

# System Center Data Protection Manager 2007 Betriebshandbuch

---

Microsoft Corporation

Veröffentlicht: Sep 2007

## Zusammenfassung

Dieses Handbuch enthält Empfehlungen für die Überwachung und Verwaltung von DPM-Servern, Bandbibliotheken, geschützten Dateiservern und Workstations sowie von geschützten Servern, auf denen SQL Server, Exchange Server und Windows SharePoint Services ausgeführt wird. Des Weiteren finden Sie hier Anleitungen für die Wiederherstellung im Notfall.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der Microsoft Corporation zum Zeitpunkt der Veröffentlichung dar. Da Microsoft auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens Microsoft dar, und Microsoft kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Whitepaper dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIESES DOKUMENT JEDE GARANTIE AUS, SEI SIE AUSDRÜCKLICH ODER KONKLUDENT.

Es obliegt der Verantwortung der Benutzer, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Ohne Einschränkung der Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Genehmigung durch die Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt, in einem Datenempfangssystem gespeichert bzw. darin gelesen oder übertragen werden, unabhängig davon, in welcher Form oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies erfolgt.

Microsoft kann Inhaber von Patenten bzw. Patentanträgen, von Marken, Urheberrechten oder anderem geistigen Eigentum sein, die den Inhalt dieses Dokuments betreffen. Das Bereitstellen dieses Dokuments überträgt Ihnen keinerlei Anspruch auf diese

Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in schriftlichen Lizenzverträgen von Microsoft eingeräumt.

# Inhalt

---

Verwalten von DPM-Servern .....	9
Allgemeine DPM-Serverwartung .....	10
Verwenden von Windows-Wartungstools auf dem DPM-Server .....	10
Anwenden von Betriebssystem-Updates auf den DPM-Server .....	12
Ausführen von Antivirusprogrammen auf dem DPM-Server .....	13
Ausführen von DPM-Serververwaltungsaufgaben .....	14
Verwalten des DPM-Datenbank-Volumes .....	15
Suchen von DPM-Servern in Active Directory-Domänendiensten .....	15
Migrieren eines DPM-Servers zu neuer Hardware .....	16
Neustarten des DPM-Servers .....	17
Verschieben des DPM-Servers in eine neue Domäne .....	18
Umbenennen des DPM-Servers .....	19
Ändern der von DPM verwendeten SQL Server-Instanz .....	19
Koordinieren des zeitzonenübergreifenden Schutzes .....	20
Ändern der Zeitzone des DPM-Servers .....	21
Verwalten des Speicherpools .....	22
Hinzufügen von Datenträgern zum Speicherpool .....	23
Ersetzen von Datenträgern im Speicherpool .....	24
Entfernen von Datenträgern aus dem Speicherpool .....	25
Überwachen des DPM-Servers .....	25
Einrichten eines Überwachungszeitplans .....	26
Suchen nach Informationen .....	27
Methoden zur Überwachung von DPM .....	28
Überwachen mit der DPM-Verwaltungskonsole .....	29
Überwachen mit Berichten und Benachrichtigungen .....	36
Überwachen mit DPM Management Packs .....	37
Verwalten von geschützten Dateiservern und Workstations .....	38
Allgemeine Wartung von Dateiservern und Workstations .....	38
Verwenden von Windows-Wartungstools für Dateiserver und Workstations .....	39
Anwenden von Betriebssystem-Updates auf Dateiserver und Workstations .....	41
Ausführen von Antivirusprogrammen auf Dateiservern und Workstations .....	41
Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations .....	42
Ändern des Pfads einer Datenquelle .....	42
Verschieben von Dateiservern und Workstations zwischen Domänen .....	43
Umbenennen von Dateiservern oder Workstations .....	44
Ändern der Zeitzone von Dateiservern oder Workstations .....	45

Verwalten von Clusterdateiservern.....	46
Ändern der Mitglieder des Dateiserverclusters.....	46
Ändern der Ressourcengruppen auf Clusterdateiservern .....	47
Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird.....	48
Allgemeine Wartung von Servern, auf denen Exchange ausgeführt wird .....	48
Verwenden von Windows-Wartungstools auf Exchange-Servern .....	49
Ausführen von Exchange-Wartungsaufgaben.....	49
Anwenden von Betriebssystem-Updates auf Exchange-Server.....	50
Ausführen von Antivirusprogrammen auf Exchange-Servern .....	50
Ausführen von Exchange Server-Verwaltungsaufgaben .....	50
Aktualisieren von Exchange Server 2003 auf Exchange Server 2007.....	51
Verschieben von Exchange-Servern zwischen Domänen .....	51
Umbenennen von Exchange-Servern .....	52
Hinzufügen von Speichergruppen und Datenbanken.....	53
Aufheben der Bereitstellung von Datenbanken .....	53
Ändern des Pfads von Datenbanken oder Protokolldateien.....	54
Umbenennen von Speichergruppen.....	55
Verschieben von Datenbanken zwischen Speichergruppen .....	55
Verwalten von Exchange-Clustervern.....	56
Ändern der Mitglieder des Exchange-Serverclusters .....	56
Ändern der Ressourcengruppen auf Exchange-Clustervern.....	57
Wiederherstellen von Exchange-Daten .....	58
Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort.....	59
Wiederherstellen einer Datenbank am ursprünglichen Speicherort.....	60
Wiederherstellen einer Datenbank in einer anderen Datenbank.....	62
Kopieren von Exchange-Daten in einen Netzwerkordner.....	63
Kopieren von Exchange-Daten auf Band .....	65
Wiederherstellen von Postfächern.....	66
So stellen Sie ein Exchange 2003-Postfach wieder her .....	67
So stellen Sie ein Exchange 2007-Postfach wieder her .....	68
Wiederherstellen von Daten auf Clustervern.....	71
Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird.....	74
Allgemeine Wartung von Servern, auf denen SQL ausgeführt wird .....	74
Verwenden von Windows-Wartungstools auf SQL-Servern.....	75
Ausführen von SQL-Wartungsaufgaben.....	75
Anwenden von Betriebssystem-Updates auf SQL-Server.....	76
Ausführen von Antivirusprogrammen auf SQL-Servern .....	76

Ausführen von SQL Server-Verwaltungsaufgaben .....	76
Aktualisieren von SQL Server 2000 auf SQL Server 2005 .....	77
Verschieben von SQL-Servern zwischen Domänen .....	77
Umbenennen von Computern, auf denen SQL Server ausgeführt wird.....	78
Ändern des Wiederherstellungsmodells einer Datenbank .....	79
Ersetzen von Datenträgern auf einem SQL-Server.....	80
Hinzufügen von Datenbanken zu einem SQL-Server.....	80
Ändern des Pfads von SQL Server-Datenbanken.....	80
Umbenennen von SQL Server-Datenbanken.....	81
Verwalten von SQL-Clustervern.....	81
Ändern der Mitglieder des SQL-Serverclusters .....	81
Ändern der Ressourcengruppen auf SQL-Clustervern .....	82
Wiederherstellen von SQL Server-Daten.....	82
Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort.....	83
Wiederherstellen und Umbenennen von SQL-Datenbanken .....	84
Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server .....	85
Kopieren von SQL-Datenbanken in einen Netzwerkordner .....	86
Kopieren von SQL-Datenbanken auf Band .....	88
Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen.....	89
Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird.....	91
Allgemeine Wartung von Servern, auf denen Windows SharePoint Services ausgeführt wird .....	92
Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern .....	92
Ausführen von Windows SharePoint Services-Wartungsaufgaben .....	93
Anwenden von Betriebssystem-Updates auf Windows SharePoint Services-Servern .....	93
Ausführen von Antivirusprogrammen auf Windows SharePoint Services-Servern.....	93
Ausführen von Windows SharePoint Services-Verwaltungsaufgaben .....	94
Aktualisieren von Windows SharePoint Services .....	94
Verschieben von Windows SharePoint Services-Servern zwischen Domänen .....	95
Umbenennen von Windows SharePoint Services-Servern .....	95
Ändern des Front-End-Webservers.....	96
Hinzufügen von Datenbanken zu einer Windows SharePoint Services-Farm .....	98
Hinzufügen oder Entfernen von Servern in einer Windows SharePoint Services-Farm .....	98
Wiederherstellen von Windows SharePoint Services-Daten .....	98
Wiederherstellen von Windows SharePoint Services-Farmen.....	99
Wiederherstellen von Windows SharePoint Services-Sites .....	101
Wiederherstellen von Windows SharePoint Services-Elementen .....	103
Verwalten von geschützten virtuellen Servern .....	104
Allgemeine Wartung von Servern, auf denen Virtual Server ausgeführt wird .....	104
Verwenden von Windows-Wartungstools auf Virtual Server.....	105
Anwenden von Betriebssystem-Updates auf Virtual Server.....	105
Ausführen von Antivirusprogrammen auf Virtual Server .....	105

Ausführen von Virtual Server-Verwaltungsaufgaben .....	106
Verschieben von Virtual-Servern zwischen Domänen .....	106
Umbenennen von Virtual-Servern .....	107
Umbenennen von virtuellen Rechnern .....	108
Verschieben von virtuellen Rechnern oder virtuellen Festplatten .....	108
Schützen von Anwendungsdaten auf virtuellen Rechnern .....	108
Wiederherstellen von Virtual Server-Daten .....	109
Wiederherstellen des Virtual Server-Hosts .....	109
Wiederherstellen von virtuellen Rechnern .....	110
Wiederherstellen von virtuellen Rechnern als Dateien .....	112
Leistungsverwaltung .....	113
Auswirkungen von DPM auf die Leistung .....	114
Replikaterstellung .....	115
Änderungsnachverfolgung .....	116
Synchronisierung .....	116
Konsistenzprüfung .....	117
Vollständige Schnellsicherung .....	117
Sicherung auf Band .....	118
DPM-Prozesse .....	118
DPM und Arbeitsspeicher .....	119
Leistungsindikatoren .....	119
Verbessern der Leistung .....	122
Ändern von Arbeitsauslastungen .....	123
Verwenden der Netzwerk-Bandbreitenbeschränkung .....	124
Verwenden der Komprimierung über das Netzwerk .....	125
Staffeln von Startzeiten für die Synchronisierung .....	125
Planen von Konsistenzprüfungen .....	127
Manuelles Erstellen von Replikaten .....	127
Erhöhen der Kapazität .....	128
Verwalten der DPM-Leistung in einem WAN .....	128
Auswirkungen von Schutzgruppenänderungen auf Aufträge .....	129
Verwalten von Bandbibliotheken .....	131
Aktualisieren von Bandbibliotheksinformationen .....	131
Neuzuweisen von Bandlaufwerken .....	132
Deaktivieren von Bandbibliotheken und Bandlaufwerken .....	133
Entfernen von Bandbibliotheken .....	134
Verwalten des Bandkatalogs .....	134
Reinigen von Bandlaufwerken .....	135

Verwalten von Bändern .....	136
Hinzufügen und Entfernen von Bändern .....	136
Identifizieren von Bändern .....	137
Importieren von Bändern .....	139
Anzeigen von Bandinhalten .....	140
Austauschen von ausgelagerten Bändern.....	140
Kopieren von Bändern .....	140
Inventarisieren von Bändern.....	142
Wiederherstellen von auf Band gesicherten Daten .....	143
Wiederherstellen von Daten von Bändern, die von einem anderen DPM-Server erstellt wurden .....	143
Wiederherstellen von Daten, wenn ein Band eines Bandsets fehlt.....	143
Wiederherstellung im Notfall .....	144
Vorbereiten auf die Notfall-Wiederherstellung .....	144
Bewährte Verfahren für die Notfall-Wiederherstellung .....	146
Sichern des Systemstatus der geschützten Computer.....	147
Sichern von DPM-Servern .....	149
Sichern von DPM durch einen sekundären DPM-Server.....	149
Sichern von DPM-Datenbanken auf Band .....	152
Sichern von DPM durch Software von Drittanbietern.....	153
Sichern für die Bare-Metal-Recovery.....	157
Installieren des DPM System Recovery Tools .....	158
Konfigurieren für die Bare-Metal-Recovery .....	159
Wiederherstellung .....	160
Wechseln des Schutzes, wenn der primäre DPM-Server ausfällt.....	160
Wiederherstellen von geschützten Computern.....	162
Wiederherstellen von DPM-Servern .....	165
Wiederherstellen von DPM-Datenbanken .....	166
Wiederherstellen von DPM-Replikaten .....	166
Erneutes Einrichten des Schutzes nach dem Wiederherstellen des primären DPM-Servers.....	167
Ausführen einer Bare-Metal-Recovery .....	168
Verwenden von DpmSync .....	168
Verwenden von Skripten vor und nach Sicherungen .....	170
Anhang A: Kurzreferenz für DPM-Aufgaben.....	172
Anhang B: Schemaerweiterungen in DPM 2007 .....	173
Anhang C: Benutzerdefinierte Berichtansichten .....	177





# Verwalten von DPM-Servern

---

Als Systemadministrator verwalten Sie Server gewöhnlich in verschiedenen Rollen. Sie planen Ihre Wartungsroutinen den einzelnen Serverrollen entsprechend, und diese Rollen werden bei strukturellen Änderungen berücksichtigt, z. B. bei Änderungen des Servernamens oder des Serverstandorts. Was müssen Sie also beachten, wenn der Netzwerkstruktur die Rolle eines Servers, auf dem System Center Data Protection Manager (DPM) ausgeführt wird, hinzugefügt wird?

In diesem Abschnitt werden die häufigsten Wartungsaufgaben für DPM-Server beschrieben. Er enthält einen Leitfaden zum Ändern von Serverkonfigurationen nach dem Einrichten von DPM sowie zum Umgang mit verschiedenen Zeitzonen. Darüber hinaus finden Sie in diesem Abschnitt Informationen zur Konfiguration von Firewalls auf dem DPM-Server und den entsprechenden geschützten Computern, damit die Kommunikationsfähigkeit gewährleistet bleibt. In diesem Abschnitt finden Sie auch Empfehlungen zur Überwachung von DPM sowie eine Beschreibung der verschiedenen Überwachungsmethoden.

## In diesem Abschnitt

[Allgemeine DPM-Serverwartung](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

[Verwalten des Speicherpools](#)

[Überwachen des DPM-Servers](#)

## Siehe auch

[Wiederherstellung im Notfall](#)

[Leistungsverwaltung](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird](#)

[Verwalten von geschützten virtuellen Servern](#)

[Verwalten von Bandbibliotheken](#)

# Allgemeine DPM-Serverwartung

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- und Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßigen Sicherungen. Bei der Wartung von DPM-Servern sind einige Besonderheiten zu berücksichtigen.

## In diesem Abschnitt

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

[Anwenden von Betriebssystem-Updates auf den DPM-Server](#)

[Ausführen von Antivirusprogrammen auf dem DPM-Server](#)

## Siehe auch

[Verwalten des Speicherpools](#)

[Überwachen des DPM-Servers](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## Verwenden von Windows-Wartungstools auf dem DPM-Server

Im Allgemeinen können Sie den DPM-Server Ihrem regulären Wartungsplan hinzufügen und die mit Windows Server 2003 bereitgestellten Wartungstools verwenden. Sie müssen jedoch bei bestimmten Tools einige Besonderheiten beachten, wenn Sie sie mit DPM verwenden. Diese Tools sind in der folgenden Tabelle aufgeführt.

### Windows-Wartungstools und DPM

Windows-Tool	Besonderheiten
<b>Datenträgerbereinigung:</b> Dient dem Entfernen temporärer Dateien, Dateien im Internetcache und nicht erforderlicher Programmdateien.	Die Datenträgerbereinigung steht für Replikatvolumen im DPM-Speicherpool nicht zur Verfügung.

Windows-Tool	Besonderheiten
<p><b>Datenträgerdefragmentierung:</b> Dient dem Analysieren des Fragmentierungsgrads von Volumes und dem Defragmentieren von Volumes.</p>	<p>Sie sollten die Datenträgerdefragmentierung nicht für Datenträger ausführen, die Mitglieder des Speicherpools auf dem DPM-Server sind. Im Knowledge Base-Artikel 312067 wird das Problem mit der Datenträgerdefragmentierung wie folgt erklärt:</p> <p>Der Systemschattenkopieanbieter verwendet ein Copy-on-Write-Verfahren, das auf einer 16-KB-Block-Ebene arbeitet. Dies geschieht unabhängig von der Größe der Clusterzuordnungseinheiten des Dateisystems. Wenn die Clustergröße des Dateisystems kleiner als 16 KB ist, kann der Systemschattenkopieanbieter nicht gut erkennen, dass die Datenträgerdefragmentierung-E/A sich von der typischen Schreib-E/A unterscheidet, und führt demzufolge einen Copy-on-Write-Vorgang aus. Dies kann dazu führen, dass der Schattenkopie-Speicherbereich sehr schnell zunimmt. Wenn der Speicherbereich das benutzerdefinierte Limit erreicht, werden die ältesten Schattenkopien gelöscht.</p> <p>Weitere Informationen zu diesem Problem finden Sie, in englischer Sprache, im Microsoft Knowledge Base-Artikel <a href="http://go.microsoft.com/fwlink/?LinkId=65210">Shadow copies may be lost when you defragment a volume</a> (http://go.microsoft.com/fwlink/?LinkId=65210).</p>
<p><b>Chkdsk.exe:</b> Dient der Fehlerüberprüfung des Dateisystems und der Dateisystemmetadaten sowie dem Anzeigen eines entsprechenden Statusberichts.</p>	<p>Führen Sie chkdisk nicht für DPM-Replikate und Wiederherstellungspunkt-Volumes aus. Chkdsk verursacht das Unmounten der Volumes, und falls Daten während des Unmountens des Wiederherstellungspunkt-Volumes auf das Replikatvolume geschrieben werden, kann dies zu einem vollständigen Verlust der Wiederherstellungspunkte führen.</p>

## **Siehe auch**

[Anwenden von Betriebssystem-Updates auf den DPM-Server](#)

[Ausführen von Antivirusprogrammen auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

[Verwenden von Windows-Wartungstools auf SQL-Servern](#)

[Verwenden von Windows-Wartungstools auf Exchange-Servern](#)

[Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern](#)

[Verwenden von Windows-Wartungstools auf virtuellen Servern](#)

## **Anwenden von Betriebssystem-Updates auf den DPM-Server**

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Updates, „Fixes“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können sowohl für DPM-Server als auch geschützte Computer die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Server Update Services. Da für einige Softwareupdates der Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

Informieren Sie sich regelmäßig, ob Updates für DPM und die erforderliche Software verfügbar sind. Die folgende Software ist für DPM erforderlich:

- Microsoft .NET Framework 2.0
- Microsoft Software Quality Metrics (SQM)
- Microsoft SQL Server 2005
- Microsoft SQL Server 2005 Service Pack 1 (SP1)

Updates für DPM sind über Microsoft Update verfügbar. Dies ist ein Service von Microsoft, der Aktualisierungen aus dem Microsoft Update Catalog anbietet. Der Microsoft Update Catalog ist ein Repository für Microsoft-Softwareaktualisierungen und enthält Updates, die Sicherheit und Zuverlässigkeit betreffen. Der Microsoft Update-Dienst fragt den Microsoft Update Catalog ab, um festzustellen, welche Aktualisierungen für den Computer, auf dem Microsoft Update installiert ist, verfügbar sind.

Sie können Microsoft Update jederzeit abonnieren; besuchen Sie dazu die [Microsoft Update-Website](http://go.microsoft.com/fwlink/?LinkId=41291) (<http://go.microsoft.com/fwlink/?LinkId=41291>).

## **Siehe auch**

[Ausführen von Antivirusprogrammen auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

## Ausführen von Antivirusprogrammen auf dem DPM-Server

Um Dateikonflikte zwischen DPM und dem Antivirusprogramm zu vermeiden, deaktivieren Sie auf dem DPM-Server die Echtzeitüberwachung der folgenden Verzeichnisse in den DPM-Programmdateien durch das Antivirusprogramm:

- \XSD
- \Temp\MTA

DPM ist mit den meisten verbreiteten Antivirusprogrammen kompatibel. Allerdings kann die Leistung von DPM durch Antivirusprogramme beeinträchtigt werden. Fehlerhafte Einstellungen können sogar Beschädigungen von Daten in Replikaten und Wiederherstellungspunkten verursachen. Ziehen Sie Folgendes in Betracht, um diese Probleme zu verringern:

- **Deaktivieren Sie die Echtzeitüberwachung von Msdpmsagent.exe auf dem DPM-Server.**

Zum Minimieren der Leistungsbeeinträchtigung deaktivieren Sie im Antivirusprogramm für alle geschützten Volumes die Echtzeitüberwachung der Replikate und Übertragungsprotokolle, indem Sie die Echtzeitüberwachung des DPM-Prozesses dpmra.exe im Ordner Programme\Microsoft Data Protection Manager\DPM\bin deaktivieren.

Bei der Echtzeitüberprüfung von Replikaten wird die Leistung beeinträchtigt, da das Antivirusprogramm bei jeder Synchronisierung von DPM mit dem geschützten Server die Replikate scannt und bei Änderungen, die DPM an den Replikaten vornimmt, alle betroffenen Dateien scannt. Wenn Sie diese Funktion für Replikate deaktivieren, ist das Problem jedoch behoben. Informationen zum Konfigurieren der Echtzeitüberwachung anhand des Prozessnamens entnehmen Sie bitte der Produktdokumentation für Ihr Antivirusprogramm.

- **Deaktivieren Sie die Echtzeitüberwachung von csc.exe auf dem DPM-Server.**

Wenn Sie bei der Verwendung der DPM-Verwaltungskonsole eine Leistungsverschlechterung bemerken, deaktivieren Sie die Echtzeitüberwachung des Prozesses csc.exe, der sich im Ordner Windows\Microsoft.net\Framework\v2.0.50727\csc.exe befindet. Der Prozess csc.exe ist der C#-Compiler. Die Leistung wird durch Echtzeitüberwachung des Prozesses csc.exe beeinträchtigt, da das Antivirusprogramm Dateien überprüft, die durch den Prozess csc.exe beim Erstellen von XML-Meldungen ausgegeben werden. Informationen zum Konfigurieren der Echtzeitüberwachung anhand des Prozessnamens entnehmen Sie bitte der Produktdokumentation für Ihr Antivirusprogramm.

- **Löschen Sie infizierte Dateien auf den geschützten Servern und auf dem DPM-Server.**

Um Datenbeschädigung in Replikaten und Wiederherstellungspunkten zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von DPM nicht erkannt werden.

Wenn DPM versucht, ein Replikat zu synchronisieren, das von einem anderen Programm geändert wurde, können Datenbeschädigungen im Replikat und in den Wiederherstellungspunkten verursacht werden. Dieses Problem wird behoben, indem Sie das Antivirusprogramm so konfigurieren, dass infizierte Dateien gelöscht werden. Informationen zur Konfiguration finden Sie im Produkthandbuch des Antivirusprogramms.

 **Wichtig**

Jedes Mal, wenn das Antivirusprogramm eine Datei des Replikats löscht, müssen Sie eine manuelle Synchronisierung mit Konsistenzprüfung ausführen, auch wenn das Replikat nicht als inkonsistent gekennzeichnet wird.

## Siehe auch

[Anwenden von Betriebssystem-Updates auf den DPM-Server](#)

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

# Ausführen von DPM-Serververwaltungsaufgaben

In diesem Abschnitt finden Sie Anleitungen und Richtlinien für die Verwaltung des DPM-Servers und zum Vornehmen von Änderungen nach der erstmaligen DPM-Konfiguration.

