufende Clusterreplikation (CCR), dass die letzte Protokolldatei geschlossen und auf den passiven Knoten im CCR-Cluster übertragen wird. Anschließend kann der passive Knoten den Postfachclusterserver und die zugrunde liegende Datenbank neu starten. Beim Neustart sollte die Datenbank dank des Protokolleinspielmechanismus auf der entfernten Seite bereits konsistent sein, was dazu führt, dass der Neustart praktisch sofort erfolgt und Clientanforderungen direkt nach Auslösen des Failovers wieder bedient werden.

Bei einem Failover im Notfall läuft der Vorgang ähnlich ab. Der passive Knoten versucht, alle Protokolldateien vom aktiven Knoten zu kopieren, die geschlossen wurden oder noch nicht geschlossen sind. Anschließend versucht er sofort, diese Dateien einzuspielen, um etwa verbliebene Daten in die passive Datenbank zu übernehmen. In diesem Augenblick kommt die Protokollverlustsicherung ins Spiel, um zu gewährleisten, dass die kopierten Protokolle vollständige Daten enthalten. Sind die Daten unvollständig, werden die Protokolle nicht in die Datenbank eingespielt, sondern es wird eine neue Protokollgeneration angelegt, um eingehende Daten damit zu verarbeiten, während die unvollständigen unbeachtet bleiben. Dadurch ist der Postfachclusterserver schnell wieder erreichbar und kann aus dem Papierkorb des Hub-Transport-Servers alle Daten holen, die verfügbar sind.

Bei einem geplanten und auch bei einem ungeplanten Failover ist Datenverlust möglich. Kann das letzte Protokoll aus irgendeinem Grund nicht auf den passiven Knoten kopiert werden und lassen sich die Daten auch nicht über den Transportpapierkorb erneut senden, gehen die Daten der Nachrichten verloren, die in diesen Protokollen teilweise verfügbar waren. Das Wiederherstellungspunktziel für den Failover kann variabel sein; es wird jedoch im Szenario durch eine VSS-Sicherung ergänzt, die einen sehr schnellen Mechanismus zum Sichern und Wiederherstellen bietet, um auf der Grundlage der VSS-Sicherung eine aktuellere Kopie zu ermöglichen. Die angepeilte Wiederherstellungszeit für den Failover ist immer noch relativ kurz, was auch für die VSS-Wiederherstellung gilt (vorausgesetzt, der VSS-Anbieter erlaubt eine schnelle Wiederherstellung).

Dieses Szenario hat u.a. folgende Nachteile:

- Ein Failover kann zu Datenverlust führen.
- Werden Sicherungen vom Replikat angefertigt, lassen sie sich nicht problemlos zwischen den Produktions- und den Replikatknoten verschieben.

- Die Lösung lässt sich möglicherweise nur schwer auf getrennte Standorte erweitern.

Datenverlust lässt sich in allen Szenarien, bei denen das Produktionsexemplar der Datenbank nicht gemeinsam mit der passiven Kopie genutzt oder synchron auf sie repliziert wird, nur schwer vermeiden. Der Umfang des Verlustes lässt sich durch Einstellungen für den Transportpapierkorb und Investitionen in die Netzwerkinfrastruktur beeinflussen, aber das Risiko ist nicht vollkommen auszuschalten. Erstellt die VSS-Sicherungsanwendung Kopien vom Replikations-Writer, können diese außerdem nur auf dem Produktions-Writer wiederhergestellt werden. Eine solche Sicherung kann auf dem Replikat also nur wiederhergestellt werden, wenn der Postfachclusterserver vor der Wiederherstellung einen Failover auf das Replikat ausführt. Falls die Sicherung vom Replikat genommen wurde und der Standort des passiven Clusterknotens unerreichbar wird, gibt es keine Sicherung, die sich wiederherstellen lässt.