## In diesem Abschnitt

[Verwalten des DPM-Datenbank-Volumes](#)

[Suchen von DPM-Servern in Active Directory-Domänendiensten](#)

[Migrieren eines DPM-Servers zu neuer Hardware](#)

[Neustarten des DPM-Servers](#)

[Verschieben des DPM-Servers in eine neue Domäne](#)

[Umbenennen des DPM-Servers](#)

[Ändern der von DPM verwendeten SQL Server-Instanz](#)

[Koordinieren des zeitzoneübergreifenden Schutzes](#)

[Ändern der Zeitzone des DPM-Servers](#)

## Siehe auch

[Verwalten des Speicherpools](#)

[Überwachen des DPM-Servers](#)

[Allgemeine DPM-Serverwartung](#)

## Verwalten des DPM-Datenbank-Volumes

Der Speicherort der DPM-Datenbank (DPMDB) wird während der DPM-Installation festgelegt. Wenn Sie die von DPM installierte dedizierte Instanz von SQL Server verwenden, wird DPMDB standardmäßig unter C:\Programme\Microsoft DPM\DPM\DPMDB gespeichert. Wenn Sie eine vorhandene Instanz von SQL Server für DPM verwenden, ist der Standardspeicherort von DPMDB der Pfad auf dem SQL Server, in dem sich die SQL-Datenbanken befinden.

Um festzustellen, welche Instanz von SQL Server von DPM verwendet wird, klicken Sie in der DPM-Verwaltungskonsole auf das Info-Symbol.

Der Speicherplatz auf dem Volume, auf dem DPMDB gespeichert wird, kann durch die folgenden Methoden vergrößert werden:

- Löschen nicht benötigter Dateien von diesem Volume (zum Beispiel temporäre Dateien)
- Vergrößern der Volumes

### Siehe auch

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## Suchen von DPM-Servern in Active Directory-Domänendiensten

Mithilfe von Active Directory-Domänendiensten können von Benutzern oder Programmen Informationen über Verzeichnisobjekte abgefragt werden. Beim Installieren von DPM auf einem Mitgliedsserver einer Domäne wird in den Active Directory-Domänendiensten ein Dienstverbindungspunkt registriert. Mit den Informationen, die mit dem Dienstverbindungspunkt registriert werden, können Sie in den Active Directory-Domänendiensten nach Computern suchen, auf denen DPM ausgeführt wird.



### Hinweis

Wird DPM auf einem Server installiert, der nicht Mitglied einer Domäne ist, und wird dieser Server anschließend einer Domäne hinzugefügt, so wird der Dienstverbindungspunkt nicht in den Active Directory-Domänendiensten registriert.

Um in Active Directory-Domänendiensten nach DPM-Servern zu suchen, verwenden Sie ein Abfragetool wie z. B. Adsiedit, mit dem Sie nach allen Computern in der Domäne suchen können, die über einen Dienstverbindungspunkt „serviceClassName=MSDPM“ verfügen.



### Hinweis

Adsiedit ist ein Microsoft Management Console (MMC)-Snap-In, das mit den Windows Server 2003-Supporttools installiert wird. Weitere Informationen zur Verwendung von Adsiedit finden Sie, in englischer Sprache, unter [Adsiedit Overview](#) im Windows Server 2003 TechCenter (<http://go.microsoft.com/fwlink/?LinkId=50377>).

### ▶ So installieren Sie Windows Server 2003-Supporttools

1. Legen Sie die Windows Server 2003-CD ein.
2. Wechseln Sie in das Verzeichnis \support\tools.
3. Doppelklicken Sie auf den Dateinamen suptools.msi.

### ▶ So suchen Sie mithilfe von Adsiedit nach DPM-Servern

1. Führen Sie adsiedit.msc aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Domäne**, zeigen Sie auf **Neu**, und klicken Sie anschließend auf **Abfrage**.
3. Geben Sie einen Namen für die Abfrage ein, z. B. „MSDPM Servers“.
4. Wählen Sie den Knoten **Computer** als Stamm der Suche aus.
5. Geben Sie unter **Abfragezeichenfolge** die Zeichenfolge **serviceClassName=MSDPM** ein.
6. Klicken Sie auf **OK**, um unter dem Knoten **Domäne** einen Knoten für die Abfrage anzuzeigen.
7. Wählen Sie den Abfrageknoten aus; im Listenbereich werden die Server angezeigt, auf denen DPM installiert ist.

### Siehe auch

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## Migrieren eines DPM-Servers zu neuer Hardware

Damit der Schutz der Datenquellen und die Verfügbarkeit der Wiederherstellungspunkte während des Migrationsprozesses gewährleistet bleiben, sollten Sie einen Plan für den DPM-Server-Migrationsprozess erstellen und dabei die folgenden Punkte berücksichtigen:

- Das Service-Level-Agreement (SLA), das für den Zeitraum der Migration aufrecht erhalten werden soll.
- Die Zeitdauer, über die der vorhandene DPM-Server betrieben werden kann, bevor er ausgemustert oder für andere Zwecke verwendet wird.
- Wartungsfenster für die geschützten Computer.



### ► So migrieren Sie einen DPM-Server zu neuer Hardware

1. Installieren Sie DPM auf einem neuen Server. Weitere Informationen hierzu finden Sie, in englischer Sprache, unter [Installing DPM](http://go.microsoft.com/fwlink/?LinkId=91851) (<http://go.microsoft.com/fwlink/?LinkId=91851>).
2. Identifizieren Sie einen geschützten Computer, der migriert werden soll, und führen Sie die folgenden Schritte aus:
  - a. Beenden Sie auf dem vorhandenen DPM-Server den Schutz für alle Daten, legen Sie fest, dass Replikate für diesen geschützten Computer beibehalten werden, und deinstallieren Sie den Schutz-Agent.
  - b. Starten Sie den Zielcomputer neu.
  - c. Installieren Sie den Schutz-Agent vom neuen DPM-Server auf dem ausgewählten Computer.
  - d. Starten Sie den geschützten Computer neu.
  - e. Wiederholen Sie diese Schritte für alle geschützten Computer.
3. Erstellen Sie auf dem neuen DPM-Server Schutzgruppen für die geschützten Computer. Weitere Informationen finden Sie, in englischer Sprache, unter [Configuring DPM](http://go.microsoft.com/fwlink/?LinkId=91852) (<http://go.microsoft.com/fwlink/?LinkId=91852>).
4. Warten Sie den vorher verwendeten DPM-Server, bis die Wiederherstellungspunkte von inaktiven Replikaten nicht mehr benötigt werden.

### Siehe auch

[Ausführen von DPM-Serververwaltungsaufgaben](#)

### Neustarten des DPM-Servers

Sollte ein Neustart des DPM-Servers notwendig sein, überprüfen Sie in der DPM-Verwaltungskonsolle im Aufgabenbereich **Überwachung**, ob zurzeit Aufträge durchgeführt werden, und befolgen Sie diese Richtlinien:

- Wenn zurzeit keine Aufträge ausgeführt werden oder für die Zeit geplant sind, die für den Neustart erforderlich ist, starten Sie den DPM-Server neu.
- Wenn eine Synchronisierung mit Konsistenzprüfung ausgeführt wird, starten Sie den DPM-Server neu. Die Synchronisierung mit Konsistenzprüfung wird zum nächsten geplanten Zeitpunkt fortgesetzt; Sie können den Auftrag jedoch auch manuell neu starten.
- Wenn ein Replikaterstellungsauftrag ausgeführt wird, verschieben Sie den Neustart, bis der Auftrag abgeschlossen ist. Wenn der Neustart nicht verschoben werden kann, müssen Sie nach dem Neustart des DPM-Servers die Synchronisierung mit Konsistenzprüfung für das Replikat manuell ausführen.

- Wenn Synchronisierungen oder vollständige Schnellsicherungen für die Zeit des Neustarts geplant ist, verschieben Sie den Neustart, bis die Wiederherstellungspunkte erstellt sind, oder führen Sie nach dem Neustart des DPM-Servers die Synchronisierungen und das Erstellen der Wiederherstellungspunkte manuell aus.
- Wenn Aufträge ausgeführt werden, die die Bandbibliothek verwenden, verschieben Sie den Neustart, bis die Aufträge abgeschlossen sind. Kann der Neustart nicht verschoben werden, werden die folgenden Auftragstypen durch den Neustart abgebrochen und müssen nach dem Neustart erneut ausgeführt werden:
  - Sicherung auf Band
  - Kopieren auf Band
  - Wiederherstellen vom Band
  - Bandüberprüfung
- Wenn Sie ein Band löschen, verschieben Sie den Neustart, bis der aktuelle Auftrag abgeschlossen ist. Brechen Sie ausstehende Bandlöschaufträge ab, starten Sie den Computer neu, und planen Sie die abgebrochenen Bandlöschaufträge neu.

### **Siehe auch**

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## **Verschieben des DPM-Servers in eine neue Domäne**

Es wird empfohlen, die Domäne des DPM-Servers nicht zu ändern, da hierbei alle Schutz- und Wiederherstellungsvorgänge fehlschlagen.

Wenn es sich nicht umgehen lässt, die Domänenmitgliedschaft eines DPM-Servers zu ändern, müssen Sie den Schutz der Schutzgruppenmitglieder, die diesem DPM-Server zugeordnet sind, beenden und den Schutz dieser Datenquellen dann neu starten. Dazu fügen Sie sie entweder Schutzgruppen auf einem anderen DPM-Server hinzu, oder Sie fügen sie neuen Schutzgruppen auf demselben DPM-Server hinzu, nachdem Sie dessen Domäne geändert haben.

### **Siehe auch**

[Ausführen von DPM-Serververwaltungsaufgaben](#)

[Umbenennen des DPM-Servers](#)

## Umbenennen des DPM-Servers

Es wird empfohlen, den Namen des DPM-Servers nicht zu ändern, da hierbei alle Schutz- und Wiederherstellungsvorgänge fehlschlagen.

Wenn es sich nicht umgehen lässt, den Namen eines DPM-Servers zu ändern, müssen Sie den Schutz der Schutzgruppenmitglieder, die diesem DPM-Server zugeordnet sind, beenden und den Schutz dieser Datenquellen dann neu starten. Dazu fügen Sie sie entweder Schutzgruppen auf einem anderen DPM-Server hinzu, oder Sie fügen sie neuen Schutzgruppen auf demselben DPM-Server hinzu, nachdem Sie dessen Namen geändert haben.

### Siehe auch

[Verschieben des DPM-Servers in eine neue Domäne](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## Ändern der von DPM verwendeten SQL Server-Instanz

DPM verwendet eine spezifische Instanz von SQL Server für die Speicherung der Datenbank. Sie legen während der DPM-Installation fest, welche Instanz von SQL Server DPM verwendet. Die von einem DPM-Server verwendete Instanz von SQL Server kann nur durch eine Deinstallation und erneute Installation von DPM geändert werden.

Gehen Sie folgendermaßen vor, wenn Sie die SQL Server-Instanz für einen DPM-Server ändern müssen:

1. Stellen Sie sicher, dass Sie über eine aktuelle Sicherungskopie der DPM-Datenbank (DPMDB) verfügen.
2. Deinstallieren Sie DPM, und legen Sie dabei fest, Daten beizubehalten.
3. Installieren Sie DPM, und wählen Sie eine neue Instanz von SQL Server. Weitere Informationen hierzu finden Sie, in englischer Sprache, unter [Installing DPM](#) (<http://go.microsoft.com/fwlink/?LinkId=91851>).
4. Führen Sie eine Wiederherstellung der DPMDB auf der neuen Instanz von SQL Server aus, führen Sie DpmSync aus, und führen Sie eine Konsistenzprüfung für die vom DPM-Server geschützten Datenquellen aus.

Der Prozess ist von der Verfügbarkeit einer Sicherungskopie der DPM-Datenbank abhängig. Weitere Informationen zum Sichern und Wiederherstellen der DPM-Datenbank finden Sie unter [Wiederherstellung im Notfall](#).

### Siehe auch

[Ausführen von DPM-Serververwaltungsaufgaben](#)

[Installieren von DPM](#)

## Koordinieren des zeitzoneübergreifenden Schutzes

In einer Active Directory-Domäne wird die Systemzeit der Server entsprechend der für jeden Server konfigurierten Zeitzone synchronisiert. Wenn ein DPM-Server jedoch Dateiserver schützt, die sich in einer anderen Zeitzone als der DPM-Server befinden, müssen Sie die Zeitunterschiede beim Planen von Aufträgen, Prüfen von Berichten, Verwalten von Warnungen und Ausführen von Datenwiederherstellungen berücksichtigen.

### Zeitanzeige in DPM

Aufträge zur Synchronisierung und zum Erstellen von Wiederherstellungspunkten werden von DPM automatisch entsprechend der Zeitzone des geschützten Computers geplant. In allen anderen Bereichen der DPM-Verwaltungskonsole werden die Systemzeiten entsprechend der Zeitzone des DPM-Servers angezeigt. Zwar werden die Aufträge entsprechend der Zeitzone des geschützten Computers geplant, die Startzeiten und die Zeiten für die Wiederherstellungspunkte der Aufträge werden jedoch in der Zeitzone des DPM-Servers angezeigt.

Angenommen, der DPM-Server befindet sich in Berlin und ein geschützter Dateiserver in Reykjavik, wo es zwei Stunden früher ist. Wenn Sie die Synchronisierung und den Wiederherstellungspunkt für 18:00 Uhr planen, werden diese Aufträge um 18:00 Uhr Reykjaviker Zeit ausgeführt, also entsprechend der Zeit des Dateiservers. Wenn jedoch ein Benutzer in Reykjavik eine Datenwiederherstellung in den Zustand von 18:00 Uhr des vorangegangenen Tages anfordert, müssen Sie die Schattenkopien von 20:00 Uhr Berliner Zeit suchen, da in der DPM-Wiederherstellungsbenutzeroberfläche die Zeiten der Wiederherstellungspunkte entsprechend der Zeitzone des DPM-Servers angezeigt werden.

In der DPM-Verwaltungskonsole wird im Aufgabenbereich „Wiederherstellung“ in der Spalte **Zuletzt geändert** das Datum und die Uhrzeit der neuesten Änderungen an der Datei angezeigt. Bei diesen Änderungen kann es sich um Änderungen am Inhalt oder um Änderungen an den Metadaten handeln.

Arbeitszeiten für Netzwerk-Bandbreitenbeschränkung verwenden die Zeitzone des geschützten Computers.

### Planen der ersten Replikaterstellung

Aufträge zur ersten Replikaterstellung werden mithilfe der Zeit des DPM-Servers geplant; es können keine Aufträge für Zeitpunkte geplant werden, die in der Vergangenheit der DPM-Serverzeit liegen, auch wenn diese Zeitpunkte in der Zukunft der Dateiserverzeit liegen. Im Beispiel des DPM-Servers in Berlin, der einen Dateiserver in Reykjavik schützt, besteht ein Zeitunterschied von zwei Stunden zwischen den beiden Serverzeiten. Sie können um 21:00 Uhr Berliner Zeit nicht das Ausführen einer ersten Replikaterstellung für den Dateiserver in Reykjavik um 20:00 Uhr am selben Tag planen, obwohl es in Reykjavik noch nicht 20:00 Uhr ist, da dieser Zeitpunkt für den DPM-Server in Berlin in der Vergangenheit liegt.

Die erste Replikaterstellung wird entsprechend der Zeit des geschützten Computers ausgeführt. Wenn Sie also die erste Replikaterstellung für den Dateiserver in Reykjavik für 21:00 Uhr an einem bestimmten Tag planen, wird der Auftrag um 21:00 Uhr Reykjaviker Zeit an diesem Tag ausgeführt.

Angenommen, der DPM-Server in Berlin schützt außerdem einen Dateiserver in Sofia, wo es eine Stunde später als in Berlin ist. Um 20:00 Uhr in Berlin planen Sie die erste Replikaterstellung für den Dateiserver in Sofia für 20:30 Uhr. Dies ist möglich, da 20:30 Uhr für den Dateiserver in der Zukunft liegt. Da es in Sofia jedoch schon nach 20:30 Uhr ist, wird sofort mit der ersten Replikaterstellung begonnen.

## Sommerzeit in DPM

DPM erkennt während der Installation des Schutz-Agents automatisch die Zeitzone eines geschützten Computers. Vorausgesetzt, sowohl der DPM-Server als auch der geschützte Dateiserver befinden sich in Zeitzonen, in denen die gleichen Regelungen für die Sommerzeit gelten, berücksichtigt DPM automatisch Beginn und Ende der Sommerzeit. Befinden sich der DPM-Server und der geschützte Computer jedoch in Zeitzonen, in denen unterschiedliche Regelungen für die Sommerzeit gelten – z. B. wenn sich der DPM-Server in einer Zeitzone befindet, in der die Zeitumstellung durchgeführt wird, der geschützte Server jedoch nicht – wird die Berücksichtigung des Zeitunterschieds zwischen DPM-Server und Dateiserver gestört.

Um dieses Problem zu lösen, können Sie den DPM-Server zwingen, den Zeitunterschied neu einzustellen, indem Sie den Schutz der Datenquellen beenden und die Datenquellen dann wieder den Schutzgruppen hinzufügen.

## Siehe auch

[Ändern der Zeitzone von Dateiservern und Workstations](#)

[Ändern der Zeitzone des DPM-Servers](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## Ändern der Zeitzone des DPM-Servers

Mit dem nachstehend beschriebenen Verfahren können Sie die Zeitzone des DPM-Servers ändern.

### So ändern Sie die Zeitzone des DPM-Servers

1. Schließen Sie die DPM-Verwaltungskonsolle.
2. Beenden Sie den DPM-Dienst (MsDpm.exe).
3. Ändern Sie die Zeitzone des DPM-Servers in der Systemsteuerung auf der Registerkarte **Zeitzone** im Dialogfeld **Eigenschaften von Datum und Uhrzeit**.
4. Öffnen Sie die DPM-Verwaltungskonsolle. Mit dieser Aktion wird auch der DPM-Dienst wieder gestartet.

5. Klicken Sie in der DPM-Verwaltungskontrolle auf **Optionen** im Bereich **Aktion**.
6. Ändern Sie im Dialogfeld **Optionen** auf der Registerkarte **AutoErmittlung** die Uhrzeit, zu der die AutoErmittlung ausgeführt werden soll, und klicken Sie auf **OK**.

Indem Sie den Zeitplan für die AutoErmittlung ändern, werden alle DPM-Aufträge mit der neuen Zeitzone des DPM-Servers neu generiert.

## Siehe auch

[Ändern der Zeitzone von Dateiservern und Workstations](#)

[Koordinieren des zeitzonenübergreifenden Schutzes](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

## Verwalten des Speicherpools

Der Speicherpool ist ein Satz von Datenträgern, auf denen der DPM-Server die Replikate und Wiederherstellungspunkte für geschützte Daten speichert. DPM kann Folgendes für den Speicherpool verwenden:

- Direct Attached Storage (DAS)
- Fibre-Channel-Speicherbereichsnetzwerk (SAN)
- iSCSI-Speichergerät oder SAN

Vom Speicherpool werden die meisten Festplattentypen unterstützt, einschließlich Integrated Drive Electronics (IDE), Serial Advanced Technology Attachment (SATA) und SCSI. Außerdem werden die Partitionsstile MBR (Master Boot Record) und GPT (GUID Partition Table) unterstützt. USB/1394-Datenträger können dem Speicherpool nicht hinzugefügt werden.

DPM kann keinen Speicherplatz von bereits vorhandenen Volumes auf Datenträgern, die dem Speicherpool hinzugefügt werden, verwenden. Auch wenn auf einem bereits bestehenden Volume auf einem Speicherpoolatragner noch Speicherplatz verfügbar ist, kann DPM nur Speicherplatz auf von DPM erstellten Volumes nutzen. Damit der gesamte Speicherplatz des Datenträgers für den Speicherpool verfügbar ist, löschen Sie bereits vorhandene Volumes auf dem Datenträger, und fügen Sie diesen dann dem Speicherpool hinzu.

### **Wichtig**

Einige Originalcomputerhersteller (OEMs) bieten eine Diagnosepartition an, die von mitgelieferten Medien installiert werden. Diese Diagnosepartition wird manchmal auch als OEM-Partition oder EISA-Partition bezeichnet. EISA-Partitionen müssen von Festplatten entfernt werden, bevor Sie diese dem DPM-Speicherpool hinzufügen können.

## In diesem Abschnitt

[Hinzufügen von Datenträgern zum Speicherpool](#)

[Ersetzen von Datenträgern im Speicherpool](#)

[Entfernen von Datenträgern aus dem Speicherpool](#)

## Siehe auch

[Überwachen des DPM-Servers](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

[Allgemeine DPM-Serverwartung](#)

## Hinzufügen von Datenträgern zum Speicherpool

DPM kann keinen Speicherplatz von bereits vorhandenen Volumes auf Datenträgern, die dem Speicherpool hinzugefügt werden, verwenden. Auch wenn auf einem bereits bestehenden Volume auf einem Speicherpoolatragner noch Speicherplatz verfügbar ist, kann DPM nur Speicherplatz auf von DPM erstellten Volumes nutzen. Damit der gesamte Speicherplatz des Datenträgers für den Speicherpool verfügbar ist, löschen Sie bereits vorhandene Volumes auf dem Datenträger, und fügen Sie diesen dann dem Speicherpool hinzu.

DPM prüft regelmäßig die Datenträger und Volumes im Speicherpool und aktualisiert den Speicherplatz im Speicherpool. Wenn Sie dem Speicherpool einen Datenträger hinzufügen, der ein Volume enthält, und dieses Volume später löschen, fügt DPM nach dem erneuten Prüfen des Datenträgers den nicht zugewiesenen Speicher dem verfügbaren Speicherpool hinzu.

Wenn der Name eines Datenträgers auf der Registerkarte **Datenträger** im Aufgabenbereich **Verwaltung** der DPM-Verwaltungskonsolle als „Unbekannt“ angezeigt wird, können Sie diesen Datenträger erst dann zum Speicherpool hinzufügen, nachdem der Datenträgername korrigiert wurde. Um dieses Problem zu beheben, gehen Sie wie nachstehend beschrieben vor.

### So korrigieren Sie einen Datenträgernamen

1. Erweitern Sie im **Geräte-Manager** den Eintrag **Laufwerke**.
2. Klicken Sie mit der rechten Maustaste auf jeden als „Laufwerk“ aufgeführten Datenträger, und wählen Sie **Deinstallieren**.



#### Hinweis

Alle Datenträger ohne Anzeigenamen werden als „Laufwerk“ aufgeführt.

Ein Beispiel für einen Anzeigenamen ist „HITACHI\_DK23EB-40“.

3. Klicken Sie im Menü **Aktion** auf **Nach geänderter Hardware suchen**, um den Datenträger neu zu installieren.

## Siehe auch

[Ersetzen von Datenträgern im Speicherpool](#)

[Entfernen von Datenträgern aus dem Speicherpool](#)

## Ersetzen von Datenträgern im Speicherpool

Falls ein Datenträger im Speicherpool ausfällt, können Sie ihn mit dem folgenden Verfahren ersetzen.

### ► So ersetzen Sie einen Datenträger im Speicherpool

1. Identifizieren Sie in der Konsole **Datenträgerverwaltung** die Replikatvolumes und Volumes mit Wiederherstellungspunkten, die auf dem ausgefallenen Datenträger gespeichert sind.
2. Entfernen Sie den Schutz von den Datenquellen, die über Replikatvolumes und Volumes mit Wiederherstellungspunkten auf dem ausgefallenen Datenträger verfügen, und wählen Sie **Geschützte Daten löschen**.
3. Bauen Sie den zu ersetzenden Datenträger aus.
4. Bauen Sie den Ersatzdatenträger ein.
5. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**, und klicken Sie dann auf die Registerkarte **Datenträger**.
6. Wählen Sie den Datenträger aus, den Sie entfernt haben, und klicken Sie im Bereich **Aktionen** auf **Entfernen**.
7. Klicken Sie im Bereich **Aktionen** auf **Hinzufügen**.
8. Wählen Sie im Bereich **Verfügbare Datenträger** den Ersatzdatenträger aus, klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **OK**.
9. Fügen Sie die Datenquellen aus Schritt 2. einer vorhandenen Schutzgruppe hinzu, oder erstellen Sie eine neue Schutzgruppe für diese Datenquellen.
  - a. Wenn Sie eine neue Schutzgruppe erstellen und über eine Sicherungskopie der Datenquellen auf Band verfügen, erstellen Sie die Replikate mithilfe dieser Bandsicherungen manuell.
  - b. Wenn Sie eine neue Schutzgruppe erstellen und nicht über eine Sicherungskopie der Datenquellen auf Band verfügen, lassen Sie zu, dass DPM die Replikate über das Netzwerk erstellt.
  - c. Wenn Sie die Datenquellen einer vorhandenen Schutzgruppe hinzufügen, startet DPM eine sofortige Konsistenzprüfung, wodurch die Replikate neu erstellt werden.



#### **Hinweis**

Weitere Informationen finden Sie, in englischer Sprache, in der TechNet Library unter [Configuring DPM](http://go.microsoft.com/fwlink/?LinkId=91852) (<http://go.microsoft.com/fwlink/?LinkId=91852>).

### **Siehe auch**

[Hinzufügen von Datenträgern zum Speicherpool](#)

[Entfernen von Datenträgern aus dem Speicherpool](#)



## Entfernen von Datenträgern aus dem Speicherpool

Ein Speicherpooldatenträger ist physisch an den DPM-Server angeschlossen und auf Programmbasis durch DPM mit dem Speicherpool verbunden.

Wenn ein Datenträger, der zum Speicherpool gehört, ausgebaut wird oder ausfällt, gibt DPM eine Warnung aus, dass ein Volume fehlt. Das fehlende Volume wird auch auf der Registerkarte **Datenträger** im Aufgabenbereich **Verwaltung** angezeigt.

Im Bereich **Details** der Warnung über das fehlende Volume sehen Sie einen Link zum Entfernen des Datenträgers aus dem Speicherpool. Wenn Sie auf diesen Link klicken, entfernen Sie die Verbindung auf Programmebene.

Wenn Sie den Datenträger aus dem Speicherpool entfernen und später wieder online bringen, kann DPM nicht auf die Daten auf diesem Datenträger zugreifen. Wenn DPM einen Datenträger als „fehlendes Volume“ kennzeichnet und Sie den Datenträger nicht aus dem Speicherpool entfernen, weist DPM die Volumes auf dem Datenträger neu zu, wenn Sie den Datenträger wieder online bringen, und kann auf die vorhandenen Daten zugreifen.

### Siehe auch

[Hinzufügen von Datenträgern zum Speicherpool](#)

[Ersetzen von Datenträgern im Speicherpool](#)

## Überwachen des DPM-Servers

Nachdem Sie den Schutz von Daten eingerichtet haben, sollten Sie die DPM-Aktivität überwachen, um eine ordnungsgemäße Funktion zu gewährleisten und gegebenenfalls auftretende Probleme zu behandeln. Die Überwachung ist entscheidend, um einen Überblick über vergangene, aktuelle und geplante Vorgänge zu erhalten. Durch eine Überwachung von DPM können Sie sicherstellen, dass alle Aktivitäten zum Schutz von Daten ordnungsgemäß durchgeführt werden, und dass Sie über gegebenenfalls auftretende Fehler und Warnungen benachrichtigt werden.



### Hinweis

Informationen zur Überwachung der Serverleistung finden Sie unter [Leistungsverwaltung](#).

### In diesem Abschnitt

[Einrichten eines Überwachungszeitplans](#)

[Suchen nach Informationen](#)

[Methoden zur Überwachung von DPM](#)

## Siehe auch

[Leistungsverwaltung](#)

[Verwalten des Speicherpools](#)

[Ausführen von DPM-Serververwaltungsaufgaben](#)

[Allgemeine DPM-Serververwaltung](#)

## Einrichten eines Überwachungszeitplans

Nachdem Sie mit dem Schutz der Daten begonnen haben, muss in die DPM-Vorgänge nur noch wenig eingegriffen werden. Wenn in einer Situation Maßnahmen erforderlich sind, werden Sie durch eine Warnung darüber informiert. Informationen zum Reagieren auf Warnungen finden Sie, in englischer Sprache, in der DPM-Hilfe unter [Resolving Alerts](#) (<http://go.microsoft.com/fwlink/?LinkId=102159>). Es wird empfohlen, dass Sie einen Überwachungszeitplan einrichten und diesen regelmäßig befolgen, sodass Sie über Trends und Probleme informiert sind und schnell auf Probleme reagieren können, die Ihr Eingreifen erfordern. In der folgenden Tabelle sind Vorschläge für einen Überwachungszeitplan aufgeführt.

### Vorschlag für einen Überwachungszeitplan

Intervall	Zu überprüfende Quellen	Zu überprüfende Informationen
Täglich	<ul style="list-style-type: none"><li>• Kritische und andere Warnungen</li><li>• E-Mail-Benachrichtigungen (falls konfiguriert)</li><li>• Statusbericht</li></ul>	Probleme mit Replikaten, Probleme mit der Synchronisierung und dem Erstellen von Wiederherstellungspunkten, Probleme mit Agents, Aufträge, die auf Band warten, fehlgeschlagene Sicherungen
Monatlich	Berichte: <ul style="list-style-type: none"><li>• Status</li><li>• Bandverwaltung</li><li>• Datenträgerauslastung</li></ul>	Trends und Muster, die auf (mögliche) Probleme hindeuten
Bei Bedarf	Status von Wiederherstellungsaufträgen	Fehler bei Wiederherstellungsaufträgen

## Siehe auch

[Suchen nach Informationen](#)

[Leistungsverwaltung](#)

[Methoden zur Überwachung von DPM](#)

## Suchen nach Informationen

Nach Implementieren des Überwachungszeitplans werden Sie bestimmte Trends feststellen und einige Warnungen bemerken. Sie können die Warnungen und damit verbundene Probleme untersuchen, Fehler beheben oder einige der Trends analysieren. DPM stellt verschiedene Ressourcen zur Durchführung dieser Aufgaben bereit. In der folgenden Tabelle sind einige Referenzen aufgeführt, mit denen Sie nach Informationen suchen können, die bei der Beantwortung häufiger Fragen hilfreich sind.

### Informationsquellen

Fragestellung	Quelle
Ist mein Eingreifen erforderlich? Sind auf geschützten Computern Änderungen vorhanden, die sich auf den Schutz von Daten auswirken?	<ul style="list-style-type: none"> <li>Ggf. abonnierte E-Mail-Benachrichtigungen mit Warnungen</li> <li>Aufgabenbereich <b>Überwachung</b>, Registerkarte <b>Warnungen</b></li> </ul>
Wurden alle für gestern geplanten Sicherungen korrekt ausgeführt? Gibt es wiederkehrende Probleme? Werden Wiederherstellungsziele erfüllt?	<ul style="list-style-type: none"> <li>Statusbericht</li> <li>Schutzbericht</li> </ul>
Muss dem Speicherpool Speicherplatz hinzugefügt werden?	<ul style="list-style-type: none"> <li>Aufgabenbereich <b>Überwachung</b>, Registerkarte <b>Warnungen</b></li> <li>Datenträgerauslastungsbericht</li> </ul>
Wann werden Aufträge durchgeführt? Wie viel Zeit nahm die letzte Konsistenzprüfung in Anspruch? Welche Datenmenge wurde durch den neuesten Synchronisierungsauftrag übertragen?	Aufgabenbereich <b>Überwachung</b> , Registerkarte <b>Aufträge</b>
Wie viele Wiederherstellungspunkte stehen für eine Datenquelle zur Verfügung? Sind alle Replikate konsistent?	<ul style="list-style-type: none"> <li>Aufgabenbereich <b>Schutz</b>, Bereich <b>Details</b></li> <li>Aufgabenbereich <b>Wiederherstellung</b></li> </ul>
Welche Bänder sind in der Bibliothek verfügbar? Welche Daten befinden sich auf den einzelnen Bändern?	Aufgabenbereich <b>Verwaltung</b> , Registerkarte <b>Bibliotheken</b>

Fragestellung	Quelle
Wurde ein Wiederherstellungsauftrag erfolgreich abgeschlossen?	<ul style="list-style-type: none"> <li>• Aufgabenbereich <b>Überwachung</b>, Registerkarte <b>Warnungen</b></li> <li>• Aufgabenbereich <b>Überwachung</b>, Registerkarte <b>Aufträge</b></li> <li>• E-Mail-Benachrichtigung (falls beim Starten einer Wiederherstellung E-Mail-Benachrichtigungen abonniert werden)</li> </ul>
Kann der DPM-Server mit jedem geschützten Computer eine Verbindung herstellen?	Aufgabenbereich <b>Verwaltung</b> , Registerkarte <b>Agents</b>
Welchen Status hat der DPM-Dienst?	<ul style="list-style-type: none"> <li>• MMC (Microsoft Management Console), Dienste-Snap-In</li> <li>• Ereignisprotokoll bei Dienstfehlern</li> </ul>
Welche Probleme sind im letzten Monat aufgetreten?	<ul style="list-style-type: none"> <li>• Statusbericht</li> <li>• Aufgabenbereich <b>Überwachung</b>, Registerkarte <b>Warnungen</b>, mit ausgewählter Option <b>Inaktive Warnungen anzeigen</b></li> </ul>
Welchen Status haben die DPM-Server und die von diesen geschützten Computer?	MOM-Operatorenkonsole, <b>Statusansicht</b>
Warum kann für ein Schutzgruppenmitglied kein Wiederherstellungspunkt erstellt werden?	Statusbericht

## Siehe auch

[Einrichten eines Überwachungszeitplans](#)

[Leistungsverwaltung](#)

[Methoden zur Überwachung von DPM](#)

## Methoden zur Überwachung von DPM

Sie können die folgenden Methoden verwenden, um den Schutz von Daten zu überwachen:

- Mit der DPM-Verwaltungskonsole zeigen Sie DPM-Vorgänge an, die auf einem bestimmten DPM-Server ausgeführt werden.
- Konfigurieren Sie DPM, um Berichte und Benachrichtigungen über Warnungen per E-Mail zu senden. Anleitungen hierzu finden Sie, in englischer Sprache, in der DPM-Hilfe unter [How to Create or Modify Report Subscriptions](#) ( <http://go.microsoft.com/fwlink/?LinkId=102161>).

- Überwachen Sie Vorgänge für mehrere DPM-Server mithilfe von System Center Data Protection Manager (DPM) Management Pack für Microsoft Operations Manager 2005 (MOM) oder System Center Operations Manager 2007.
- Überwachen Sie die Instanz von SQL Server, die DPM installiert, mit System Center SQL Server Management Pack für Microsoft Operations Manager 2005.

## In diesem Abschnitt

[Überwachen mit der DPM-Verwaltungskonsole](#)

[Überwachen mit Berichten und Benachrichtigungen](#)

[Überwachen mit DPM Management Packs](#)

## Siehe auch

[Einrichten eines Überwachungszeitplans](#)

[Suchen nach Informationen](#)

[Leistungsverwaltung](#)

## Überwachen mit der DPM-Verwaltungskonsole

Damit Sie die DPM-Verwaltungskonsole verwenden können, müssen Sie sich beim DPM-Server unter einem Benutzerkonto mit Administratorberechtigungen für diesen Server anmelden.

In diesem Abschnitt werden die einzelnen Aufgabenbereiche der DPM-Verwaltungskonsole erläutert und es wird beschrieben, welche Informationen durch die Aufgabenbereiche jeweils bereitgestellt werden.

- [Aufgabenbereich Überwachung](#)
- [Aufgabenbereich Schutz](#)
- [Aufgabenbereich Verwaltung](#)



### Hinweis

Sie brauchen nicht jeden Aufgabenbereich in der DPM-Verwaltungskonsole zu überwachen. Weitere Informationen finden Sie unter [Einrichten eines Überwachungszeitplans](#).

### Aufgabenbereich Überwachung

Der Aufgabenbereich **Überwachung** enthält zwei Registerkarten: **Aufträge** und **Warnungen**.

Zu Überwachungszwecken finden Sie auf der Registerkarte **Warnungen** die wichtigeren Informationen. Sie sollten die Registerkarte **Warnungen** täglich überprüfen, um rechtzeitig Probleme zu erkennen und zu beheben, die den erfolgreichen Schutz von Daten verhindern könnten.

## **Aufgabenbereich Überwachung: Warnungen**

Auf der Registerkarte **Warnungen** finden Sie die folgenden Informationen:

- Aktuelle Probleme (wichtige Warnungen)
- Potenzielle Probleme (Warnungen)
- Wichtige Aktivitäten (Informationswarnungen)
- Empfohlene Maßnahmen

Auf der Registerkarte **Warnungen** werden Fehler, Warnungen und Informationsmeldungen angezeigt. Warnungen können nach Schutzgruppe, Server oder Schweregrad gruppiert werden. Sie können außerdem auswählen, ob nur aktive Warnungen oder sowohl aktive als auch inaktive Warnungen (deren Ursache bereits behoben wurde) angezeigt werden. Darüber hinaus können Sie Benachrichtigungen abonnieren, sodass Sie Warnungen per E-Mail empfangen.

Von DPM wird sichergestellt, dass auf der Registerkarte **Warnungen** die Probleme wiedergegeben werden, die im System zurzeit aktiv sind. Wenn das Problem behoben wird, durch das eine Warnung erzeugt wurde, wird diese Warnung inaktiv. Tatsächlich müssen für viele Probleme, für die eine Warnung ausgegeben wird, keinerlei Maßnahmen ergriffen werden, da diese Probleme auf eine vorübergehende Situation zurückzuführen sind oder automatisch behoben werden. Beispielsweise kann die Ursache für die Warnung, dass der DPM-Server keine Verbindung zu einem geschützten Computer herstellen kann, ein vorübergehendes Netzwerkproblem sein, und ein weiterer Versuch ist unter Umständen erfolgreich. In manchen Fällen wird eine Informationswarnung von DPM nach einer vordefinierten Zeitdauer automatisch als inaktiv festgelegt. Die Warnung „Wiederherstellungssammlung erfolgreich abgeschlossen“ wird beispielsweise zwei Tage nach Abschluss der Wiederherstellung inaktiv.

Sie können Warnungen in DPM auch selbst als inaktiv kennzeichnen. Sie können Warnungen aus verschiedenen Gründen als inaktiv kennzeichnen, zum Beispiel, wenn eine Warnung keine Bedeutung mehr hat oder Sie nicht planen, das Problem zu beheben. Angenommen, Sie sehen Warnungen für die letzten drei Tage, dass eine Datenquelle, für die tägliche Bandsicherungen geplant sind, nicht gesichert wurde. Sie entscheiden sich, nur den letzten fehlgeschlagenen Sicherungsauftrag zu wiederholen. Die Warnungen für die früheren fehlgeschlagenen Sicherungsaufträge können Sie als inaktiv kennzeichnen.

Wenn Sie eine Warnung als inaktiv kennzeichnen, ändert sich der Schutzstatus der Schutzgruppe zu **OK** in der DPM-Verwaltungskonsolle und im DPM Management Pack.

Weitere Informationen finden Sie, in englischer Sprache, unter „Resolving Alerts“ in der Data Protection Manager-Hilfe.

Als allgemeine Richtlinie wird folgende Vorgehensweise empfohlen:

- Zeigen Sie aktive Warnungen an, wenn Sie Ihr Augenmerk auf aktive, aktuelle Probleme richten möchten.
- Verwenden Sie inaktive Warnungen als Informationsquelle, um Trends zu ermitteln oder Probleme zu analysieren.
- Kennzeichnen Sie Warnungen nur dann als inaktiv, wenn Sie sicher sind, dass Sie das Problem nicht beheben müssen.

 **Hinweis**

Das Kennzeichnen von Warnungen als inaktiv sollte für jeden Einzelfall sorgfältig geprüft werden und nur vorgenommen werden, wenn es wirklich notwendig ist.

### **Aufgabenbereich Überwachung: Aufträge**

Auf der Registerkarte **Aufträge** finden Sie die folgenden Informationen:

- Ausführungszeitpunkt von Aufträgen
- Zeitplan für die Ausführung von Aufträgen
- Welche Aufträge eines bestimmten Typs geplant sind
- Welche Aufträge für einen geschützten Computer geplant sind
- Welche Aufträge für eine Schutzgruppe geplant sind
- Welche Aufträge nicht erfolgreich abgeschlossen wurden sowie die Ursache dafür
- Ausführungsdauer von Aufträgen
- Die für einen Auftrag übertragene Datenmenge
- Anzahl der Dateien, die bei einer Konsistenzprüfung überprüft wurden
- Welche Band- und Bibliotheksressourcen verwendet wurden

Auf der Registerkarte **Aufträge** wird der Status von Aufträgen angezeigt. Sie können Aufträge nach Schutzgruppe, Server, Status oder Typ gruppieren. Es ist auch möglich, Filter zu erstellen, um die Auftragsansicht an eine Kombination aus bestimmten Parametern anzupassen.

Ausführliche Informationen zu einzelnen Aufträgen stehen nur auf der Registerkarte **Aufträge** im Bereich **Details** zur Verfügung. Ausführliche Informationen zu Auftragsfehlern können für die erweiterte Problembehandlung von Nutzen sein.

Sie können auswählen, ob Sie in der Auftragsliste auch regelmäßig geplante Synchronisierungsvorgänge anzeigen möchten. Es ist jedoch nicht erforderlich, Synchronisierungsaufträge regelmäßig zu überwachen, da Probleme gegebenenfalls auf der Registerkarte **Warnungen** angezeigt werden.

### **Aufgabenbereich Schutz**

Auf der Registerkarte **Schutz** finden Sie folgende Informationen:

- Status von Volumes und Freigaben in den einzelnen Schutzgruppen
- Konfiguration jeder Schutzgruppe, z. B. Wiederherstellungsziele, Datenträgerzuweisung und Schutzzeitplan

Im Aufgabenbereich **Schutz** wird der Status jedes geschützten Elements bereitgestellt angezeigt.

### **Aufgabenbereich Verwaltung**

Der Aufgabenbereich **Verwaltung** enthält drei Registerkarten: **Datenträger**, **Agents** und **Bibliotheken**.

#### **Aufgabenbereich Verwaltung: Datenträger**

Auf der Registerkarte **Datenträger** finden Sie folgende Informationen:

- Kapazität von Datenträgern im Speicherpool (belegter und freier Speicherplatz)
- Status von Datenträgern im Speicherpool
- Welche geschützten Volumes sich auf den einzelnen Datenträgern befinden

Auf der Registerkarte **Datenträger** wird eine Liste mit Datenträgern im Speicherpool angezeigt. Außerdem können Sie an dieser Stelle Datenträger zum Pool hinzufügen oder entfernen.

#### **Aufgabenbereich Verwaltung: Agents**

Auf der Registerkarte **Agents** finden Sie folgende Informationen:

- Version bereitgestellter Agents
- Status bereitgestellter Agents
- Verfügbarkeit von Agent-Lizenzen

Auf der Registerkarte **Agents** wird eine Liste von Datei-Agents angezeigt, die auf Dateiservern bereitgestellt werden. Außerdem können Sie an dieser Stelle Agents installieren und deinstallieren sowie Agents und Agent-Lizenzen aktualisieren.

#### **Aufgabenbereich Verwaltung: Bibliotheken**

Auf der Registerkarte **Bibliotheken** finden Sie die folgenden Informationen:

- Status der Bandbibliotheken und der eigenständigen Bandlaufwerke
- Status einzelner Bänder

Auf der Registerkarte **Bibliotheken** wird eine Liste der Bibliotheken und Bandlaufwerke, die an den DPM-Server angeschlossen sind, angezeigt. Außerdem können Sie an dieser Stelle Bänder inventarisieren, hinzufügen und entfernen.



## Aufgabenbereich Berichterstellung

Im Aufgabenbereich **Berichterstellung** haben Sie die folgenden Möglichkeiten:

- Berichte zu DPM-Vorgängen erstellen und anzeigen
- automatische Berichterstellung planen
- Reporting Services-Einstellungen verwalten
- Berichtübermittlung per E-Mail abonnieren

Die Berichterstellungsfunktionen in DPM basieren auf Microsoft SQL Server Reporting Services. SQL Server Reporting Services enthält ein Berichts-Manager-Tool, das nicht mit DPM installiert wird. Da mit dem Berichts-Manager festgelegte Einstellungen Konflikte mit DPM-Einstellungen hervorrufen können, wird empfohlen, das in SQL Server Reporting Services enthaltene Berichts-Manager-Tool nicht zu installieren.

Sie können die DPM-Berichterstellungsfunktion nach der Installation und Konfiguration von DPM jederzeit aktivieren. Um jedoch sicherzustellen, dass DPM über ausreichende Informationen zum Erstellen sinnvoller Berichtsdaten verfügt, wird empfohlen, nach Beginn der Aktivitäten zum Schutz von Daten mit dem Anzeigen von Berichten noch wenigstens einen Tag zu warten. Eine Anleitung zum Aktivieren der DPM-Berichterstellung finden Sie, in englischer Sprache, in der DPM-Hilfe unter „[Using Reports](http://go.microsoft.com/fwlink/?LinkId=102085)“ (<http://go.microsoft.com/fwlink/?LinkId=102085>).




### Hinweis

Wenn ein DPM-Server eine große Anzahl von Dateiservern schützt, sollten Sie den Zeitplan für die Bereitstellung von E-Mail-Berichten zeitlich staffeln. Wenn Ihre Planung das Senden aller Berichte zur selben Zeit vorsieht, können die Speichereinschränkungen von SQL Server Reporting Services möglicherweise das Senden einiger Berichte verhindern.

In der folgenden Tabelle werden die verfügbaren Berichte zusammengefasst und deren Verwendung kurz beschrieben. Informationen zur Interpretation der Berichtsdaten finden Sie, in englischer Sprache, in der DPM-Hilfe unter „[Report Types](http://go.microsoft.com/fwlink/?LinkId=102086)“ (<http://go.microsoft.com/fwlink/?LinkId=102086>).