## Einzelkopiecluster mit Streamingsicherungen

Das zweite Szenario ist der Einzelkopiecluster (Single Copy Clustering, SCC) mit Streamingsicherung. Es kombiniert die herkömmliche SCC-Technologie mit der älteren Streamingsicherung-API. Diese Möglichkeit bietet in Ihrer Umgebung gegenüber den Lösungen mit Datenreplikation einige Vorteile: minimaler Datenverlust, optimale Wiederherstellungszeit und das geringste Risiko für eine Beschädigung der Datenbanken. Die Techniken in einem Szenario zu verknüpfen bedeutet, dass Ihre Umgebung aus folgender Hardware besteht:

- Ein Cluster mit dem Microsoft-Clusterdienst, der aus zwei oder mehr Exchange Server 2007-Postfachservern und einem Quorumgerät besteht.
  - Die Server im Cluster sollten alle die gleichen Komponenten enthalten und den Standard WHQL für Cluster erfüllen.
  - Das Quorumlaufwerk muss für alle Server des Clusters erreichbar sein.
- Ein Server zur Durchführung von Sicherungen, der nur für die Steuerung der Sicherungen zuständig ist. Die Postfachserver leisten selbst den Großteil der Arbeit, um die Daten in der Datenbank an einen externen Ort zu verlagern.

Beim Implementieren eines derartigen Szenarios sind zwei wichtige Aspekte zu bedenken:

- Welche Menge an Datenverlust kann Ihre Umgebung verkraften (Wiederherstellungspunkt)?
- Innerhalb welcher Zeit muss Ihre Umgebung neu gestartet werden (Wiederherstellungszeit)?

Bei einem geplanten Failover führt SCC einen Neustart des Postfachclusterservers auf dem bevorzugten passiven Knoten des Clusters durch. Der aktive Knoten fährt die Datenbank des Postfachclusterservers herunter und startet sie auf dem passiven Knoten neu. Sobald alle Dienste gestartet und die Datenbanken bereitgestellt sind, ist der Postfachclusterserver wieder benutzbar.

Bei einem ungeplanten Failover versucht SCC zuerst einen Neustart auf dem aktiven Knoten, der den Postfachclusterserver beherbergt. Gibt es Einschränkungen, zum Beispiel den Ausfall der Hauptplattine des aktiven Knotens, versucht SCC, den Postfachclusterserver auf dem bevorzugten passiven Knoten neu zu starten, wobei der Zustand der Datenbank keine Rolle spielt. Sind Protokolle vorhanden, für die noch kein Commit durchgeführt wurde, werden die abgeschlossenen Transaktionen in die Datenbank überspielt und alle unvollständigen Transaktionen mit einem Rollback zurückgenommen.

Bei einem geplanten Failover sorgt diese Vorgehensweise ebenso wie bei einem ungeplanten dafür, dass es keinen Datenverlust gibt, wodurch der Wiederherstellungspunkt auf null gesetzt wird. Außerdem stellt sie sicher, dass die Dauer des Neustarts der Zeit für den Neustart der Dienste auf demselben Knoten entspricht, was auch die Wiederherstellungszeit nahezu null werden lässt.

Die letzte Komponente bilden die Streamingsicherungen. Dabei kann die Wiederherstellung der Daten länger dauern als bei einer Wiederherstellung auf VSS-Basis. Da dieses Szenario aber eine derart hohe Dienstverfügbarkeit bietet, muss eine Wiederherstellung zum Auffangen von Datenverlusten durch Ausfälle bei den Prozeduren nicht bedacht werden. Dies ermöglicht es, eine teure Verfügbarkeitslösung mit einer kostengünstigeren Sicherungslösung zu verknüpfen.

Zu den Nachteilen dieses Szenarios zählen die Kosten für die Serverhardware, die lange Dauer der Sicherungen und die langwierige Wiederherstellung der Datenbanken. Die Hardwarekosten lassen sich bei einem Einzelkopiocluster nicht vermeiden; sie stellen den Preis für optimalen Wiederherstellungspunkt und -zeit dar. Der zeitliche Aufwand für Sicherung und Wiederherstellung ist ebenfalls in der Lösung selbst begründet. Eine Alternative bilden Investitionen in eine VSS-basierte Lösung.