## DPM-Berichte

Name des Berichts	Zusammenfassung des Inhalts
Status	<p>Der Statusbericht gibt den Status aller Wiederherstellungspunkte für einen bestimmten Zeitraum an, führt Wiederherstellungsaufträge auf und zeigt die Gesamtzahl erfolgreicher und fehlgeschlagener Wiederherstellungspunkte sowie die Erstellungen festplatten-gestützter und bandgestützter Wiederherstellungspunkte an. Dieser Bericht zeigt Trends in der Fehlerhäufigkeit auf und listet die Anzahl der Warnungen auf.</p> <p>Anhand dieses Berichts können Sie die folgenden Fragen beantworten:</p> <ul style="list-style-type: none"><li>• Was ist gestern passiert? Letzte Woche? Letzten Monat?</li><li>• Was war erfolgreich, und was ist fehlgeschlagen?</li><li>• Welche Fehlertrends gibt es? Welche Fehler treten am häufigsten auf?</li><li>• Werden die Wiederherstellungsziele erreicht, die im Service-Level-Agreement (SLA) festgelegt wurden?</li></ul> <p> <b>Hinweis</b></p> <p>Der Statusbericht enthält die Fehlercodes für alle Warnungen, die während des Berichtszeitraums aufgezeichnet wurden. Die Fehlermeldungen, die mit den einzelnen Fehlercodes verknüpft sind, finden Sie, in englischer Sprache, im <a href="http://go.microsoft.com/fwlink/?LinkId=91861">Error Code Catalog</a> (<a href="http://go.microsoft.com/fwlink/?LinkId=91861">http://go.microsoft.com/fwlink/?LinkId=91861</a>).</p>
Bandverwaltung	<p>Im Bandverwaltungsbericht finden Sie Details zur Bandrotation und -entnahme, und es wird überprüft, dass der Grenzwert freier Medien nicht überschritten wird.</p> <p>Mit diesem Bericht können Sie den Bandaustausch zwischen den Bibliotheken und Offsite-Standorten verwalten.</p>
Bandauslastung	<p>Der Bandauslastungsbericht stellt eine Übersicht über die Ressourcenauslastung (Festplatte/Band) im Laufe der Zeit zur Verfügung, um die Kapazitätsplanung zu erleichtern.</p> <p>Dieser Bericht ist hilfreich, wenn Sie Entscheidungen über Bandzuweisungen und den Erwerb von Bändern treffen.</p>

Name des Berichts	Zusammenfassung des Inhalts
Schutz	<p>Der Schutzbericht enthält die gebräuchlichen Metriken für erfolgreiche Sicherungen über einen langen Zeitraum, um den Überblick über die Sicherungen zu behalten.</p> <p>Mit diesem Bericht können Sie ermitteln, welche Computer oder Schutzgruppen erfolgreich gesichert wurden.</p>
Wiederherstellung	<p>Der Wiederherstellungsbericht enthält die gebräuchlichen Metriken für erfolgreiche Wiederherstellungen über einen langen Zeitraum, um den Überblick über die Wiederherstellungen zu behalten.</p> <p>Mit diesem Bericht können Sie feststellen, wie erfolgreich Sie bezüglich der im Service-Level-Agreement festgelegten Ziele für Wiederherstellungszeiten und Erfolgsgarantien waren.</p>
Datenträgerauslastung	<p>Der Datenträgerauslastungsbericht stellt eine Übersicht über die Datenträgerkapazität, -zuweisung und -auslastung im DPM-Speicherpool bereit.</p> <p>Mit diesem Bericht können Sie die folgenden Aufgaben durchführen:</p> <ul style="list-style-type: none"> <li>• Datenträgerauslastungstrends ermitteln</li> <li>• Darüber entscheiden, ob Datenträgerzuweisungen für Schutzgruppen geändert und dem Speicherpool Datenträger hinzugefügt werden</li> <li>• Feststellen, wie viele Datenträgerressourcen die einzelnen Computer mit DPM verwenden</li> </ul>

**Siehe auch**

[Leistungsverwaltung](#)

[Überwachen des DPM-Servers](#)

[Überwachen mit DPM Management Packs](#)

[Überwachen mit Berichten und Benachrichtigungen](#)

## Überwachen mit Berichten und Benachrichtigungen

Benachrichtigungen erleichtern Routineaufgaben bei der Überwachung. Statt eine Verbindung mit der DPM-Verwaltungskonsolle herzustellen, um gegebenenfalls vorhandene wichtige Warnungen anzuzeigen, können Sie E-Mails abonnieren, um die folgenden Informationen zu erhalten:

- Einige oder alle DPM-Berichte mit benutzerdefiniertem Format und Zeitplan.
- Individuelle Benachrichtigung für jede Warnung des abonnierten Typs und eine Benachrichtigung, wenn die Warnung aufgehoben wurde.

Wenn Sie Benachrichtigungen aktivieren oder Berichte abonnieren, sollten Sie in Betracht ziehen, in Microsoft Office Outlook eine Regel einzurichten, um Benachrichtigungs- und Berichts-E-Mails in einen oder mehrere Posteingangsortner zu filtern. Sie können diese E-Mails mithilfe der **Absenderadresse** oder der Betreffzeile filtern. Die **Absenderadresse** der E-Mail-Nachrichten, die Benachrichtigungen oder Berichte enthalten, geben Sie beim Konfigurieren des SMTP-Servers als Adresse an.

Die Tabelle **Betreffzeilen in E-Mail-Benachrichtigungen** enthält eine Liste mit Betreffzeilen, die in den einzelnen Typen von Warnbenachrichtigungen und DPM-Berichten verwendet werden. Sie können mit dem Text in diesen Betreffzeilen Regeln in Outlook einrichten, um Berichte und Warnbenachrichtigungen in bestimmte Ordner zu filtern. Mit Operations Manager können Sie Ihre E-Mail-Benachrichtigungen anpassen.

### Betreffzeilen in E-Mail-Benachrichtigungen

E-Mail-Typ	Betreffzeile
Warnbenachrichtigung	<ul style="list-style-type: none"><li>• DPM: Informationsbenachrichtigung von (Name des geschützten Computers)</li><li>• DPM: Warnungsbenachrichtigung von (Name des geschützten Computers)</li><li>• DPM: Wichtige Benachrichtigung von (Name des geschützten Computers)</li><li>• DPM: Wiederherstellungsbenachrichtigung von (Name des geschützten Computers)</li></ul>
Benachrichtigung über aufgelöste Warnung	<ul style="list-style-type: none"><li>• DPM: Aufgelöst von (Name des geschützten Computers)</li></ul>
Bericht	<ul style="list-style-type: none"><li>• Statusbericht vom angegebenen Server</li><li>• Medienverwaltungsbericht vom angegebenen Server</li><li>• Schutzbericht vom angegebenen Server</li><li>• Wiederherstellungsbericht vom angegebenen Server</li><li>• Bandauslastungsbericht vom angegebenen Server</li><li>• Datenträgerauslastungsbericht vom angegebenen Server</li></ul>

## **Siehe auch**

[Leistungsverwaltung](#)

[Überwachen des DPM-Servers](#)

[Überwachen mit der DPM-Verwaltungskonsole](#)

[Überwachen mit DPM Management Packs](#)

## **Überwachen mit DPM Management Packs**

Die System Center Data Protection Manager 2007 Management Packs für Operations Manager (MOM) ermöglichen es Administratoren, mit einem MOM-Verwaltungsserver den Schutz von Daten, den Status, den Zustand und die Leistung von mehreren DPM-Servern und den von ihnen geschützten Computern zentral zu überwachen.

Mit der Operations Manager Operator-Operatorkonsole kann ein Administrator gleichzeitig DPM und die Netzwerkinfrastruktur überwachen und auf diese Weise Probleme beim Schutz von Daten im Zusammenhang mit anderen Faktoren der System- und Netzwerkleistung analysieren. Mit derselben Konsole kann der Administrator andere wichtige Anwendungen wie Microsoft SQL Server und Microsoft Exchange Server überwachen.

Vom Operations Manager-Server aus können Administratoren die folgenden Überwachungsaufgaben für verwaltete DPM-Server und die von ihnen geschützten Computer durchführen:

- Zentrales Überwachen von Zustand und Status des Schutzes von Daten und von wichtigen Leistungsindikatoren mehrerer DPM-Server und den von ihnen geschützten Computern.
- Anzeigen des Status aller Rollen auf DPM-Servern und Computerservern.
- Überwachen aktionsgebundener DPM-Warnungen in Zusammenhang mit Replikaterstellung, Synchronisierung und Erstellung von Wiederherstellungspunkten. DPM Management Pack filtert Warnungen heraus, für die keine Aktion erforderlich ist, z. B. ein gerade ausgeführter Synchronisierungsauftrag.
- Überwachen des Status des Arbeitsspeichers, der CPU und von Datenträgerressourcen auf DPM-Servern und Anzeigen von DPM-Datenbankfehlern über Operations Manager-Warnungen.
- Überwachen von Ressourcennutzung und Leistungstrends für DPM-Server.
- Problemdiagnose und -behandlung auf einem remoten DPM-Server.

Die DPM Management Packs gehören nicht zum Lieferumfang von DPM. Die Management Packs stehen auf der [DPM Management Pack-Downloadsite](http://go.microsoft.com/fwlink/?linkid=50208) (<http://go.microsoft.com/fwlink/?linkid=50208>) zum Herunterladen zur Verfügung.

## **Siehe auch**

[Leistungsverwaltung](#)

[Überwachen des DPM-Servers](#)

[Überwachen mit der DPM-Verwaltungskonsole](#)

[Überwachen mit Berichten und Benachrichtigungen](#)

# Verwalten von geschützten Dateiservern und Workstations

---

In diesem Abschnitt finden Sie Informationen über die Ausführung häufiger Wartungsaufgaben für geschützte Dateiserver und Workstations sowie einen Leitfaden für das Ändern der Computerkonfiguration oder Clusterkonfiguration, wenn der Computer oder Cluster von DPM geschützt wird.

## In diesem Abschnitt

[Allgemeine Wartung von Dateiservern und Workstations](#)

[Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations](#)

[Verwalten von Clusterdateiservern](#)

## Siehe auch

[Wiederherstellung im Notfall](#)

[Verwalten von DPM-Servern](#)

[Leistungsverwaltung](#)

[Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird](#)

[Verwalten von geschützten virtuellen Servern](#)

[Verwalten von Bandbibliotheken](#)

## Allgemeine Wartung von Dateiservern und Workstations

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- und Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßigen Sicherungen.

Wenn Sie Wartungsaufgaben für einen geschützten Servers ausführen müssen und für den Zeitraum der Wartungsarbeiten keine Schutzaufträge fortgesetzt werden sollen, können Sie den Schutz-Agent mit dem folgenden Verfahren deaktivieren.

### Hinweis

Wenn Sie einen Schutz-Agent für einen Server deaktivieren, der ein Clusterknoten ist, sollten Sie den Schutz-Agent für jeden Knoten des Clusters deaktivieren.

### ► So deaktivieren Sie einen Schutz-Agent

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Wählen Sie auf der Registerkarte **Agents** im Anzeigebereich den Namen des Computers mit dem zu deaktivierenden Schutz-Agent aus.
3. Klicken Sie im Bereich **Aktionen** auf **Schutz-Agent deaktivieren**.
4. Klicken Sie im Dialogfeld auf **OK**, um zu bestätigen, dass Sie den Vorgang fortsetzen möchten.

## In diesem Abschnitt

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

[Anwenden von Betriebssystem-Updates auf Dateiserver und Workstations](#)

[Ausführen von Antivirusprogrammen auf Dateiservern und Workstations](#)

## Siehe auch

[Verwalten von Clusterdateiservern](#)

[Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations](#)

## Verwenden von Windows-Wartungstools für Dateiserver und Workstations

Im Allgemeinen können Sie die Wartung von Dateiservern und Workstations, die von DPM geschützt werden, nach Ihrem gewohnten Wartungszeitplan und mit den vom Betriebssystem angebotenen Wartungstools fortführen. Diese Tools und mögliche Auswirkungen auf den Schutz von Daten sind in der folgenden Tabelle aufgeführt.

## Windows-Wartungstools und geschützte Computer

Windows-Tool	Besonderheiten
<b>Datenträgerbereinigung:</b> Dient dem Entfernen temporärer Dateien, Dateien im Internetcache und nicht erforderlicher Programmdateien.	Das Ausführen der Datenträgerbereinigung sollte keine negativen Auswirkungen auf die Leistung oder den Schutz von Daten haben.
<b>Datenträgerdefragmentierung:</b> Dient dem Analysieren des Fragmentierungsgrads von Volumes und dem Defragmentieren von Volumes.	Bevor Sie ein Volume einer Schutzgruppe hinzufügen, überprüfen Sie das Volume auf Defragmentierung, und defragmentieren Sie es ggf. mit dem Tool Datenträgerdefragmentierung. Wenn Schutz auf extrem fragmentierte Volumes angewendet wird, braucht der geschützte Computer länger zum Starten, und Schutzaufträge können fehlschlagen.  Es wird empfohlen, die Datenträgerbereinigung auszuführen, bevor die Datenträgerdefragmentierung ausgeführt wird.
<b>Chkdsk.exe:</b> Dient der Fehlerüberprüfung des Dateisystems und der Dateisystemmetadaten sowie dem Anzeigen eines entsprechenden Statusberichts.	Bevor Sie <b>chkdsk /f</b> auf einem geschützten Volume ausführen, stellen Sie sicher, dass keine Konsistenzprüfung für dieses Volume ausgeführt wird. Wenn Sie für ein geschütztes Volume <b>chkdsk /f</b> während einer Konsistenzprüfung ausführen, kann dies zu einer CPU-Auslastung von 100 % führen.  Führen Sie eine Synchronisierung mit Konsistenzprüfung aus, nachdem Sie auf dem geschützten Computer Chkdsk.exe ausgeführt haben.

### Siehe auch

[Anwenden von Betriebssystem-Updates auf Dateiserver und Workstations](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Ausführen von Antivirusprogrammen auf Dateiservern und Workstations](#)

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools auf Exchange-Servern](#)

[Verwenden von Windows-Wartungstools auf SQL-Servern](#)

[Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern](#)

[Verwenden von Windows-Wartungstools auf virtuellen Servern](#)



## **Anwenden von Betriebssystem-Updates auf Dateiserver und Workstations**

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Updates, „Fixes“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können für Computer, die mit DPM geschützt werden, die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Server Update Services. Da für einige Softwareupdates der Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

### **Siehe auch**

[Verwalten von geschützten Dateiservern und Workstations](#)

[Ausführen von Antivirusprogrammen auf Dateiservern und Workstations](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

## **Ausführen von Antivirusprogrammen auf Dateiservern und Workstations**

Um Datenbeschädigung in Replikaten und Schattenkopien zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von DPM nicht erkannt werden. Informationen zur Konfiguration finden Sie im Produkthandbuch des Antivirusprogramms.

Informationen zum Konfigurieren von Firewalls auf Computern bei der Installation von Schutz-Agents finden Sie, in englischer Sprache, unter [Installing Protection Agents](#) (<http://go.microsoft.com/fwlink/?LinkId=95113>).

### **Siehe auch**

[Anwenden von Betriebssystem-Updates auf Dateiserver und Workstations](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

# Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations

Verschiedene Ereignisse oder Geschäftsanforderungen können Änderungen an den geschützten Dateiservern und Workstations oder an den Datenquellen auf dem geschützten Computer erforderlich machen. In diesem Abschnitt finden Sie Informationen darüber, welche Auswirkungen bestimmte Änderungen auf den DPM-Schutz haben können.

## In diesem Abschnitt

[Ändern des Pfads einer Datenquelle](#)

[Verschieben von Dateiservern und Workstations zwischen Domänen](#)

[Umbenennen von Dateiservern oder Workstations](#)

[Ändern der Zeitzone von Dateiservern oder Workstations](#)

## Siehe auch

[Verwalten von Clusterdateiservern](#)

[Leistungsverwaltung](#)

[Allgemeine Wartung von Dateiservern und Workstations](#)

## Ändern des Pfads einer Datenquelle

### Ändern des Pfads einer freigegebenen Datenquelle

Wenn Sie einen freigegebenen Ordner schützen, enthält der Pfad zum freigegebenen Ordner den logischen Pfad auf dem Volume. Wenn Sie den freigegebenen Ordner verschieben, wird er nicht mehr geschützt.

Ist es erforderlich, einen geschützten freigegebenen Ordner zu verschieben, entfernen Sie ihn aus seiner Schutzgruppe und fügen Sie ihn nach dem Verschieben wieder einer Schutzgruppe hinzu.

### Ändern des Pfads einer verschlüsselten Datenquelle

Wenn Sie den Pfad einer von DPM geschützten Datenquelle auf einem Volume verschieben, welches das verschlüsselnde Dateisystem (Encrypting File System, EFS) verwendet, und wenn der neue Pfad mehr als 5120 Zeichen enthält, ist der Schutz der Daten nicht möglich. Sie müssen darauf achten, dass der neue Pfad der geschützten Datenquelle weniger als 5120 Zeichen enthält.

## Siehe auch

[Ändern der Zeitzone von Dateiservern oder Workstations](#)

[Umbenennen von Dateiservern oder Workstations](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Verschieben von Dateiservern und Workstations zwischen Domänen](#)

## Verschieben von Dateiservern und Workstations zwischen Domänen

Folgendes ist für geschützte Computer nicht möglich:

- Domäne eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Domäne eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem Computer zuordnen, wenn der Computer wieder geschützt wird.

Es wird empfohlen, die Domäne eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen, während der Computer seine ursprüngliche Domänenmitgliedschaft beibehält.
- Die Datenquellen auf dem Computer schützen, nachdem er Mitglied einer anderen Domäne geworden ist.

### So ändern Sie die Domänenmitgliedschaft eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie die Domänenmitgliedschaft des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Siehe auch

[Ändern des Pfads einer Datenquelle](#)

[Ändern der Zeitzone von Dateiservern oder Workstations](#)

[Umbenennen von Dateiservern oder Workstations](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

## Umbenennen von Dateiservern oder Workstations

DPM verwendet den Namen des Computers als eindeutigen Bezeichner für Replikate, Wiederherstellungspunkte, DPM-Datenbankeinträge, Berichtsdatenbankeinträge usw.

Folgende Aktionen können nicht durchgeführt werden:

- Namen eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Namen eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem neuen Computernamen zuordnen.

Es wird empfohlen, den Namen eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen (alter Computername).
- Die Datenquellen auf dem Computer schützen (neuer Computername).

### So ändern Sie den Namen eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie den Namen des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Siehe auch

[Ändern des Pfads einer Datenquelle](#)

[Ändern der Zeitzone von Dateiservern oder Workstations](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Verschieben von Dateiservern und Workstations zwischen Domänen](#)

## Ändern der Zeitzone von Dateiservern oder Workstations

DPM erkennt während der Installation des Schutz-Agents automatisch die Zeitzone eines geschützten Computers. Wenn ein geschützter Computer nach dem Konfigurieren des Schutzes in eine andere Zeitzone verschoben wird, führen Sie Folgendes aus:

- Ändern Sie die Computerzeit in der Systemsteuerung mithilfe der Registerkarte **Zeitzone** im Dialogfeld **Eigenschaften von Datum und Uhrzeit**.
- Aktualisieren Sie die Zeitzone in der DPM-Datenbank.

Weitere Informationen zu Zeitzonen und dem Schutz mit DPM finden Sie unter [Koordinieren des zeitzonenübergreifenden Schutzes](#).

### ► So aktualisieren Sie die Zeitzone in der DPM-Datenbank

1. Deinstallieren Sie auf dem geschützten Computer unter **Software** das Programm **Microsoft System Center Data Protection Manager Schutz-Agent**.
2. Wählen Sie in der DPM-Verwaltungskonsole auf dem DPM-Server im Aufgabenbereich **Verwaltung** auf der Registerkarte **Agents** den Computer aus, und klicken Sie dann im Bereich **Aktionen** auf **Informationen aktualisieren**.  
Der Agent-Status ändert sich zu **Fehler**.
3. Klicken Sie im Bereich **Details** auf **Entferne den Dateiservereintrag auf diesem DPM-Computer**.
4. Installieren Sie den Schutz-Agent erneut auf dem Computer.
5. Führen Sie eine Synchronisierung mit Konsistenzprüfung für jedes geschützte Volume auf dem geschützten Computer aus.

## Siehe auch

[Ändern des Pfads einer Datenquelle](#)

[Umbenennen von Dateiservern oder Workstations](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Verschieben von Dateiservern und Workstations zwischen Domänen](#)

# Verwalten von Clusterdateiservern

Bei einem geplanten Failover eines Clusters erhält DPM den Schutz aufrecht. Bei einem ungeplanten Failover gibt DPM einen Alarm aus, dass eine Konsistenzprüfung erforderlich ist.

Bei einem nicht freigegebenen Datenträgercluster ist bei einem geplanten Failover möglicherweise auch eine Konsistenzprüfung erforderlich.

## In diesem Abschnitt

[Ändern der Mitglieder des Dateiserverclusters](#)

[Ändern der Ressourcengruppen auf Clusterdateiservern](#)

## Siehe auch

[Leistungsverwaltung](#)

[Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations](#)

[Allgemeine Wartung von Dateiservern und Workstations](#)

## Ändern der Mitglieder des Dateiserverclusters

Wenn Sie Änderungen an einem von DPM geschützten Servercluster vornehmen, führt DPM Folgendes aus:

- Wenn einem Cluster ein neuer Server hinzugefügt wird, gibt DPM eine Warnung aus, dass ein Schutz-Agent auf dem neuen Clusterknoten installiert werden muss, und der Schutz schlägt fehl.
- Wenn ein Server aus einem Cluster entfernt wird, erkennt DPM, dass ein Knoten im Cluster fehlt, und der Server wird jetzt separat vom Cluster aufgeführt und die darauf enthaltenen Daten werden nicht geschützt.

Angenommen, Sie haben einen Servercluster mit vier Computern: Knoten1, Knoten2, Knoten 3 und Knoten 4. Sie müssen den Computer Knoten4 durch einen neuen Computer, Knoten5, ersetzen.

Sie verwenden die Verwaltungskonsole Ihres Clusterdiensts, um Knoten5 zum Cluster hinzuzufügen und konfigurieren die Ressourcen für das Failover zu Node5.

DPM gibt eine Warnung aus, dass der Schutz des Serverclusters fehlschlägt, bis ein Schutz-Agent auf Node5 installiert wird. Sie installieren den Schutz-Agent auf Node5.

Sie führen ein Failover der Ressourcen von Node4 zu anderen Knoten im Cluster aus. Wenn sich keine Ressourcen mehr auf Node4 befinden, entfernen Sie diesen Knoten aus dem Cluster. DPM erkennt die Failover und setzt den Schutz des Clusters fort.

DPM erkennt, dass Node4 nicht mehr zum Cluster gehört – dieser Computer erscheint jetzt als eigenständiger Knoten. Er ist nicht länger im Netzwerk vorhanden, und Sie können den Eintrag für diesen Server in der DPM-Verwaltungskonsole entfernen.

## **Siehe auch**

[Ändern der Ressourcengruppen auf Clusterdateiservern](#)

[Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations](#)

[Allgemeine Wartung von Dateiservern und Workstations](#)

## **Ändern der Ressourcengruppen auf Clusterdateiservern**

Ein Clusterknoten kann beliebig viele Ressourcengruppen enthalten. Wenn Sie von DPM geschützte Datenquellen in eine Ressourcengruppe verschieben, zwischen Ressourcengruppen verschieben oder aus einer Ressourcengruppe verschieben, können Schutzaufträge fehlschlagen. Führen Sie die folgenden Schritte aus, damit Änderungen an Ressourcengruppenmitgliedschaften erfolgreich durchgeführt werden:

1. Beenden Sie den Schutz der Datenquelle. Die Datenquelle kann als eine einzelne Datenquelle auf einem geschützten Server zu einer Schutzgruppe gehören oder als Datenquelle, die Mitglied einer Ressourcengruppe ist.
2. Starten Sie den Schutz der Datenquelle ihrem neuen Status entsprechend entweder als einzelne Datenquelle auf einem geschützten Server oder als Datenquelle, die Mitglied einer Ressourcengruppe ist. Damit wird ein neues Replikat für die Datenquelle zugewiesen.

Die Namensänderung einer Ressourcengruppe wirkt sich auf den Schutz aller Datenquellen in der Ressourcengruppe aus. Um den Namen einer Ressourcengruppe zu ändern, führen Sie die folgenden Schritte aus:

1. Beenden Sie den Schutz der Ressourcengruppe.
2. Ändern Sie den Namen der Ressourcengruppe.
3. Beginnen Sie mit dem Schutz der Ressourcengruppe unter dem neuen Namen.

## **Siehe auch**

[Ändern der Mitglieder des Dateiserverclusters](#)

[Ausführen von Verwaltungsaufgaben für Dateiserver und Workstations](#)

[Allgemeine Wartung von Dateiservern und Workstations](#)

# Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird

---

Alle Informationen in diesem Abschnitt gelten sowohl für Microsoft Exchange 2003 als auch für Exchange 2007, sofern nicht anders angegeben.

## In diesem Abschnitt

[Allgemeine Wartung von Servern, auf denen Exchange ausgeführt wird](#)

[Ausführen von Exchange Server-Verwaltungsaufgaben](#)

[Verwalten von Exchange-Clustervern](#)

[Wiederherstellen von Exchange-Daten](#)

## Allgemeine Wartung von Servern, auf denen Exchange ausgeführt wird

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- und Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßigen Sicherungen.