## **Einzelner Multifunktions-Postfachserver mit VSS**

Das dritte Szenario ist ein einzelner Multifunktions-Postfachserver mit VSS-Sicherungen. Hierbei sind mehrere Funktionen auf einem Server kombiniert, um eine Gesamtentität für eine Wiederherstellung bereitzustellen. Auf einem solchen Server sind normalerweise die Serverfunktionen Postfach, Hub-Transport und Clientzugriff zu finden. Die Kombination dieser Entität mit VSS-Sicherungen verbessert den Gesamtwiederherstellungspunkt und möglicherweise die Wiederherstellungszeit. Die Zusammenfassung von Funktionen führt dazu, dass die Umgebung aus folgender Hardware besteht:

- Ein Computer mit Windows Server 2003, auf dem zwei oder mehr Exchange Server 2007-Funktionen ausgeführt werden
- Ein Server zur Durchführung von Sicherungen, der nur für die Steuerung der Sicherungen zuständig ist

Dieses Szenario ist normalerweise so eingerichtet, dass die Wiederherstellung des Servers auf einem unmittelbar betriebsbereiten, einem betriebsbereiten oder einem einfachen Standbyserver an einem anderen Standort möglich ist. Die vorrangige Wiederherstellungsmethode ist eine VSS-Wiederherstellung auf demselben oder einem neuen physischen Server. Beim Implementieren eines derartigen Szenarios sind zwei wichtige Aspekte zu bedenken:

- Welche Menge an Datenverlust kann Ihre Umgebung verkraften (Wiederherstellungspunkt)?
- Innerhalb welcher Zeit muss Ihre Umgebung neu gestartet werden (Wiederherstellungszeit)?

Einzigartig bei diesem Szenario ist die Unmöglichkeit eines geplanten Failovers; jede Nichterreichbarkeit führt zum Dienstausschlag. Dies ist auch ein Hinweis auf die bei einem ungeplanten Failover erforderliche Zeit für die Wiederherstellung der Funktionen auf einem neuen Server. Der Vorgang umfasst das Hochfahren eines neuen Servers, wie es bereits im Abschnitt »Einen Exchange-Postfachserver wiederherstellen« beschrieben wurde.

Sowohl bei geplanten als auch bei ungeplanten Systemwiederherstellungen ist Datenverlust möglich, wenn die Datenbank vor der Wiederherstellung nicht sauber heruntergefahren wurde.

Die Nachteile sollten bei diesem Szenario deutlicher erkennbar sein als bei den beiden anderen: Es gibt keinen automatischen Failover der Exchange-Serverfunktionen, und die Wiederherstellung kann je nach Zustand des Bereitschaftsservers langwierig sein.

## **Bewerten der Beispielszenarien**

Die drei vorgestellten Szenarien sind mit Sicherheit nicht die einzigen Möglichkeiten. Sie wurden ausgewählt, um Ihnen die Breite der verfügbaren Lösungen aufzuzeigen und Ihnen zu verdeutlichen, welche Elemente der Konfiguration in Ihrer Umgebung Einfluss auf die drei wesentlichen Anforderungen haben.

Das erste Szenario zeigt eine Lösung mit geringen Kosten und hoher Verfügbarkeit mit einer teureren Lösung für Sicherung und Wiederherstellung. Dies ermöglicht einen zuverlässigen Failover-Mechanismus, der geringen Datenverlust in Kombination mit einem schnellen Sicherungs- und Wiederherstellungsmechanismus zulässt, um häufigere zeitpunktgenaue Kopien anzulegen, die sich bei Bedarf schnell wiederherstellen lassen.

Das zweite Szenario verwendet eine teurere Lösung mit hoher Verfügbarkeit in Verbindung mit einem preisgünstigeren Sicherungs- und Wiederherstellungsmechanismus. Dadurch müssen nur geringe oder gar keine Datenverluste und Ausfallzeiten hingenommen werden, während Sicherung und Wiederherstellung lange dauern.

Das dritte Szenario verwendet keine Lösung mit hoher Verfügbarkeit, sondern einen schnellen Sicherungs- und Wiederherstellungsmechanismus, der bei einem Ausfall eine schnelle Wiederherstellung ermöglicht. Diese Lösung ist häufig bei kleinen und mittelgroßen Unternehmen anzutreffen, aber auch bei großen, die eine andere Form hoher Verfügbarkeit nutzen.

**HINWEIS**

Eine häufige Erweiterung des dritten Szenarios besteht darin, in Verbindung mit dem Exchange-Multifunktionsserver die fortlaufende lokale Replikation einzusetzen. Die Replikation wird auf Speichergruppenebene implementiert, sodass ihr Umfang genauer konfiguriert werden kann, was für Organisationen mit knappem Budget wichtig ist.

## Empfohlene Vorgehensweisen

Um eine Operation erfolgreich zu sichern oder wiederherzustellen, sollten Sie sich an folgende Vorgehensweisen halten:

- Dokumentieren Sie Ihre Sicherungs- und Wiederherstellungsprozeduren.
- Sorgen Sie dafür, dass Kopien der Sicherungen an einem anderen Ort aufbewahrt werden.
- Überprüfen Sie Ihr System zum Überwachen und Protokollieren der Sicherung täglich, um zu gewährleisten, dass die Sicherungen des Exchange Server-Computers in der vorhergehenden Nacht erfolgreich verlaufen sind.
- Führen Sie monatlich oder vierteljährlich einen Sicherungs- und Wiederherstellungsversuch durch, um zu gewährleisten, dass Ihre Lösung funktioniert, und um in Übung zu bleiben.
- Technologien zur Deduplizierung sind gut für die Platzausnutzung Ihrer Sicherungsmedien.
- Wenn Sie Ihre Sicherungen auf Band speichern:
  - Reinigen Sie die Bandlaufwerke regelmäßig nach den Vorgaben des Herstellers.
  - Verwenden Sie die Bänder nicht zu lange. Sondern Sie sie aus, wenn sie die vom Hersteller angegebene maximale Zyklanzahl erreicht haben.
  - Sorgen Sie dafür, dass die Rohkapazität Ihres Bandes um einen Sicherheitszuschlag über die komprimierte Kapazität Ihrer Datenbank hinausgeht. Wenn nicht, planen Sie Bandwechsel bei der Sicherung ein.
- Wenn Sie Ihre Sicherungen auf Platten speichern:
  - Überprüfen Sie routinemäßig die Integrität der gespeicherten Daten.
  - Sorgen Sie dafür, dass die Rohkapazität Ihrer Sicherungsplatten um einen Sicherheitszuschlag über die komprimierte Kapazität Ihrer Datenbank hinausgeht. Wenn nicht, planen Sie für die Zukunft größere oder mehr Platten ein.

# Zusammenfassung

In diesem Kapitel kam eine Menge Stoff über Sicherung und Wiederherstellung zur Sprache. Es zeigte auf, wie die Wiederherstellung Ihrer Exchange-Datenbanken durchzuführen ist und welche allgemeinen Schritte bei der Wiederherstellung eines ganzen Servers zu befolgen sind, und gab einen kurzen Überblick darüber, wie sich VSS in Windows Server 2003 nutzen lässt, um die Wiederherstellungsdauer so gering wie möglich zu halten. Wenn Ihre Datenbanken beschädigt werden oder etwas schief geht, sollten Sie darauf achten, dass Sie Ihre Datenbanken und Ihre Exchange-Informationen mithilfe der in diesem Kapitel dargestellten Techniken wiederherstellen.