Für Server, auf denen Microsoft Exchange Server ausgeführt wird, werden außerdem regelmäßig Exchange-Wartungsaufgaben ausgeführt, zum Beispiel Datenbank-Defragmentierung und Indexbereinigung.

Wenn Sie Wartungsaufgaben für einen geschützten Servers ausführen müssen und für den Zeitraum der Wartungsarbeiten keine Schutzaufträge fortgesetzt werden sollen, können Sie den Schutz-Agent mit dem folgenden Verfahren deaktivieren.

### Hinweis

Wenn Sie einen Schutz-Agent für einen Server deaktivieren, der ein Clusterknoten ist, sollten Sie den Schutz-Agent für jeden Knoten des Clusters deaktivieren.

### So deaktivieren Sie einen Schutz-Agent

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Wählen Sie auf der Registerkarte **Agents** im Anzeigebereich den Namen des Computers mit dem zu deaktivierenden Schutz-Agent aus.
3. Klicken Sie im Bereich **Aktionen** auf **Schutz-Agent deaktivieren**.
4. Klicken Sie im Dialogfeld auf **OK**, um zu bestätigen, dass Sie den Vorgang fortsetzen möchten.



## **In diesem Abschnitt**

[Verwenden von Windows-Wartungstools auf Exchange-Servern](#)

[Ausführen von Exchange-Wartungsaufgaben](#)

[Anwenden von Betriebssystem-Updates auf Exchange-Server](#)

[Ausführen von Antivirusprogrammen auf Exchange-Servern](#)

## **Verwenden von Windows-Wartungstools auf Exchange-Servern**

Das Ausführen der Datenträgerbereinigung, der Datenträgerdefragmentierung oder von Chkdsk.exe sollte keine negativen Auswirkungen auf die Leistung oder den Schutz von Daten haben.

### **Siehe auch**

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

[Verwenden von Windows-Wartungstools auf SQL-Servern](#)

[Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern](#)

[Verwenden von Windows-Wartungstools auf virtuellen Servern](#)

## **Ausführen von Exchange-Wartungsaufgaben**

Die meisten Microsoft Exchange-Wartungsaufgaben sollten keine negativen Auswirkungen auf die Leistung oder auf den Schutz von Daten haben. Es gibt jedoch einige Besonderheiten, die zu berücksichtigen sind, wenn Sie auf Exchange-Servern, die von Data Protection Manager (DPM) geschützt werden, eine Offline-Datenbankdefragmentierung ausführen.

Bei der Offline-Defragmentierung werden die Exchange Server Database Utilities (Eseutil.exe) verwendet. Mit diesem Dienstprogramm können Sie Exchange Server-Datenbanken defragmentieren, reparieren und die Integrität der Datenbanken überprüfen.

Wenn Sie eine Offlinedefragmentierung durchführen müssen, sollten Sie nach Abschluss der Defragmentierung eine Synchronisierung mit Konsistenzprüfung für die geschützten Speichergruppen ausführen.

## **Anwenden von Betriebssystem-Updates auf Exchange-Server**

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Updates, „Fixes“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können für Exchange-Server, die mit Data Protection Manager (DPM) geschützt werden, die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Server Update Services. Da für einige Softwareupdates der Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

## **Ausführen von Antivirusprogrammen auf Exchange-Servern**

Um Datenbeschädigung in Replikaten und Schattenkopien zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von Data Protection Manager (DPM) nicht erkannt werden. Anleitungen zur Konfiguration, damit das Antivirusprogramm infizierte Dateien löscht, finden Sie im Produkthandbuch des Antivirusprogramms.

Anleitungen zum Konfigurieren von Firewalls auf Computern bei der Installation von Schutz-Agents finden Sie, in englischer Sprache, unter [Installing Protection Agents](#) (<http://go.microsoft.com/fwlink/?LinkId=95113>) im Handbuch *Deploying DPM 2007*.

## **Ausführen von Exchange Server-Verwaltungsaufgaben**

In diesem Abschnitt finden Sie Anleitungen und Richtlinien für die Verwaltung eines geschützten Exchange-Servers und zum Vornehmen von Änderungen nach der erstmaligen DPM-Konfiguration.

### **In diesem Abschnitt**

[Aktualisieren von Exchange Server 2003 auf Exchange Server 2007](#)

[Verschieben von Exchange-Servern zwischen Domänen](#)

[Umbenennen von Exchange-Servern](#)

[Hinzufügen von Speichergruppen und Datenbanken](#)

[Aufheben der Bereitstellung von Datenbanken](#)

[Ändern des Pfads von Datenbanken oder Protokolldateien](#)

[Umbenennen von Speichergruppen](#)

[Verschieben von Datenbanken zwischen Speichergruppen](#)

## Aktualisieren von Exchange Server 2003 auf Exchange Server 2007

Es ist nicht möglich, einen Computer, auf dem Microsoft Exchange Server 2003 ausgeführt wird, auf Exchange Server 2007 zu aktualisieren. Anleitungen zum Übergang von Exchange Server 2003 zu Exchange Server 2007 finden Sie unter [Aktualisieren auf Exchange Server 2007](http://go.microsoft.com/fwlink/?LinkId=72602) (<http://go.microsoft.com/fwlink/?LinkId=72602>).

Allgemein ausgedrückt besteht der Übergang darin, Computer mit Exchange Server 2007 bereitzustellen und dann Speichergruppen von den Computern mit Exchange Server 2003 auf die neuen Server zu verschieben.

### ► Schutz von Daten während des Übergangs zu Exchange Server 2007

1. Stellen Sie Exchange Server 2007 bereit.
2. Erstellen Sie leere Speichergruppen und Datenbanken auf den Computern, auf denen Exchange Server 2007 ausgeführt wird.
3. Installieren Sie Schutz-Agents auf den Computern, auf denen Exchange Server 2007 ausgeführt wird.
4. Erstellen Sie neue Schutzgruppen, und fügen Sie die Datenbanken und Speichergruppen hinzu, die Sie in Schritt 2 erstellt haben.
5. Verschieben Sie die Mailboxen auf die Computer, auf denen Exchange Server 2007 ausgeführt wird.
6. Entfernen Sie alle Speichergruppen, die aus ihren vorhandenen Schutzgruppen auf Computer mit Exchange Server 2007 verschoben werden; wählen Sie dabei die Option **Daten beibehalten** aus.

DPM bewahrt die zugeordneten Replikate, Wiederherstellungspunkte und Bänder für den angegebenen Aufbewahrungszeitraum. Sie können Daten von Wiederherstellungspunkten und Bändern auf einem Computer, auf dem Exchange Server 2003 ausgeführt wird, wiederherstellen.

## Verschieben von Exchange-Servern zwischen Domänen

Folgendes ist für geschützte Computer nicht möglich:

- Domäne eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Domäne eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem Computer zuordnen, wenn der Computer wieder geschützt wird.

Es wird empfohlen, die Domäne eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen, während der Computer seine ursprüngliche Domänenmitgliedschaft beibehält.
- Die Datenquellen auf dem Computer schützen, nachdem er Mitglied einer anderen Domäne geworden ist.

### ► So ändern Sie die Domänenmitgliedschaft eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.

Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.

2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie die Domänenmitgliedschaft des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.

Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Umbenennen von Exchange-Servern

DPM verwendet den Namen des Computers als eindeutigen Bezeichner für Replikate, Wiederherstellungspunkte, DPM-Datenbankeinträge, Berichtsdatenbankeinträge usw.

Folgende Aktionen können nicht durchgeführt werden:

- Namen eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Namen eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem neuen Computernamen zuordnen.

Es wird empfohlen, den Namen eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen (alter Computernamen).
- Die Datenquellen auf dem Computer schützen (neuer Computernamen).

### ► So ändern Sie den Namen eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikat und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikat löschen. Für die Endbenutzerwiederherstellung sind die Replikat jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie den Namen des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Hinzufügen von Speichergruppen und Datenbanken

Wenn Sie einem geschützten Microsoft Exchange-Server eine neue Speichergruppe hinzufügen, müssen Sie sie manuell einer Schutzgruppe hinzufügen.

Wenn Sie der Speichergruppe eine neue Datenbank hinzufügen, ist eine vollständige Sicherung erforderlich. Dazu können Sie entweder eine vollständige Schnellsicherung oder eine Konsistenzprüfung ausführen. Inkrementelle Sicherungen schlagen fehl, bis eine vollständige Sicherung abgeschlossen wurde.

## Aufheben der Bereitstellung von Datenbanken

Wenn die Bereitstellung einer Datenbank, die zu einer geschützten Speichergruppe gehört, aufgehoben wird, schlagen nur die Schutzaufträge für diese Datenbank fehl. Protokolle für diese Speichergruppe werden nicht abgeschnitten. Je länger die Bereitstellung der Datenbank jedoch aufgehoben bleibt, umso wahrscheinlicher wird es, dass es im Protokollspeicher auf dem Microsoft Exchange-Server zu einem Überlauf kommt. Dies führt wiederum dazu, dass die Bereitstellung der Speichergruppe auf dem Exchange-Server aufgehoben wird. Wenn die Datenbank nicht benötigt wird, sollten Sie sie löschen.

## Ändern des Pfads von Datenbanken oder Protokolldateien

Wenn geschützte Datenbanken oder Protokolldateien auf ein Volume verschoben werden, das Daten enthält, die von Data Protection Manager (DPM) geschützt werden, wird der Schutz fortgesetzt. Wenn geschützte Datenbanken oder Protokolldateien auf ein Volume verschoben werden, das nicht von DPM geschützt wird, zeigt DPM eine Warnung an, und Schutzaufträge können nicht ausgeführt werden. Um die Warnung aufzuheben, klicken Sie im Detailbereich der Warnung auf den Link **Schutzauftrag ändern**, und führen Sie eine Konsistenzprüfung aus.

Wenn nach der Pfadänderung ein Wiederherstellungspunkt erstellt wird, können Sie die Speichergruppe oder Wiederherstellungspunkte nicht von Wiederherstellungspunkten, die auf dem alten Pfad basieren, wiederherstellen. Sie können jedoch Daten in einen Netzwerkordner wiederherstellen.

Wenn Sie eine Microsoft Exchange 2003-Speichergruppe wiederherstellen, nachdem der Pfad für Datenbanken oder Protokolldateien geändert wurde und der neueste Wiederherstellungspunkt vor der Pfadänderung erstellt wurde, werden die Dateien bei der Wiederherstellung in den alten Pfad kopiert, und es wird versucht, die Datenbanken bereitzustellen. Wenn die Datenbank bereitgestellt werden kann, scheint die Wiederherstellung erfolgreich zu sein.

In diesem Fall können Sie einen der beiden folgenden Schritte ausführen:

- Ändern Sie die Datenbanken zurück zum ursprünglichen Pfad, und stellen Sie die Speichergruppen erneut wieder her.
- Stellen Sie die Datenbanken mit der Option **In Netzwerkordner kopieren** wieder her. Geben Sie den neuen Speicherort der Datenbanken als Ziel des Kopiervorgangs an. Wählen Sie die Option **Bring database to a clean shutdown after copying the files** (Datenbank nach dem Kopieren in einen Clean Shutdown-Status versetzen) aus. Stellen Sie die Datenbank nach der Wiederherstellung bereit.

Wenn Sie eine Exchange 2007-Speichergruppe wiederherstellen, nachdem der Pfad für Datenbanken oder Protokolldateien geändert wurde, und der neueste Wiederherstellungspunkt vor der Pfadänderung erstellt wurde, stellt DPM die Datenbanken am neuen Speicherort wieder her.

Wenn Sie den Pfad von Protokolldateien für eine Speichergruppe ändern, die Festplatte-auf-Band-Sicherungen verwendet, und seit der Pfadänderung nur inkrementelle Sicherungen ausgeführt werden, schlägt das Wiederherstellen einer Speichergruppe mit dem **neuesten** Wiederherstellungspunkt fehl. Um dieses Problem zu vermeiden, gehen Sie wie folgt vor:

- Führen Sie eine vollständige Sicherung aus, und wiederholen Sie dann die Wiederherstellung der Speichergruppe.
- Stellen Sie einzelne Datenbanken wieder her anstatt Speichergruppen.
- Stellen Sie die Speichergruppe als Dateien in einem Netzwerkordner wieder her.

## Umbenennen von Speichergruppen

Es wird empfohlen, den Namen einer geschützten Speichergruppe nicht zu ändern. Wenn Sie den Namen einer Speichergruppe ändern möchten, müssen Sie den Schutz der Speichergruppe beenden, den Namen ändern und die Speichergruppe dann wieder in den Schutz aufnehmen.

Folgende Aktionen können nicht durchgeführt werden:

- Namen einer geschützten Speichergruppe ändern und den Schutz der Daten ohne Störung fortsetzen.
- Namen einer geschützten Speichergruppe ändern und die vorhandenen Replikat und Wiederherstellungspunkte der Speichergruppe zuordnen, wenn diese wieder geschützt wird.

### ► So ändern Sie den Namen einer geschützten Speichergruppe

1. Entfernen Sie die Speichergruppe aus der Schutzgruppe.

Wenn Sie das Replikat und die Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie das Replikat löschen.

2. Ändern Sie den Namen der Speichergruppe.
3. Fügen Sie die Speichergruppe einer Schutzgruppe auf dem Data Protection Manager (DPM)-Server hinzu.

Anleitungen für Aufgaben, an denen Schutzgruppen beteiligt sind, finden Sie in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Verschieben von Datenbanken zwischen Speichergruppen

In der folgenden Tabelle werden die Auswirkungen auf den Schutz von Daten beim Verschieben einer Datenbank zwischen Speichergruppen beschrieben.

### Schutz von Daten, wenn Datenbanken zwischen Speichergruppen verschoben werden

Quelle	Ziel	Ergebnis
Geschützte Speichergruppe	Geschützte Speichergruppe	Data Protection Manager (DPM) setzt den Schutz der Datenbank fort. Führen Sie nach dem Verschieben eine Konsistenzprüfung für beide Speichergruppen durch.
Geschützte Speichergruppe	Nicht geschützte Speichergruppe	DPM beendet den Schutz der Datenbank. Führen Sie nach dem Verschieben eine Konsistenzprüfung für die geschützte Speichergruppe durch.

Quelle	Ziel	Ergebnis
Nicht geschützte Speichergruppe	Geschützte Speichergruppe	DPM beginnt mit dem Schutz der Datenbank, falls die Datenbankdateien sich auf einem von DPM geschützten Volume befinden. Wenn sich die Datenbankdateien nicht auf einem geschützten Volume befinden, führen Sie den Assistenten zum Ändern von Gruppen aus. Führen Sie nach dem Verschieben eine Konsistenzprüfung für die geschützte Speichergruppe durch.

## Verwalten von Exchange-Clusterversern

Bei einem geplanten Failover eines Clusters erhält Data Protection Manager (DPM) den Schutz aufrecht. Bei einem ungeplanten Failover gibt DPM einen Alarm aus, dass eine Konsistenzprüfung erforderlich ist.

Bei einem nicht freigegebenen Datenträgercluster ist bei einem geplanten Failover möglicherweise auch eine Konsistenzprüfung erforderlich.

### In diesem Abschnitt

[Ändern der Mitglieder des Exchange-Serverclusters](#)

[Ändern der Ressourcengruppen auf Exchange-Clusterversern](#)

### Ändern der Mitglieder des Exchange-Serverclusters

Wenn Sie Änderungen an einem von Data Protection Manager (DPM) geschützten Servercluster vornehmen, führt DPM Folgendes aus:

- Wenn einem Cluster ein neuer Server hinzugefügt wird, gibt DPM eine Warnung aus, dass ein Schutz-Agent auf dem neuen Clusterknoten installiert werden muss, und der Schutz schlägt fehl.
- Wenn ein Server aus einem Cluster entfernt wird, erkennt DPM, dass ein Knoten im Cluster fehlt, und der Server wird jetzt separat vom Cluster aufgeführt und die darauf enthaltenen Daten werden nicht geschützt.



Angenommen, Sie haben einen Servercluster mit vier Computern: Knoten1, Knoten2, Knoten 3 und Knoten 4. Sie müssen den Computer Knoten4 durch einen neuen Computer, Knoten5, ersetzen.

Sie verwenden die Verwaltungskonsole Ihres Clusterdiensts, um Knoten5 zum Cluster hinzuzufügen und konfigurieren die Ressourcen für das Failover zu Knoten5.

DPM gibt eine Warnung aus, dass der Schutz des Serverclusters fehlschlägt, bis ein Schutz-Agent auf Knoten5 installiert wird. Sie installieren den Schutz-Agent auf Knoten5.

Sie führen ein Failover der Ressourcen von Knoten4 zu anderen Knoten im Cluster aus. Wenn sich keine Ressourcen mehr auf Knoten4 befinden, entfernen Sie diesen Knoten aus dem Cluster. DPM erkennt die Failover und setzt den Schutz des Clusters fort.

DPM erkennt, dass Knoten4 nicht mehr zum Cluster gehört – dieser Computer erscheint jetzt als eigenständiger Knoten. Er ist nicht länger im Netzwerk vorhanden, und Sie können den Eintrag für diesen Server in der DPM-Verwaltungskonsole entfernen.

## **Ändern der Ressourcengruppen auf Exchange-Clustervern**

Ein Clusterknoten kann beliebig viele Ressourcengruppen enthalten. Wenn Sie geschützte Datenquellen in eine Ressourcengruppe verschieben, zwischen Ressourcengruppen verschieben oder aus einer Ressourcengruppe verschieben, können Schutzaufträge fehlschlagen. Führen Sie die folgenden Schritte aus, damit Änderungen an Ressourcengruppenmitgliedschaften erfolgreich durchgeführt werden:

1. Beenden Sie den Schutz der Datenquelle. Die Datenquelle kann als eine einzelne Datenquelle auf einem geschützten Server zu einer Schutzgruppe gehören oder als Datenquelle, die Mitglied einer Ressourcengruppe ist.
2. Starten Sie den Schutz der Datenquelle ihrem neuen Status entsprechend entweder als einzelne Datenquelle auf einem geschützten Server oder als Datenquelle, die Mitglied einer Ressourcengruppe ist. Damit wird ein neues Replikat für die Datenquelle zugewiesen.

Die Namensänderung einer Ressourcengruppe wirkt sich auf den Schutz aller Datenquellen in der Ressourcengruppe aus. Um den Namen einer Ressourcengruppe zu ändern, führen Sie die folgenden Schritte aus:

1. Beenden Sie den Schutz der Ressourcengruppe.
2. Ändern Sie den Namen der Ressourcengruppe.
3. Beginnen Sie mit dem Schutz der Ressourcengruppe unter dem neuen Namen.

# Wiederherstellen von Exchange-Daten

Wenn Sie eine Microsoft Exchange-Datenbank für die Wiederherstellung auswählen, können Sie unter den folgenden Wiederherstellungsoptionen wählen:

- **Datenbank am ursprünglichen Speicherort wiederherstellen.**

Diese Option ist nur verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt auswählen.

Wenn Sie diese Option auswählen und das Wiederherstellungsziel Dateien enthält, die denselben Namen haben wie die Dateien, die Sie wiederherstellen, werden die aktuellen Datenbankdateien bei der Wiederherstellung überschrieben.

Nur für Exchange 2003: Sie müssen die Zieldatenbank so konfigurieren, dass sie von den wiederhergestellten Daten überschrieben werden kann. Anleitungen hierzu finden Sie unter [„Konfigurieren der Exchange-Datenbanken, sodass sie bei der Wiederherstellung überschrieben werden“](http://go.microsoft.com/fwlink/?LinkId=97929) (<http://go.microsoft.com/fwlink/?LinkId=97929>).

- **Datenbank in einer anderen Datenbank auf einem Exchange 2007-Server wiederherstellen.**

Diese Option ist nur für Exchange 2007 verfügbar.

Diese Option ist nicht verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt auswählen. Sie müssen eine vorhandene Datenbank angeben, in der die ausgewählte Datenbank wiederhergestellt wird. Sie müssen die Zieldatenbank so konfigurieren, dass sie von den wiederhergestellten Daten überschrieben werden kann. Anleitungen hierzu finden Sie unter [„Konfigurieren der Exchange-Datenbanken, sodass sie bei der Wiederherstellung überschrieben werden“](http://go.microsoft.com/fwlink/?LinkId=97929) (<http://go.microsoft.com/fwlink/?LinkId=97929>).

- **In Wiederherstellungsspeichergruppe wiederherstellen.**

Diese Option ist nur für Exchange 2007 verfügbar.

Diese Option ist nicht verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt auswählen.

- **Datenbank in einen Netzwerkordner kopieren.**

Diese Option ist nicht verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt auswählen. Data Protection Manager (DPM) erstellt die folgende Verzeichnisstruktur an dem Ziel, das Sie angeben:

*DPM\_Recovery\_Point\_Zeitstempel\DPM\_Recovered\_At\_Zeitstempel\Servername\Exchange-Anwendung\Datenbankname\Dateien*

Um die Option **Datenbank nach dem Kopieren in einen Clean Shutdown-Status versetzen** zu verwenden, müssen der DPM-Schutz-Agent und das Dienstprogramm Eseutil auf dem Zielsystem installiert sein. Das Dienstprogramm Eseutil kann als Teil einer Exchange Server-Installation oder einer Exchange Server-Installation nur für Administratoren installiert werden.

- **Datenbank auf Band kopieren.**

Diese Option ist nicht verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt auswählen. Mit dieser Option wird das Replikat der Speichergruppe, die die ausgewählte Datenbank enthält, kopiert.

## **In diesem Abschnitt**

[Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank in einer anderen Datenbank](#)

[Kopieren von Exchange-Daten in einen Netzwerkordner](#)

[Kopieren von Exchange-Daten auf Band](#)

[Wiederherstellen von Mailboxen](#)

[Wiederherstellen von Daten auf Clusterservern](#)

## **Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort**

Wenn Sie eine Speichergruppe am ursprünglichen Speicherort wiederherstellen und das Wiederherstellungsziel Dateien enthält, die denselben Namen haben wie die Dateien, die Sie wiederherstellen, werden die aktuellen Datenbankdateien bei der Wiederherstellung überschrieben.

### **So stellen Sie eine Speichergruppe am ursprünglichen Speicherort wieder her**

1. Konfigurieren Sie auf dem Server, auf dem die Speichergruppe wiederhergestellt werden soll, jede Datenbank so, dass das Überschreiben durch die wiederhergestellten Daten zulässig ist. Anleitungen hierzu finden Sie unter „[Konfigurieren der Exchange-Datenbanken, sodass sie bei der Wiederherstellung überschrieben werden](#)“ (<http://go.microsoft.com/fwlink/?LinkId=97929>).
2. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
3. Wählen Sie mithilfe der Durchsuchen-Funktion die Speichergruppe aus, die Sie wiederherstellen möchten.
4. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
5. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten.

6. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet. Die Optionen des Assistenten sind von der verwendeten Exchange-Version abhängig.
7. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
8. Wählen Sie **Recover to original Exchange Server location** (Am ursprünglichen Exchange Server-Speicherort wiederherstellen), und klicken Sie auf **Weiter**.
9. Im Fenster **Specify recovery options** (Wiederherstellungsoptionen festlegen) können Sie die Option **Send an e-mail when this recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden) wählen.  
Wählen Sie diese Option, um eine E-Mail-Adresse oder mehrere Adressen anzugeben, die bei Abschluss der Wiederherstellung benachrichtigt werden. Wenn Sie diese Option wählen, müssen Sie die gewünschte E-Mail-Adresse eingeben, an die eine Benachrichtigung gesendet werden soll. Mehrere E-Mail-Adressen trennen Sie durch ein Komma.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen einer Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank in einer anderen Datenbank](#)

[Kopieren von Exchange-Daten in einen Netzwerkordner](#)

[Kopieren von Exchange-Daten auf Band](#)

[Wiederherstellen von Mailboxen](#)

[Wiederherstellen von Daten auf Clusterservern](#)

## Wiederherstellen einer Datenbank am ursprünglichen Speicherort

Wenn Sie eine Microsoft Exchange Server 2003-Datenbank am ursprünglichen Speicherort wiederherstellen, verwendet Data Protection Manager (DPM) nicht die neuesten Protokolldateien vom geschützten Server. Die Wiederherstellung erfolgt deshalb nicht im letzten gespeicherten Zustand. Um eine Datenbankwiederherstellung ohne Datenverluste auszuführen, stellen Sie die Datenbank am ursprünglichen Speicherort mit einer der folgenden Methoden wieder her:

- Wenn unter der Speichergruppe keine Datenbanken bereitgestellt sind, stellen Sie die Speichergruppe mit dem **neuesten** Wiederherstellungspunkt wieder her.
- Wenn eine Datenbank unter der Speichergruppe bereitgestellt wird, erstellen Sie einen Wiederherstellungspunkt für die Speichergruppe und stellen Sie die Datenbank mit dem **neuesten** Wiederherstellungspunkt wieder her.

Wenn Sie den **neuesten** Wiederherstellungspunkt für eine Exchange Server 2007-Datenbank auswählen, wendet DPM die Protokolldateien vom geschützten Server an und führt ohne weitere Schritte eine verlustfreie Wiederherstellung aus.



#### **Hinweis**

Wenn sich unter Exchange 2007 mehrere Datenbanken in einer Speichergruppe befinden, wird bei der Wiederherstellung die Bereitstellung aller Datenbanken aufgehoben. Es wird empfohlen, unter Exchange 2007 mit einer Datenbank pro Speichergruppe zu arbeiten.

#### **► So stellen Sie eine Datenbank am ursprünglichen Speicherort wieder her**

1. Konfigurieren Sie auf dem Server, auf dem die Datenbank wiederhergestellt werden soll, die Zieldatenbank so, dass das Überschreiben durch die wiederhergestellten Daten zulässig ist. Anleitungen hierzu finden Sie unter [„Konfigurieren der Exchange-Datenbanken, sodass sie bei der Wiederherstellung überschrieben werden“](http://go.microsoft.com/fwlink/?LinkId=97929) (<http://go.microsoft.com/fwlink/?LinkId=97929>).
2. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
3. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Eintrag **Neueste**.  
Sie müssen den aktuellsten Wiederherstellungspunkt auswählen, um die Speichergruppe am ursprünglichen Speicherort wiederherzustellen.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet. Die Optionen des Assistenten sind von der verwendeten Exchange-Version abhängig.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Recover to original Exchange Server location** (Am ursprünglichen Exchange Server-Speicherort wiederherstellen), und klicken Sie auf **Weiter**.
8. Im Fenster **Specify recovery options** (Wiederherstellungsoptionen festlegen) können Sie die Option **Send an e-mail when this recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden) wählen.  
Wählen Sie diese Option, um eine E-Mail-Adresse oder mehrere Adressen anzugeben, die bei Abschluss der Wiederherstellung benachrichtigt werden. Wenn Sie diese Option wählen, müssen Sie auch die gewünschte E-Mail-Adresse eingeben, an die eine Benachrichtigung gesendet werden soll. Mehrere E-Mail-Adressen trennen Sie durch ein Komma.
9. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank in einer anderen Datenbank](#)

[Kopieren von Exchange-Daten in einen Netzwerkordner](#)

[Kopieren von Exchange-Daten auf Band](#)

[Wiederherstellen von Mailboxen](#)

[Wiederherstellen von Daten auf Clusterservern](#)

## Wiederherstellen einer Datenbank in einer anderen Datenbank

Verwenden Sie das folgende Verfahren, um eine Datenbank in einer anderen Datenbank wiederherzustellen.

### ► So stellen Sie einen Datenbank in einer anderen Datenbank wieder her

1. Konfigurieren Sie auf dem Server, auf dem die Datenbank wiederhergestellt werden soll, die Zieldatenbank so, dass das Überschreiben durch die wiederhergestellten Daten zulässig ist. Anleitungen hierzu finden Sie unter „[Konfigurieren der Exchange-Datenbanken, sodass sie bei der Wiederherstellung überschrieben werden](#)“ (<http://go.microsoft.com/fwlink/?LinkId=97929>).
2. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
3. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
4. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
5. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten.
6. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet. Die Optionen des Assistenten sind von der verwendeten Exchange-Version abhängig.
7. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
8. Wählen Sie **Recover to another database on an Exchange Server** (In einer anderen Datenbank auf Exchange Server wiederherstellen), und klicken Sie auf **Weiter**.

9. Im Fenster **Specify recovery options** (Wiederherstellungsoptionen festlegen) können Sie die Option **Send an e-mail when this recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden) wählen.

Wählen Sie diese Option, um eine E-Mail-Adresse oder mehrere Adressen anzugeben, die bei Abschluss der Wiederherstellung benachrichtigt werden. Wenn Sie diese Option wählen, müssen Sie die gewünschte E-Mail-Adresse eingeben, an die eine Benachrichtigung gesendet werden soll. Mehrere E-Mail-Adressen trennen Sie durch ein Komma.

10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank am ursprünglichen Speicherort](#)

[Kopieren von Exchange-Daten in einen Netzwerkordner](#)

[Kopieren von Exchange-Daten auf Band](#)

[Wiederherstellen von Mailboxen](#)

[Wiederherstellen von Daten auf Clusterservern](#)

## Kopieren von Exchange-Daten in einen Netzwerkordner

Wenn Sie eine Speichergruppe in einen Netzwerkordner kopieren, erstellt Data Protection Manager (DPM) die folgenden Verzeichnisstruktur an dem Ziel, das Sie angeben:

**DPM\_Recovery\_Point\_Zeitstempel\DPM\_Recovered\_At\_Zeitstempel\Server name\Exchange-Anwendung\Datenbankname\Dateien**

### Beispiel:

**DPM\_Recovery\_Point\_8-12-2007\_0.1.54AM\DPM\_Recovered\_At\_8-13-2007\_10.49.21AM\Server1.DPM.LAB\J-Volume\Dateien**

Der DPM-Schutz-Agent und das Dienstprogramm Eseutil müssen auf dem Zielsystem installiert sein. Das Dienstprogramm Eseutil kann als Teil einer Microsoft Exchange Server-Installation oder einer Exchange Server-Installation nur für Administratoren installiert werden.

### So kopieren Sie Exchange-Daten in einen Netzwerkordner

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Speichergruppe oder Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Zeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.

4. Wählen Sie im Menü **Zeit** den Wiederherstellungspunkt, den Sie verwenden möchten. Wählen Sie nicht den **neuesten** Wiederherstellungspunkt.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet. Die Optionen des Assistenten sind von der verwendeten Exchange-Version abhängig.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Copy to a network folder** (In einen Netzwerkordner kopieren), und klicken Sie auf **Weiter**.
8. Geben Sie den Zielpfad an, in den die Speichergruppe oder Datenbank kopiert werden soll.
9. Im Fenster **Specify recovery options** (Wiederherstellungsoptionen festlegen) können Sie aus den folgenden Optionen wählen:
  - **Bring the database to a clean shutdown after copying the files** (Datenbank nach dem Kopieren in einen Clean Shutdown-Status versetzen).  
Diese Option ist verfügbar, wenn Sie eine Datenbank kopieren. Damit werden die Datenbankdateien in einen Zustand versetzt, der die Bereitstellung ermöglicht, indem die Protokolle kopiert werden. Wählen Sie diese Option nur dann, wenn das Ziel ein Exchange-basierter Server ist, der über dieselbe Version der Exchange-Anwendung und dieselbe oder eine höhere Version von Eseutil.exe verfügt wie zum Zeitpunkt des Schutzes.
  - **Send an e-mail when this recovery completes (Nach Abschluss der Wiederherstellung E-Mail senden)**.  
Wählen Sie diese Option, um eine E-Mail-Adresse oder mehrere Adressen anzugeben, die bei Abschluss der Wiederherstellung benachrichtigt werden. Wenn Sie diese Option wählen, müssen Sie die gewünschte E-Mail-Adresse eingeben, an die eine Benachrichtigung gesendet werden soll. Mehrere E-Mail-Adressen trennen Sie durch ein Komma.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank in einer anderen Datenbank](#)

[Kopieren von Exchange-Daten auf Band](#)

[Wiederherstellen von Mailboxen](#)

[Wiederherstellen von Daten auf Clusterservern](#)



## Kopieren von Exchange-Daten auf Band

Verwenden Sie das nachstehende Verfahren, um Exchange-Daten auf Band zu kopieren.

### So kopieren Sie Exchange-Daten auf Band

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Speichergruppe oder Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Zeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Zeit** den Wiederherstellungspunkt, den Sie verwenden möchten. Wählen Sie nicht den **neuesten** Wiederherstellungspunkt.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet. Die Optionen des Assistenten sind von der verwendeten Exchange-Version abhängig.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Copy to tape** (Auf Band kopieren), und klicken Sie dann auf **Weiter**.
8. Wählen Sie im Fenster **Specify Library** (Bibliothek festlegen) unter **Primary library** (Primäre Bibliothek) eine Bibliothek, die Sie für die Wiederherstellung verwenden möchten. (**Copy library** (Kopiebibliothek) ist nur verfügbar, wenn der Auftrag nur mit der **Primary library** ausgewählten Bandbibliothek nicht abgeschlossen werden kann.)
  - Wenn die Daten von der Festplatte kopiert werden, kopiert die unter **Primary library** ausgewählte Bibliothek auf Band.
  - Wenn die Daten vom Band kopiert werden und die Bandbibliothek über mehrere Bandlaufwerke verfügt, liest die Bibliothek, die Sie unter **Primary library** (Primärbibliothek) ausgewählt haben, vom Quellband und kopiert die Daten auf ein anderes Band.
  - Wenn die Daten vom Band kopiert werden und die Bandbibliothek nur über ein Bandlaufwerk verfügt, liest die Bibliothek, die Sie unter **Primary library** (Primärbibliothek) ausgewählt haben, vom Quellband, und die Bibliothek, die Sie unter **Copy library** (Kopiebibliothek) ausgewählt haben, kopiert die Daten auf Band.
9. Geben Sie eine Bezeichnung für das Band ein, auf das die Speichergruppe kopiert wird.
10. Geben Sie an, ob die kopierten Daten komprimiert werden sollen.

11. Im Fenster **Specify recovery options** (Wiederherstellungsoptionen festlegen) können Sie die Option **Send an e-mail when this recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden) wählen.

Wählen Sie diese Option, um eine E-Mail-Adresse oder mehrere Adressen anzugeben, die bei Abschluss der Wiederherstellung benachrichtigt werden. Wenn Sie diese Option wählen, müssen Sie die gewünschte E-Mail-Adresse eingeben, an die eine Benachrichtigung gesendet werden soll. Mehrere E-Mail-Adressen trennen Sie durch ein Komma.

12. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Kopieren von Bändern](#)

[Wiederherstellen einer Speichergruppe am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank in einer anderen Datenbank](#)

[Kopieren von Exchange-Daten in einen Netzwerkordner](#)

## Wiederherstellen von Postfächern

Sie können gelöschte E-Mail-Nachrichten mit Microsoft Outlook wiederherstellen. Anleitungen hierzu finden Sie unter „[Wiederherstellen von gelöschten Elementen](#)“ (<http://go.microsoft.com/fwlink/?LinkId=97933>). Um ein gelöschtes Postfach wiederherzustellen, verwenden Sie die Exchange Management Shell oder die Exchange Management Console. Anleitungen hierzu finden Sie unter „[Wiederherstellen von gelöschten Postfächern](#)“ (<http://go.microsoft.com/fwlink/?LinkId=97934>).

Wenn Sie ein Postfach nicht mit der Exchange Management Shell oder der Exchange Management Console wiederherstellen können, zum Beispiel weil der Aufbewahrungszeitraum abgelaufen ist, können Sie das Postfach mit Data Protection Manager (DPM) wiederherstellen.

Um ein Postfach wiederherzustellen, muss DPM die gesamte Datenbank kopieren, da dies die von Exchange unterstützte empfohlene Methode ist, wie im Knowledge Base-Artikel 904845, „[Microsoft support policy for third-party products that modify or extract Exchange database contents](#)“ (<http://go.microsoft.com/fwlink/?LinkId=96542>), beschrieben.

Wenn Sie ein Postfach für die Wiederherstellung auswählen, können Sie nicht den **neuesten** Wiederherstellungspunkt verwenden. Mit der Option **Neuester** werden die Daten vom aktuellsten Wiederherstellungspunkt wiederhergestellt, und dann werden alle übergebenen Transaktionen von den Serverprotokollen angewendet. Diese Funktion steht für einzelne Postfächer nicht zur Verfügung.

Die Details zu den Elementen werden auf der Zusammenfassungsseite des Wiederherstellungsassistenten für Exchange Server-Postfächer nicht angezeigt.

## So stellen Sie ein Exchange 2003-Postfach wieder her

Beim Wiederherstellen eines Postfachs für Microsoft Exchange 2003 werden die Dienstprogramme Eseutil.exe und Exmerge.exe verwendet. Weitere Informationen über das „Tool Exchange Server Database Utilities“ (Eseutil.exe) finden Sie unter [Eseutil](http://go.microsoft.com/fwlink/?LinkId=83451) (<http://go.microsoft.com/fwlink/?LinkId=83451>). Weitere Informationen zu Exmerge.exe finden Sie im Knowledge Base-Artikel 174197, „[Microsoft Exchange Mailbox Merge program \(Exmerge.exe\) information](http://go.microsoft.com/fwlink/?LinkId=83459)“ (<http://go.microsoft.com/fwlink/?LinkId=83459>).

### So stellen Sie eine frühere Version eines aktiven Exchange 2003-Postfachs wieder her

1. Verwenden Sie die Registerkarte **Suchen** und einen Datumsbereich, um das Postfach zu suchen, das Sie wiederherstellen möchten.
2. Wählen Sie einen Wiederherstellungspunkt für die Datenbank, die das wiederherzustellende Postfach enthält.
3. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**. Der Wiederherstellungsassistent wird gestartet.
4. Überprüfen Sie die Auswahl für die Wiederherstellung, und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster **Select Recovery Type** (Wiederherstellungstyp wählen) die Option **Copy to a network folder** (In einen Netzwerkordner kopieren).
6. Geben Sie im Fenster **Specify Destination** (Ziel festlegen) ein Volume auf einem Exchange-Server ein, auf dem eine Wiederherstellungsspeichergruppe aktiviert ist.
7. Wählen Sie im Fenster **Select Recovery Options** (Wiederherstellungsoptionen wählen) das Kontrollkästchen **Bring the database to a clean shut down state after copying the files** (Datenbank nach dem Kopieren der Dateien in einen Clean Shutdown-Status versetzen) aus.
8. Verschieben Sie die Datenbankdatei an den Speicherort der Exchange-Datenbank für die Wiederherstellungsspeichergruppe.
9. Stellen Sie die Datenbank unter der Wiederherstellungsspeichergruppe bereit.
10. Schließen Sie den Wiederherstellungsassistenten ab. DPM stellt die Datenbank wieder her.
11. Extrahieren Sie das Postfach aus der wiederhergestellten Datenbank.
  - Unter Exchange Server 2003 verwenden Sie Microsoft Exchange Server Mailbox Merge (ExMerge).
  - Unter Exchange Server 2003 SP1 können Sie Daten mit dem Exchange 2003 System Manager extrahieren und zusammenführen.

### ► So stellen Sie ein deaktiviertes oder gelöscht Exchange 2003-Postfach wieder her

1. Verwenden Sie die Registerkarte **Suchen** und einen Datumsbereich, um das Postfach zu suchen, das Sie wiederherstellen möchten.
2. Wählen Sie einen Wiederherstellungspunkt für die Datenbank, die das wiederherzustellende Postfach enthält.
3. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**. Der Wiederherstellungsassistent wird gestartet.
4. Überprüfen Sie die Auswahl für die Wiederherstellung, und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster **Select Recovery Type** (Wiederherstellungstyp wählen) die Option **Recover mailbox to an Exchange server database** (Postfach in einer Exchange-Serverdatenbank wiederherstellen).
6. Geben Sie im Fenster **Specify Destination** (Ziel festlegen) die vollständigen Namen des Exchange-Servers ein, einschließlich Domäne, Speichergruppe und Datenbank.  
Die Bereitstellung der Datenbank sollte aufgehoben werden, und Sie müssen sie so konfigurieren, dass sie von den wiederhergestellten Daten überschrieben werden kann. Anleitungen hierzu finden Sie unter „[Konfigurieren der Exchange-Datenbanken, sodass sie bei der Wiederherstellung überschrieben werden](http://go.microsoft.com/fwlink/?LinkId=97929)“ (<http://go.microsoft.com/fwlink/?LinkId=97929>).
7. Schließen Sie den Wiederherstellungsassistenten ab. DPM stellt die Datenbank wieder her.
8. Extrahieren Sie das Postfach aus der wiederhergestellten Datenbank.
  - Unter Exchange Server 2003 verwenden Sie Microsoft Exchange Server Mailbox Merge (ExMerge).
  - Unter Exchange Server 2003 SP1 können Sie Daten mit dem Exchange 2003 System Manager extrahieren und zusammenführen.

#### Siehe auch

[Kopieren von Exchange-Daten in einen Netzwerkordner](#)

[Wiederherstellen von Postfächern](#)

[So stellen Sie ein Exchange 2007-Postfach wieder her](#)

### So stellen Sie ein Exchange 2007-Postfach wieder her

Um ein Microsoft Exchange 2007-Postfach wiederherzustellen, müssen die wiederhergestellten .edb- und .log-Dateien der Wiederherstellungsspeichergruppe in Exchange hinzugefügt werden, und Sie müssen von Exchange unterstützte Tools verwenden, zum Beispiel Exmerge.exe, um eine .pst-Datei zu extrahieren.

Welches Verfahren Sie verwenden, ist davon abhängig, ob ein Postfach vorhanden ist, in dem Sie eine frühere Version wiederherstellen möchten, oder ob das Postfach nicht mehr vorhanden ist und Sie es wiederherstellen möchten.

▶ **So stellen Sie ein Exchange 2007-Postfach für ein vorhandenes Postfach wieder her**

1. Wenn keine Wiederherstellungsspeichergruppe vorhanden ist, erstellen Sie diese, indem Sie das Cmdlet `new-storagegroup` in der Exchange Management Shell verwenden.
2. Erstellen Sie eine Wiederherstellungsdatenbank in der Wiederherstellungsspeichergruppe, indem Sie das Cmdlet `new-mailboxdatabase` in der Exchange Management Shell verwenden.
3. Konfigurieren Sie die Wiederherstellungsdatenbank so, dass sie überschrieben werden kann, indem Sie das Cmdlet `set-mailboxdatabase` in der Exchange Management Shell verwenden.
4. Klicken Sie in der DPM-Verwaltungskonsole auf die Registerkarte **Suchen**, und wählen Sie einen Datumsbereich aus, um das Postfach zu suchen, das Sie wiederherstellen möchten.
5. Wählen Sie einen Wiederherstellungspunkt, der das wiederherzustellende Postfach enthält, und klicken Sie auf **Wiederherstellen**.

DPM stellt die Datenbank mit dem ausgewählten Postfach wieder her.

6. Klicken Sie im Fenster **Review Recovery Selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie im Fenster **Select Recovery Type** (Wiederherstellungstyp wählen) die Option **Recover mailbox to an Exchange server database** (Postfach in einer Exchange-Serverdatenbank wiederherstellen).
8. Geben Sie im Fenster **Specify Destination** (Ziel festlegen) die vollständigen Namen des Exchange-Servers ein, einschließlich Domäne, Name der in Schritt 1 erstellten Wiederherstellungsspeichergruppe und Name der in Schritt 2 erstellten Wiederherstellungsdatenbank.
9. Schließen Sie den Wiederherstellungsassistenten ab. DPM stellt die Datenbank wieder her.
10. Konfigurieren Sie die Zieldatenbank so, dass sie überschrieben werden kann, indem Sie das Cmdlet `set-mailboxdatabase` in der Exchange Management Shell verwenden.
11. Führen Sie die Postfachdaten in der Wiederherstellungsdatenbank mit der Postfach-Produktionsdatenbank zusammen. Verwenden Sie hierzu das Cmdlet `restore-mailbox` in der Exchange Management Shell.

**Beispiel**

Sie brauchen Zugriff auf einige Elemente aus dem Postfach eines ehemaligen Mitarbeiters. Dies ist die Identifikation des Postfachs:

- Exchange Server: `exchangeserver1`
- Speichergruppe: `SG1`
- Datenbank: `DB11`
- Postfach: `John`

Speichergruppe SG1 wird von DPM geschützt. Sie möchten das Postfach von John im Postfach des Managers wiederherstellen, damit er auf die erforderlichen Elemente zugreifen kann. Dies ist die Identifikation des Manager-Postfachs:

- Exchange Server: exchangeserver1
- Speichergruppe: SG2
- Datenbank: DB21
- Postfach: Simon

Um das Postfach John im Postfach Simon wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie eine Wiederherstellungsspeichergruppe (Recovery Storage Group, RSG), indem Sie in der Exchange Management Shell das folgende Cmdlet ausführen:  
**new-storagegroup -Server exchangeserver1 -LogFolderPath C:\RSG\ -Name RSG -SystemFolderPath C:\RSG\ -Recovery**  
Damit wird eine Speichergruppe mit dem Namen RSG auf exchangeserver1 erstellt.
2. Fügen Sie RSG eine Wiederherstellungsdatenbank hinzu, indem Sie in der Exchange Management Shell das folgende Cmdlet ausführen:  
**new-mailboxdatabase -mailboxdatabasetorecover exchangeserver1\SG1\DB11 -storagegroup exchangeserver1\RSG -edbfilepath C:\RSG\DB11.edb**  
Damit wird ein Postfach auf exchangeserver1\RSG\DB11 erstellt. Der .edb-Dateiname muss identisch sein mit dem .edb-Dateinamen für das Postfach, das Sie wiederherstellen.
3. Konfigurieren Sie die Wiederherstellungsdatenbank so, dass Überschreibungen zulässig sind, indem Sie in der Exchange Management Shell das folgende Cmdlet ausführen:  
**set-mailboxdatabase -identity exchangeserver1\RSG\DB11 -AllowFileRestore 1**
4. Öffnen Sie die DPM-Verwaltungskonsolle, und klicken Sie in der Navigationsleiste auf **Wiederherstellung**.
5. Erweitern Sie die Struktur, und wählen Sie SG1 aus.
6. Doppelklicken Sie auf die Datenbank DB11.
7. Wählen Sie **John** aus, und klicken Sie auf **Wiederherstellen**.
8. Klicken Sie im Wiederherstellungsassistenten im Fenster **Review Recovery Selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
9. Wählen Sie im Fenster **Select Recovery Type** (Wiederherstellungstyp wählen) die Option **Recover mailbox to an Exchange server database** (Postfach in einer Exchange-Serverdatenbank wiederherstellen).
10. Geben Sie im Fenster **Specify Destination** (Ziel festlegen) die folgenden Informationen ein:
  - Als Exchange-Server: exchangeserver1
  - Als Speichergruppe: RSG
  - Als Datenbank: DB11
11. Legen Sie die Wiederherstellungsoptionen fest, und klicken Sie auf **Wiederherstellen**.

12. Konfigurieren Sie die Zieldatenbank so, dass Überschreibungen zulässig sind, indem Sie in der Exchange Management Shell das folgende Cmdlet ausführen:

**set-mailboxdatabase -identity exchangeserver1\SG2\DB21 -AllowFileRestore 1**

Die Zieldatenbank ist die Datenbank, die das Postfach enthält, in dem die E-Mails aus Johns Postfach wiederhergestellt werden sollen.

13. Nach Abschluss der Wiederherstellung führen Sie das folgende Cmdlet in der Exchange Management Shell aus:

**Restore-Mailbox -RSGMailbox „John“ -RSGDatabase „RSG\DB11“ -id „Simon“ -TargetFolder „John E-mail“**

Der Manager öffnet sein Postfach und findet einen neuen Ordner mit dem Namen „John E-mail“, der die E-Mail-Elemente aus dem wiederhergestellten Postfach enthält.

**Siehe auch**

[Wiederherstellen von Postfächern](#)

[So stellen Sie ein Exchange 2003-Postfach wieder her](#)

## Wiederherstellen von Daten auf Clusterservern

### Wiederherstellung von eigenständigen und freigegebenen Datenträgerclustern

▶ **So stellen Sie die Speichergruppe oder Datenbank zum aktuellsten Zeitpunkt wieder her**

1. Legen Sie die Eigenschaft **Override by restore** (Überschreiben durch Wiederherstellung) der Exchange-Serverdatenbank auf **True** (Wahr) fest.
2. Stellen Sie auf dem DPM-Server die Speichergruppe oder Datenbank wieder her mit der Option **Restore to original location** (Am ursprünglichen Speicherort wiederherstellen).

▶ **So stellen Sie die Speichergruppe zu einem früheren Zeitpunkt wieder her**

1. Löschen Sie die vorhandenen Protokolldateien und Prüfpunktdateien auf dem Exchange-Server.
2. Legen Sie die Eigenschaft **Override by restore** (Überschreiben durch Wiederherstellung) der Exchange-Serverdatenbank auf **True** (Wahr) fest.
3. Stellen Sie auf dem DPM-Server die Speichergruppe oder Datenbank wieder her mit der Option **Restore to original location** (Am ursprünglichen Speicherort wiederherstellen).

Um eine Speichergruppe oder Datenbank in einem Clean-Shutdown-Zustand in einer Netzwerkfreigabe wiederherzustellen, dürfen Sie nicht den **neuesten** Wiederherstellungspunkt auswählen.

▶ **So stellen Sie die Speichergruppe oder Datenbank in einem Clean-Shutdown-Zustand in einer Netzwerkfreigabe wieder her**

1. Stellen Sie auf dem DPM-Server die Speichergruppe oder Datenbank wieder her mit der Option **Copy to a network folder** (In einen Netzwerkordner kopieren).
2. Geben Sie im Fenster **Specify Destination** (Ziel festlegen) einen Ordner auf einem Server mit Exchange 2007 an.
3. Wählen Sie im Fenster **Specify Recovery Options** (Wiederherstellungsoptionen festlegen) die Option **Bring the database to a clean shutdown state after copying the files** (Datenbank nach dem Kopieren der Dateien in einen Clean Shutdown-Status versetzen) aus.
4. Klicken Sie im Fenster **Zusammenfassung** auf **Wiederherstellen**.

## **Wiederherstellung mit fortlaufender Clusterreplikation (CCR) und fortlaufender lokaler Replikation (LCR)**

Data Protection Manager (DPM) stellt immer den aktiven Knoten wieder her, unabhängig von der Schutztechnologie.

▶ **Wiederherstellung nach Fehlschlag des aktiven Knotens**

1. Legen Sie die Eigenschaft **Override by restore** (Überschreiben durch Wiederherstellung) der Exchange Server-Datenbank auf **True** (Wahr) fest.
2. Stellen Sie auf dem DPM-Server die Speichergruppe oder Datenbank wieder her mit der Option **Restore to original location** (Am ursprünglichen Speicherort wiederherstellen).
3. Führen Sie auf dem Exchange-Server in der Exchange Management Shell den Befehl **get-storagegroupcopystatus** aus, um den Kopierstatus zu überprüfen.  
Nach der Wiederherstellung sollten Sie die passiven Knoten mit dem aktiven Knoten synchronisieren.

Wenn die Datenbank oder die Protokolle auf dem passiven Knoten beschädigt sind, stellen Sie die Daten mit einem der folgenden Verfahren wieder her.

▶ **Wiederherstellung nach Fehlschlag des passiven Knotens**

1. Führen Sie auf dem Exchange-Server in der Exchange Management Shell den Befehl **suspend-storagegroupcopy** für die fehlerhafte Speichergruppe aus.
2. Löschen Sie alle .logs-, .chk- und .edb-Dateien vom Kopierspeicherort (passiver Knoten).
3. Kopieren Sie im DPM-Wiederherstellungsassistenten die Datenbankdateien, ohne sie in den Clean Shutdown-Zustand zu versetzen, auf den passiven Knoten.
4. Verschieben Sie die Dateien an geeignete Speicherorte auf dem passiven Knoten.



5. Entfernen Sie die gemeinsamen Protokolldateien (für den aktiven und die passiven Knoten) vom passiven Knoten. Möglicherweise wurde zum Beispiel durch ein Failover ein neuer Protokoll-Stream mit denselben Protokolldateinamen erstellt.
6. Führen Sie auf dem Exchange-Server in der Exchange Management Shell den Befehl **resume-storagegroupcopy** für die fehlerhafte Speichergruppe aus.

▶ **Wiederherstellung nach Fehlschlag des passiven Knotens (wenn beide Kopien beschädigt sind)**

1. Legen Sie die Eigenschaft **Override by restore** (Überschreiben durch Wiederherstellung) der Exchange Server-Datenbank auf **True** (Wahr) fest.
2. Führen Sie mit dem DPM-Wiederherstellungsassistenten eine Wiederherstellung auf den aktiven Knoten aus.
3. Führen Sie auf dem Exchange-Server in der Exchange Management Shell den Befehl **get-storagegroupcopystatus** aus, um den Kopierstatus zu überprüfen.
4. Synchronisieren Sie nach der Wiederherstellung die passiven Knoten mit dem aktiven Knoten.

### **Siehe auch**

[Verwalten von Exchange-Clusterservern](#)

[Wiederherstellen von Exchange-Daten](#)

# Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird

---

Der Inhalt dieses Abschnitts gilt für Microsoft® SQL Server 2000 und SQL Server 2005, sofern nicht anders angegeben.

## In diesem Abschnitt

[Allgemeine Wartung von Servern, auf denen SQL ausgeführt wird](#)

[Ausführen von SQL Server-Verwaltungsaufgaben](#)

[Verwalten von SQL-Clustervern](#)

[Wiederherstellen von SQL Server-Daten](#)

## Allgemeine Wartung von Servern, auf denen SQL ausgeführt wird

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- und Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßigen Sicherungen. Es gibt jedoch einige Besonderheiten, die zu berücksichtigen sind, wenn Sie auf SQL-Servern, die von Data Protection Manager (DPM) geschützt werden, Serververwaltungsaufgaben ausführen.

Wenn Sie Wartungsaufgaben für einen geschützten Servers ausführen müssen und für den Zeitraum der Wartungsarbeiten keine Schutzaufträge fortgesetzt werden sollen, können Sie den Schutz-Agent mit dem folgenden Verfahren deaktivieren.

### Hinweis

Wenn Sie einen Schutz-Agent für einen Server deaktivieren, der ein Clusterknoten ist, sollten Sie den Schutz-Agent für jeden Knoten des Clusters deaktivieren.

### So deaktivieren Sie einen Schutz-Agent

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**.
2. Wählen Sie auf der Registerkarte **Agents** im Anzeigebereich den Namen des Computers mit dem zu deaktivierenden Schutz-Agent aus.
3. Klicken Sie im Bereich **Aktionen** auf **Schutz-Agent deaktivieren**.
4. Klicken Sie im Dialogfeld auf **OK**, um zu bestätigen, dass Sie den Vorgang fortsetzen möchten.

## **In diesem Abschnitt**

[Verwenden von Windows-Wartungstools auf SQL-Servern](#)

[Ausführen von SQL-Wartungsaufgaben](#)

[Anwenden von Betriebssystem-Updates auf SQL-Server](#)

[Ausführen von Antivirusprogrammen auf SQL-Servern](#)

## **Verwenden von Windows-Wartungstools auf SQL-Servern**

Das Ausführen der Datenträgerbereinigung, der Datenträgerdefragmentierung oder von Chkdsk.exe sollte keine negativen Auswirkungen auf die Leistung oder den Schutz von Daten haben.

Auf einem Computer, auf dem SQL Server ausgeführt wird und der von DPM geschützt wird, sollten Sie keine anderen Sicherungsanwendungen verwenden.

### **Siehe auch**

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

[Verwenden von Windows-Wartungstools auf Exchange-Servern](#)

[Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern](#)

[Verwenden von Windows-Wartungstools auf virtuellen Servern](#)

## **Ausführen von SQL-Wartungsaufgaben**

Stimmen Sie sich mit dem SQL Server-Administrator ab, um sicherzustellen, dass die folgenden Aufgaben nicht für denselben Zeitraum wie die von DPM ausgeführten vollständigen Schnellsicherungen geplant sind:

- Überprüfen der Datenbankintegrität
- Verlaufs-Cleanup
- Wartungs-Cleanup
- Neuerstellen des Index
- Neuorganisieren des Index
- Verkleinern der Datenbank
- Aktualisieren der Statistik

Es hat sich bewährt, für SQL Server eine wöchentliche Konsistenzprüfung der Datenbank (DBCC) auszuführen. Dies sollten Sie auch für Datenbanken, die mit DPM geschützt werden, fortsetzen, um zu verhindern, dass Sie eine Datenbank mit Fehlern sichern.

## **Anwenden von Betriebssystem-Updates auf SQL-Server**

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Updates, „Fixes“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können für Computer, auf denen SQL Server ausgeführt wird und die von DPM geschützt werden, die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Server Update Services. Da für einige Softwareupdates der Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

## **Ausführen von Antivirusprogrammen auf SQL-Servern**

Um Datenbeschädigung in Replikaten und Wiederherstellungspunkten zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von DPM nicht erkannt werden. Anleitungen zur Konfiguration, damit das Antivirusprogramm infizierte Dateien löscht, finden Sie im Produkthandbuch des Antivirusprogramms.

## **Ausführen von SQL Server-Verwaltungsaufgaben**

In diesem Abschnitt finden Sie Anleitungen und Richtlinien für die Verwaltung eines geschützten SQL-Servers und zum Vornehmen von Änderungen nach der erstmaligen Konfiguration von Data Protection Manager.

### **In diesem Abschnitt**

[Aktualisieren von SQL Server 2000 auf SQL Server 2005](#)

[Verschieben von SQL-Servern zwischen Domänen](#)

[Umbenennen von Computern, auf denen SQL Server ausgeführt wird](#)

[Ändern des Wiederherstellungsmodells einer Datenbank](#)

[Ersetzen von Datenträgern auf einem SQL-Server](#)

[Hinzufügen von Datenbanken zu einem SQL-Server](#)

[Ändern des Pfads von SQL Server-Datenbanken](#)

[Umbenennen von SQL Server-Datenbanken](#)

## Aktualisieren von SQL Server 2000 auf SQL Server 2005

Wenn Sie einen geschützten Server, auf dem SQL Server 2000 aufgeführt wird, auf SQL Server 2005 aktualisieren, müssen Sie die Datenbanken nach der Aktualisierung erneut in den Schutz einbinden, indem Sie folgendermaßen vorgehen:

1. Beenden Sie den Schutz der Datenbanken, und wählen Sie die Option zum Beibehalten der Daten.
2. Starten Sie den SQL Writer Service auf dem aktualisierten Server.
3. Fügen Sie die Datenbanken auf dem aktualisierten Server einer neuen Schutzgruppe hinzu.

Sie können die beibehaltenen Replikate verwenden, um Daten aus der Zeit vor der Aktualisierung wiederherzustellen. Daten, die von SQL Server 2000 erstellt wurden, müssen auf einem Computer wiederhergestellt werden, auf dem SQL Server 2000 ausgeführt wird.

Sie können die beibehaltenen Replikate auch verwenden, um das erste Replikat für jede Datenbank in der Schutzgruppe manuell zu erstellen.



### Hinweis

Nachdem Sie den Schutz neu konfiguriert haben, zeigt die DPM-Verwaltungskonsolle die geschützte Datenbank als zwei separate Knoten an. Der Schutzstatus im Aufgabenbereich „Schutz“ wird als **Inaktives Replikat** für einen der Datenbankknoten angezeigt, und im Aufgabenbereich „Wiederherstellung“ werden zwei Datenbankknoten mit demselben Namen angezeigt.

## Verschieben von SQL-Servern zwischen Domänen

Folgendes ist für geschützte Computer nicht möglich:

- Domäne eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Domäne eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem Computer zuordnen, wenn der Computer wieder geschützt wird.

Es wird empfohlen, die Domäne eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen, während der Computer seine ursprüngliche Domänenmitgliedschaft beibehält.
- Die Datenquellen auf dem Computer schützen, nachdem er Mitglied einer anderen Domäne geworden ist.

### ► So ändern Sie die Domänenmitgliedschaft eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie die Domänenmitgliedschaft des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Umbenennen von Computern, auf denen SQL Server ausgeführt wird

DPM verwendet den Namen des Computers als eindeutigen Bezeichner für Replikate, Wiederherstellungspunkte, DPM-Datenbankeinträge, Berichtsdatenbankeinträge usw.

Folgende Aktionen können nicht durchgeführt werden:

- Namen eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Namen eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem neuen Computernamen zuordnen.

Es wird empfohlen, den Namen eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen (alter Computernamen).
- Die Datenquellen auf dem Computer schützen (neuer Computernamen).

### ► So ändern Sie den Namen eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie den Namen des Computers.

4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (http://go.microsoft.com/fwlink/?LinkId=102087).

## Ändern des Wiederherstellungsmodells einer Datenbank

SQL Server-Datenbanken verwenden eines von drei Wiederherstellungsmodellen: einfach, vollständig oder massenprotokolliert. Standardmäßig werden neue Datenbanken normalerweise mit dem vollständigen Wiederherstellungsmodell erstellt. In der folgenden Tabelle ist aufgeführt, wie die einzelnen Modelle Protokollsicherungen verwenden.

### Wiederherstellungsmodelle für SQL Server-Datenbanken

Wiederherstellungsmodell	Verwendung von Protokollsicherungen
Einfach	Es werden keine Protokollsicherungen verwendet.
Vollständig	SQL Server pflegt die Transaktionsprotokolle für die Datenbanken, sodass Protokollsicherungen erfolgen können. Die Protokolle müssen ausdrücklich abgeschnitten werden; andernfalls nehmen sie in der Größe ständig zu.
Massenprotokolliert	Dieses Modell ähnelt dem vollständigen Modell, allerdings werden bestimmte Transaktionstypen nicht protokolliert.

Wenn einer Schutzgruppe eine Datenbank hinzugefügt wird, erkennt DPM das Wiederherstellungsmodell, für dessen Verwendung die Datenbank konfiguriert ist. DPM lässt keine Protokollsicherungen (inkrementellen Sicherungen) zu für Datenbanken, die mit dem einfachen Wiederherstellungsmodell konfiguriert sind. Protokollsicherungen sind nur für Datenbanken zulässig, die mit den vollständigen und massenprotokollierten Wiederherstellungsmodellen konfiguriert sind.

Wenn das Wiederherstellungsmodell einer geschützten Datenbank von „einfach“ zu „vollständig“ oder „massenprotokolliert“ geändert wird, wird der DPM-Schutz wie konfiguriert fortgeführt. Wenn das Wiederherstellungsmodell einer geschützten Datenbank von „vollständig“ oder „massenprotokolliert“ zu „einfach“ geändert wird, werden vollständige Schnellsicherungen weiterhin erfolgreich ausgeführt, inkrementelle Sicherungen werden jedoch fehlschlagen.

### ► So ändern Sie das Wiederherstellungsmodell einer geschützten Datenbank zum einfachen Wiederherstellungsmodell

1. Beenden Sie den Schutz der Datenbank, und wählen Sie die Option zum Beibehalten der Replikat.
2. Ändern Sie das Wiederherstellungsmodell in der SQL Server-Datenbank.
3. Fügen Sie die Datenbank einer Schutzgruppe hinzu.

Sie sollten den Schutz einer Datenbank auch beenden, bevor Sie den Protokollversand für die Datenbank konfigurieren oder die Datenbank zu „Schreibgeschützt“ ändern. Nachdem Sie die Änderungen an der Datenbank vorgenommen haben, können Sie den Schutz für die Datenbank neu konfigurieren.

Wenn Sie SQL Server-Datenbanken schützen, die für das vollständige oder massenprotokollierte Wiederherstellungsmodell konfiguriert sind, erstellt DPM einen Ordner auf dem geschützten SQL-Server. Der Ordner wird am selben Speicherort erstellt wie die erste Protokolldatei (\*.ldf) jeder geschützten Datenbank.

Dieser Ordner wird während der SQL Server-Protokollsicherung und der SQL Server-Protokollwiederherstellung durch DPM als temporärer Speicher für Protokolle verwendet. Wenn DPM erkennt, dass der Ordner fehlt, erstellt DPM den Ordner neu.

## Ersetzen von Datenträgern auf einem SQL-Server

Sie können einen Datenträger auf einem SQL-Server ersetzen, um die Kapazität zu erhöhen oder um einen fehlerhaften Datenträger auszutauschen. Wenn Sie einen Datenträger ersetzen, der von DPM geschützte SQL Server-Daten enthält, sollten Sie dem neuen Datenträger denselben Laufwerksbuchstaben zuweisen. Sie können die geschützten Daten dann vom DPM-Server auf dem neuen Datenträger wiederherstellen.

## Hinzufügen von Datenbanken zu einem SQL-Server

Neue Datenbanken auf einem geschützten Computer, auf dem SQL Server ausgeführt wird, werden nicht automatisch einer vorhandenen Schutzgruppe hinzugefügt. Wenn eine neue Datenbank erstellt wird, sollten Sie die Datenbank manuell einer vorhandenen oder neuen Schutzgruppe zuweisen, um sicherzustellen, dass die Daten geschützt sind.

## Ändern des Pfads von SQL Server-Datenbanken

Wenn der Pfad einer geschützten Datenbank geändert wird, schlagen Sicherungsaufträge fehl. Um dieses Problem zu vermeiden, entfernen Sie die Datenbank aus dem Schutz und führen Sie sie dann wieder der Schutzgruppe hinzu. Diese Änderung an der Schutzgruppe macht eine Konsistenzprüfung erforderlich. Nach dem erfolgreichen Abschluss der Konsistenzprüfung werden normale Schutzaufträge fortgesetzt.



## Umbenennen von SQL Server-Datenbanken

Wenn Sie eine Datenbank umbenennen, die von DPM geschützt wird, müssen Sie die Datenbank unter ihrem neuen Namen einer vorhandenen oder neuen Schutzgruppe hinzufügen und die Datenbank dann unter ihrem alten Namen aus der Schutzgruppe entfernen. Die Datenbank wird als eine neue Datenquelle geschützt.

## Verwalten von SQL-Clustervern

Bei einem geplanten Failover eines Clusters erhält DPM den Schutz aufrecht. Bei einem ungeplanten Failover gibt DPM einen Alarm aus, dass eine Konsistenzprüfung erforderlich ist.

Bei einem nicht freigegebenen Datenträgercluster ist bei einem geplanten Failover möglicherweise auch eine Konsistenzprüfung erforderlich.

Die Masterdatenbank für SQL-Clustervern kann nicht gesichert und wiederhergestellt werden.

### In diesem Abschnitt

[Ändern der Mitglieder des SQL-Serverclusters](#)

[Ändern der Ressourcengruppen auf SQL-Clustervern](#)

## Ändern der Mitglieder des SQL-Serverclusters

Wenn Sie Änderungen an einem von DPM geschützten Servercluster vornehmen, führt DPM Folgendes aus:

- Wenn einem Cluster ein neuer Server hinzugefügt wird, gibt DPM eine Warnung aus, dass ein Schutz-Agent auf dem neuen Clusterknoten installiert werden muss, und der Schutz schlägt fehl.
- Wenn ein Server aus einem Cluster entfernt wird, erkennt DPM, dass ein Knoten im Cluster fehlt, und der Server wird jetzt separat vom Cluster aufgeführt und die darauf enthaltenen Daten werden nicht geschützt.

Angenommen, Sie haben einen Servercluster mit vier Computern: Knoten1, Knoten2, Knoten 3 und Knoten 4. Sie müssen den Computer Knoten4 durch einen neuen Computer, Knoten5, ersetzen.

Sie verwenden die Verwaltungskonsole Ihres Clusterdiensts, um Knoten5 zum Cluster hinzuzufügen und konfigurieren die Ressourcen für das Failover zu Knoten5.

DPM gibt eine Warnung aus, dass der Schutz des Serverclusters fehlschlägt, bis ein Schutz-Agent auf Knoten5 installiert wird. Sie installieren den Schutz-Agent auf Knoten5.

Sie führen ein Failover der Ressourcen von Knoten4 zu anderen Knoten im Cluster aus. Wenn sich keine Ressourcen mehr auf Knoten4 befinden, entfernen Sie diesen Knoten aus dem Cluster. DPM erkennt die Failover und setzt den Schutz des Clusters fort.

DPM erkennt, dass Knoten nicht mehr zum Cluster gehört – dieser Computer erscheint jetzt als eigenständiger Knoten. Er ist nicht länger im Netzwerk vorhanden, und Sie können den Eintrag für diesen Server in der DPM-Verwaltungskonsole entfernen.

## Ändern der Ressourcengruppen auf SQL-Clustervern

Ein Clusterknoten kann beliebig viele Ressourcengruppen enthalten. Wenn Sie geschützte Datenquellen in eine Ressourcengruppe verschieben, zwischen Ressourcengruppen verschieben oder aus einer Ressourcengruppe verschieben, können Schutzaufträge fehlschlagen. Führen Sie die folgenden Schritte aus, damit Änderungen an Ressourcengruppenmitgliedschaften erfolgreich durchgeführt werden:

1. Beenden Sie den Schutz der Datenquelle. Die Datenquelle kann als eine einzelne Datenquelle auf einem geschützten Server zu einer Schutzgruppe gehören oder als Datenquelle, die Mitglied einer Ressourcengruppe ist.
2. Starten Sie den Schutz der Datenquelle ihrem neuen Status entsprechend entweder als einzelne Datenquelle auf einem geschützten Server oder als Datenquelle, die Mitglied einer Ressourcengruppe ist. Damit wird ein neues Replikat für die Datenquelle zugewiesen.

Die Namensänderung einer Ressourcengruppe wirkt sich auf den Schutz aller Datenquellen in der Ressourcengruppe aus. Um den Namen einer Ressourcengruppe zu ändern, führen Sie die folgenden Schritte aus:

1. Beenden Sie den Schutz der Ressourcengruppe.
2. Ändern Sie den Namen der Ressourcengruppe.
3. Beginnen Sie mit dem Schutz der Ressourcengruppe unter dem neuen Namen.

## Wiederherstellen von SQL Server-Daten

Wenn Sie SQL Server-Daten wiederherstellen, können Sie zwischen folgenden Optionen wählen:

- Datenbank am ursprünglichen Speicherort wiederherstellen
- Datenbank unter einem neuen Namen am ursprünglichen Speicherort oder auf einer anderen Instanz von SQL Server wiederherstellen
- Datenbank auf einer anderen Instanz von SQL Server wiederherstellen
- Datenbank in einen Netzwerkordner kopieren
- Datenbank auf Band kopieren

Wenn Sie eine SQL Server 2000-Datenbank auf einer anderen Instanz von SQL Server wiederherstellen, muss der Wiederherstellungspfad auf dem neuen Server identisch sein mit dem Pfad der Datenbank wie zum Zeitpunkt des Schutzes auf dem Quellserver. Beispiel: DB1 unter D:\beispiel auf server1 kann nur unter D:\beispiel auf server2 wiederhergestellt werden. Wenn Sie in einen vollständig neuen Pfad wiederherstellen möchten, können Sie nur vollständige Schnellsicherungen (normalerweise eine Kopie pro Tag) wiederherstellen.

Wenn Sie eine SQL Server 2005-Datenbank auf einer anderen Instanz von SQL Server wiederherstellen, können Sie die Datenbank in jedem beliebigen Pfad auf dem neuen Server wiederherstellen. Sie können alle 15 Minuten eine Sicherung ausführen und jeden Zeitpunkt auf dem Ziel-SQL-Server wiederherstellen.

Sowohl in SQL Server 2000 und SQL Server 2005 können Sie die Datenbank umbenennen und auf der ursprünglichen SQL-Instanz wiederherstellen.

Es ist nicht möglich, eine Datenbank von einer Instanz von SQL Server auf einem Computer mit Windows Server 2008 auf einer Instanz von SQL Server auf einem Computer mit Windows Server 2003 wiederherzustellen.

Sie können eine Systemdatenbank nicht auf einer anderen Instanz von SQL Server wiederherstellen.

## In diesem Abschnitt

[Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen und Umbenennen von SQL-Datenbanken](#)

[Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server](#)

[Kopieren von SQL-Datenbanken in einen Netzwerkordner](#)

[Kopieren von SQL-Datenbanken auf Band](#)

[Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen](#)

## Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort

► So stellen Sie eine Datenbank am ursprünglichen Speicherort wieder her

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Recover to original SQL Server location** (Am ursprünglichen SQL Server-Speicherort wiederherstellen), und klicken Sie auf **Weiter**.
8. Wenn Sie einen anderen Wiederherstellungspunkt als den **neuesten** ausgewählt haben, wählen Sie im Fenster **Specify Database State** (Datenbankstatus festlegen) die Option **Leave database operational** (Datenbank betriebsfähig lassen).

9. Legen Sie Wiederherstellungsoptionen für die Netzwerk-Bandbreitenbeschränkung, SAN-basierte Wiederherstellung und E-Mail-Benachrichtigungen fest, und klicken Sie dann auf **Weiter**.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen und Umbenennen von SQL-Datenbanken](#)

[Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server](#)

[Kopieren von SQL-Datenbanken in einen Netzwerkordner](#)

[Kopieren von SQL-Datenbanken auf Band](#)

[Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen](#)

## Wiederherstellen und Umbenennen von SQL-Datenbanken

Um eine Datenbank wiederherzustellen und ihren Namen zu ändern, verwenden Sie die Option **Recover to any SQL instance** (Auf beliebiger SQL-Instanz wiederherstellen). Diese Option ist nicht verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt für die Wiederherstellung der Datenbank auswählen.

### So können Sie eine Datenbank wiederherstellen und umbenennen

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten. Wählen Sie nicht den **neuesten** Wiederherstellungspunkt.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Recover to any SQL instance** (Auf beliebiger SQL-Instanz wiederherstellen), und klicken Sie auf **Weiter**.
8. Geben Sie im Fenster **Specify recovery destination** (Wiederherstellungsziel festlegen) den Pfad ein, unter dem die Datenbank wiederhergestellt werden soll, und geben Sie einen neuen Namen für die wiederhergestellte Datenbank ein.

9. Legen Sie Wiederherstellungsoptionen für die Netzwerk-Bandbreitenbeschränkung, SAN-basierte Wiederherstellung und E-Mail-Benachrichtigungen fest, und klicken Sie dann auf **Weiter**.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server](#)

[Kopieren von SQL-Datenbanken in einen Netzwerkordner](#)

[Kopieren von SQL-Datenbanken auf Band](#)

[Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen](#)

## Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server

Um eine Datenbank auf einer anderen Instanz von SQL Server wiederherzustellen, verwenden Sie die Option **Recover to any SQL instance** (Auf beliebiger SQL-Instanz wiederherstellen). Diese Option ist nicht verfügbar, wenn Sie den **neuesten** Wiederherstellungspunkt für die Wiederherstellung der Datenbank auswählen.

### ► So stellen Sie eine Datenbank auf einer anderen Instanz von SQL Server wieder her

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten. Wählen Sie nicht den **neuesten** Wiederherstellungspunkt.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Recover to any SQL instance** (Auf beliebiger SQL-Instanz wiederherstellen), und klicken Sie auf **Weiter**.

8. Welche Aktionen Sie im Fenster **Specify recovery destination** (Wiederherstellungsziel festlegen) ausführen, ist von der Version der SQL Server-Datenbank abhängig:
  - Wenn Sie eine von SQL Server 2000 erstellte Datenbank wiederherstellen, geben Sie die alternative Instanz von SQL Server an, auf der die Datenbank wiederhergestellt werden soll. Die Datenbank muss denselben vollständigen Pfad verwenden, der am ursprünglichen Speicherort verwendet wurde.
  - Wenn Sie eine von SQL Server 2005 erstellte Datenbank wiederherstellen, geben Sie die alternative Instanz von SQL Server an, auf der die Datenbank wiederhergestellt werden soll. Sie können auch einen Pfad für die Datenbank angeben, der sich von dem am ursprünglichen Speicherort verwendeten Pfad unterscheidet.
9. Legen Sie Wiederherstellungsoptionen für die Netzwerk-Bandbreitenbeschränkung, SAN-basierte Wiederherstellung und E-Mail-Benachrichtigungen fest, und klicken Sie auf **Weiter**.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen und Umbenennen von SQL-Datenbanken](#)

[Kopieren von SQL-Datenbanken in einen Netzwerkordner](#)

[Kopieren von SQL-Datenbanken auf Band](#)

[Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen](#)

## Kopieren von SQL-Datenbanken in einen Netzwerkordner

Sie können eine SQL Server-Datenbank nur von einem Wiederherstellungspunkt kopieren, der aus einer vollständigen Schnellsicherung erstellt wurde.

### So kopieren Sie eine Datenbank in einen Netzwerkordner

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten.

5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Copy to a network folder** (In einen Netzwerkordner kopieren), und klicken Sie auf **Weiter**.  
Wenn der ausgewählte Wiederherstellungspunkt nicht aus einer vollständigen Schnellsicherung erstellt wurde, werden andere Wiederherstellungspunkte zur Auswahl angezeigt.
8. Geben Sie den Zielpfad an, in den die Datenbank kopiert werden soll.
9. Im Fenster **Specify recovery options** (Wiederherstellungsoptionen festlegen) können Sie eine oder beide der folgenden Optionen wählen:
  - **Restore security (Sicherheit wiederherstellen)**  
Legen Sie fest, ob die Sicherheitseinstellungen der wiederherzustellenden Daten oder die Sicherheitseinstellungen des Ziels verwendet werden sollen.
  - **Send an e-mail when this recovery completes (Nach Abschluss der Wiederherstellung E-Mail senden).**  
Wählen Sie diese Option, um eine E-Mail-Adresse oder mehrere Adressen anzugeben, die bei Abschluss der Wiederherstellung benachrichtigt werden. Wenn Sie diese Option wählen, müssen Sie die gewünschte E-Mail-Adresse eingeben, an die eine Benachrichtigung gesendet werden soll. Mehrere E-Mail-Adressen trennen Sie durch ein Komma.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## **Siehe auch**

[Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen und Umbenennen von SQL-Datenbanken](#)

[Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server](#)

[Kopieren von SQL-Datenbanken auf Band](#)

[Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen](#)

## Kopieren von SQL-Datenbanken auf Band

Sie können eine SQL Server-Datenbank nur von einem Wiederherstellungspunkt auf Band kopieren, der aus einer vollständigen Schnellsicherung erstellt wurde.

### ► So kopieren Sie eine Datenbank auf Band

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten.  
Sie müssen den aktuellsten Wiederherstellungspunkt auswählen, um die Speichergruppe am ursprünglichen Speicherort wiederherzustellen.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Copy to tape** (Auf Band kopieren), und klicken Sie dann auf **Weiter**.  
Wenn der ausgewählte Wiederherstellungspunkt nicht aus einer vollständigen Schnellsicherung erstellt wurde, werden andere Wiederherstellungspunkte zur Auswahl angezeigt.
8. Wählen Sie im Fenster **Specify Library** (Bibliothek festlegen) unter **Primary library** (Primäre Bibliothek) eine Bibliothek, die Sie für die Wiederherstellung verwenden möchten. (**Copy library** (Kopiebibliothek) ist nur verfügbar, wenn der Auftrag nur mit der **Primary library** ausgewählten Bandbibliothek nicht abgeschlossen werden kann.)
  - Wenn die Daten von der Festplatte kopiert werden, kopiert die unter **Primary library** ausgewählte Bibliothek auf Band.
  - Wenn die Daten vom Band kopiert werden und die Bandbibliothek über mehrere Bandlaufwerke verfügt, liest die Bibliothek, die Sie unter **Primary library** (Primärbibliothek) ausgewählt haben, vom Quellband und kopiert die Daten auf ein anderes Band.
  - Wenn die Daten vom Band kopiert werden und die Bandbibliothek nur über ein Bandlaufwerk verfügt, liest die Bibliothek, die Sie unter **Primary library** (Primärbibliothek) ausgewählt haben, vom Quellband, und die Bibliothek, die Sie unter **Copy library** (Kopiebibliothek) ausgewählt haben, kopiert die Daten auf Band.



9. Geben Sie eine Bezeichnung für das Band ein, auf das die Speichergruppe kopiert wird.
10. Geben Sie an, ob die kopierten Daten komprimiert oder verschlüsselt werden sollen.
11. Im Fenster **Set notification** (Benachrichtigung festlegen) können Sie die Option **Send an e-mail when this recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden) wählen.
12. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Kopieren von Bändern](#)

[Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen und Umbenennen von SQL-Datenbanken](#)

[Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server](#)

[Kopieren von SQL-Datenbanken in einen Netzwerkordner](#)

[Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen](#)

## Wiederherstellen von SQL-Datenbanken und Zulassen von zusätzlichen Protokollsicherungen

Der DPM-Wiederherstellungsprozess verwendet eine SQL Server-Funktion, um eine Datenbank so wiederherzustellen, dass für alle nicht übermittelten Transaktionen ein Rollback ausgeführt wird. Der Wiederherstellungsprozess öffnet das Transaktionsprotokoll, um nicht übermittelte Transaktionen zu identifizieren. Nicht übermittelte Transaktionen werden rückgängig gemacht, indem ein Rollback ausgeführt wird, sofern sie nicht mit Sperren versehen sind, die verhindern, dass andere Transaktionen inkonsistente Daten anzuzeigen. Dieser Schritt wird als Rückgängig-Phase oder *Rollback*-Phase bezeichnet.

Unter bestimmten Umständen fordert der SQL Server-Administrator möglicherweise die Wiederherstellung der Datenbank in einem Modus an, sodass Protokollsicherungen selektiv rückgängig gemacht werden. Mit DPM können Sie eine Datenbank wiederherstellen und in einem Wiederherstellungsstatus belassen, in dem zusätzliche Protokollsicherungen auf die Datenbank angewendet werden können.

► **So stellen Sie eine Datenbank ohne Transaktions-Rollback wieder her**

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Datenbank aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten. Sie können alle Wiederherstellungspunkte mit Ausnahme des **neuesten** auswählen.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Recover to original SQL Server location** (Am ursprünglichen SQL Server-Speicherort wiederherstellen) oder **Recover to any SQL instance** (Auf beliebiger SQL-Instanz wiederherstellen) und klicken Sie auf **Weiter**.
8. Wenn Sie **Recover to any SQL instance** (Auf beliebiger SQL-Instanz wiederherstellen) wählen, geben Sie im Fenster **Specify recovery destination** (Wiederherstellungsziel festlegen) an, auf welcher Instanz von SQL Server die Datenbank wiederhergestellt werden soll.
9. Wählen Sie im Fenster **Specify Database State** (Datenbankstatus festlegen) die Option **Leave database non-operational but able to restore additional transaction logs** (Datenbank nicht betriebsfähig aber zusätzliche Transaktionsprotokolle können wiederhergestellt werden).
10. Wählen Sie **Copy SQL transaction logs between the selected recovery point and latest available recovery point** (SQL-Transaktionsprotokolle zwischen dem ausgewählten Wiederherstellungspunkt und dem letzten verfügbaren Wiederherstellungspunkt kopieren), und klicken Sie auf **Weiter**.  
DPM benötigt Schreibberechtigungen für das Kopierziel der Transaktionsprotokolle.
11. Legen Sie Wiederherstellungsoptionen für die Netzwerk-Bandbreitenbeschränkung, SAN-basierte Wiederherstellung und E-Mail-Benachrichtigungen fest, und klicken Sie dann auf **Weiter**.
12. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

13. Verwenden Sie den Transact-SQL-Befehl „Restore“ mit dem HeaderOnly-Argument, um die Header-Informationen für die Transaktionsbefehle abzurufen. Der Header enthält Informationen, die die richtige Reihenfolge der Protokollsicherungssequenzen ermöglichen.
14. Verwenden Sie den Restore-Befehl mit dem Log-Argument, um die gewünschten Protokolle in der richtigen Reihenfolge auf die Datenbank anzuwenden.  
Weitere Informationen zum Restore-Befehl finden Sie unter [RESTORE-Argumente \(Transact-SQL\)](http://go.microsoft.com/fwlink/?LinkId=104665) (<http://go.microsoft.com/fwlink/?LinkId=104665>).

### **Siehe auch**

[Wiederherstellen einer SQL-Datenbank am ursprünglichen Speicherort](#)

[Wiederherstellen und Umbenennen von SQL-Datenbanken](#)

[Wiederherstellen einer Datenbank auf einer anderen Instanz von SQL Server](#)

[Kopieren von SQL-Datenbanken in einen Netzwerkordner](#)

[Kopieren von SQL-Datenbanken auf Band](#)

## **Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird**

---

In diesem Abschnitt finden Sie Anleitungen zum Verwalten geschützter Server, auf denen Windows SharePoint Services ausgeführt wird. Alle Informationen in diesem Abschnitt gelten sowohl für Microsoft® Office SharePoint® Server 2007 als auch für Windows SharePoint Services 3.0, sofern nicht anders angegeben.

### **In diesem Abschnitt**

[Allgemeine Wartung von Servern, auf denen Windows SharePoint Services ausgeführt wird](#)

[Ausführen von Windows SharePoint Services-Verwaltungsaufgaben](#)

[Wiederherstellen von Windows SharePoint Services-Daten](#)

# Allgemeine Wartung von Servern, auf denen Windows SharePoint Services ausgeführt wird

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- und Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßigen Sicherungen. Es gibt jedoch einige Besonderheiten, die zu berücksichtigen sind, wenn Sie auf Computern mit Microsoft® Windows® SharePoint Services, die von System Center Data Protection Manager (DPM) geschützt werden, Serververwaltungsaufgaben ausführen.

Wenn Sie Wartungsaufgaben für einen geschützten Servers ausführen müssen und für den Zeitraum der Wartungsarbeiten keine Schutzaufträge fortgesetzt werden sollen, können Sie den Schutz-Agent deaktivieren.

## So deaktivieren Sie einen Schutz-Agent

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Wählen Sie auf der Registerkarte **Agents** im Anzeigebereich den Namen des Computers mit dem zu deaktivierenden Schutz-Agent aus.
3. Klicken Sie im Bereich **Aktionen** auf **Schutz-Agent deaktivieren**.
4. Klicken Sie im Dialogfeld auf **OK**, um zu bestätigen, dass Sie den Vorgang fortsetzen möchten.

## In diesem Abschnitt

[Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern](#)

[Ausführen von Windows SharePoint Services-Wartungsaufgaben](#)

[Anwenden von Betriebssystem-Updates auf Windows SharePoint Services-Servern](#)

[Ausführen von Antivirusprogrammen auf Windows SharePoint Services-Servern](#)

## Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern

Das Ausführen der Datenträgerbereinigung, der Datenträgerdefragmentierung oder von Chkdsk.exe sollte keine negativen Auswirkungen auf die Leistung oder den Schutz von Daten haben.

## **Siehe auch**

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

[Verwenden von Windows-Wartungstools auf Exchange-Servern](#)

[Verwenden von Windows-Wartungstools auf SQL-Servern](#)

[Verwenden von Windows-Wartungstools auf virtuellen Servern](#)

## **Ausführen von Windows SharePoint Services-Wartungsaufgaben**

Wenn Sie das automatische Löschen von inaktiven Websites planen, koordinieren Sie diesen Zeitplan mit dem Schutzzeitplan, damit Ihnen immer eine aktuelle Kopie der gesicherten Site zur Verfügung steht.

## **Anwenden von Betriebssystem-Updates auf Windows SharePoint Services-Servern**

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Updates, „Fixes“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können für Computer, auf denen Windows SharePoint Services ausgeführt wird und die von DPM geschützt werden, die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Server Update Services. Da für einige Softwareupdates der Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

## **Ausführen von Antivirusprogrammen auf Windows SharePoint Services-Servern**

Um Datenbeschädigung in Replikaten und Wiederherstellungspunkten zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von DPM nicht erkannt werden. Anleitungen zur Konfiguration, damit das Antivirusprogramm infizierte Dateien löscht, finden Sie im Produkthandbuch des Antivirusprogramms.

# Ausführen von Windows SharePoint Services-Verwaltungsaufgaben

In diesem Abschnitt finden Sie Anleitungen und Richtlinien für die Verwaltung eines geschützten Windows SharePoint Services-Servers und zum Vornehmen von Änderungen nach der erstmaligen DPM-Konfiguration.

## In diesem Abschnitt

[Aktualisieren von Windows SharePoint Services](#)

[Verschieben von Windows SharePoint Services-Servern zwischen Domänen](#)

[Umbenennen von Windows SharePoint Services-Servern](#)

[Ändern des Front-End-Webservers](#)

[Hinzufügen von Datenbanken zu einer Windows SharePoint Services-Farm](#)

[Hinzufügen oder Entfernen von Servern in einer Windows SharePoint Services-Farm](#)

## Aktualisieren von Windows SharePoint Services

Windows SharePoint Services-Daten, zum Beispiel die Konfigurationsdatenbanken, die Inhaltsdatenbanken und andere Datenbanken und Dateien, die Teil der Windows SharePoint Services-Farm für Windows SharePoint Services 2.0 (WSS 2.0) sind, können von DPM als SQL Server-Datenbanken geschützt werden.

Wenn Sie WSS 2.0-Daten als SQL Server-Datenbanken schützen und dann ein Upgrade auf WSS 3.0 oder Microsoft Office SharePoint Server 2007 ausführen, müssen Sie den Schutz der Daten neu konfigurieren.

### So aktualisieren Sie von Windows SharePoint Services 2.0 auf Windows SharePoint Services 3.0 oder Microsoft Office SharePoint Server 2007

1. Erstellen Sie einen Wiederherstellungspunkt der WSS 2.0-Daten, die als SQL Server-Datenbank geschützt werden.
2. Beenden Sie den Schutz der Daten, und wählen Sie dabei die Option **Retain replica** (Replikat beibehalten).
3. Aktualisieren Sie den Server, auf dem Windows SharePoint Services ausgeführt wird.
4. Fügen Sie die aktualisierte Windows SharePoint Services-Farm einer Schutzgruppe hinzu, indem Sie sie als Windows SharePoint Services-Datenquelle auswählen.

Daten im beibehaltenen Replikat bleiben für die Wiederherstellung verfügbar, sind jedoch nicht der aktualisierten Windows SharePoint Services-Farm zugeordnet.

## Verschieben von Windows SharePoint Services-Servern zwischen Domänen

Folgendes ist für geschützte Computer nicht möglich:

- Domäne eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Domäne eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem Computer zuordnen, wenn der Computer wieder geschützt wird.

Es wird empfohlen, die Domäne eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen, während der Computer seine ursprüngliche Domänenmitgliedschaft beibehält.
- Die Datenquellen auf dem Computer schützen, nachdem er Mitglied einer anderen Domäne geworden ist.

### So ändern Sie die Domänenmitgliedschaft eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie die Domänenmitgliedschaft des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Umbenennen von Windows SharePoint Services-Servern

DPM verwendet den Namen des Computers als eindeutigen Bezeichner für Replikate, Wiederherstellungspunkte, DPM-Datenbankeinträge, Berichtsdatenbankeinträge usw.

Folgendes ist nicht möglich:

- Namen eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Namen eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem neuen Computernamen zuordnen.

Es wird empfohlen, den Namen eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen (alter Computernamen).
- Die Datenquellen auf dem Computer schützen (neuer Computernamen).

### **So ändern Sie den Namen eines geschützten Computers**

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikat und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikat löschen. Für die Endbenutzerwiederherstellung sind die Replikat jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie den Namen des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## **Ändern des Front-End-Webserver**

Um eine Serverfarm auf Servern mit Microsoft Windows SharePoint Services 3.0 oder Microsoft Office SharePoint Server 2007 zu schützen, starten Sie den Windows SharePoint Services VSS Writer-Dienst (WSS Writer-Dienst) und installieren den DPM-Schutz-Agent auf einem einzelnen Front-End-Webserver. DPM verwendet diesen Front-End-Webserver für die Ausführung von Sicherungen.

Im folgenden Verfahren wird als Beispiel eine Serverfarm mit zwei Front-End-Webservern, Server1 und Server2, verwendet. DPM verwendet Server1, um die Farm zu schützen. Sie müssen den Front-End-Webserver, den DPM verwendet, zu Server2 ändern, damit Sie Server1 aus der Farm entfernen können.

### **Hinweis**

Wenn der Front-End-Webserver, den DPM zum Schutz der Farm verwendet, nicht verfügbar ist, gehen Sie wie nachstehend ab Schritt 4 beschrieben vor, um den Front-End-Webserver zu ändern.



► **So ändern Sie den Front-End-Webserver, den DPM zum Schutz der Farm verwendet**

1. Beenden Sie den WSS Writer-Dienst auf Server1, indem Sie den folgenden Befehl in einer Befehlszeile eingeben:

**stsadm -o unregisterwsswriter**

2. Öffnen Sie auf Server1 den Registrierungs-Editor und navigieren Sie zum folgenden Schlüssel:

**HKLM\System\CCS\Services\VSS\VssAccessControl**

3. Überprüfen Sie alle Werte, die für den Teilschlüssel VssAccessControl aufgeführt sind. Wenn ein Eintrag einen Wert von 0 hat und ein anderer VSS Writer unter den zugeordneten Kontodetails ausgeführt wird, ändern Sie den Wert zu 1.

4. Installieren Sie einen Schutz-Agent auf Server2.

5. Ändern Sie auf Server2 in einer Befehlszeile das Verzeichnis zu *DPM-Installationsordner\bin\* und führen Sie den folgenden Befehl aus:

**ConfigureSharepoint.exe**

Sie werden aufgefordert, die Administratoranmeldedaten für die Windows SharePoint Services-Farm einzugeben. Diese Anmeldedaten für die Windows SharePoint Services-Farm müssen für einen lokalen Administrator auf dem Server gelten.

6. Es gibt ein bekanntes Problem, wenn die Serverfarm das einzige Mitglied der Schutzgruppe ist und die Schutzgruppe für den bandgestützten Schutz konfiguriert ist. Wenn Ihre Serverfarm das einzige Mitglied der Schutzgruppe ist, der bandgestützte Schutz verwendet wird und Sie den Front-End-Webserver, der von DPM zum Schutz der Farm verwendet wird, ändern möchten, müssen Sie der Schutzgruppe vorübergehend ein weiteres Mitglied hinzufügen, um die folgenden Schritte auszuführen:
  - a. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
  - b. Wählen Sie die Schutzgruppe aus, zu der die Serverfarm gehört, und klicken Sie auf **Schutzgruppe ändern**.
  - c. Fügen Sie im Assistenten zum Ändern von Gruppen einem beliebigen Server in der Schutzgruppe ein Volume hinzu. Nach Abschluss des Verfahrens können Sie dieses Volume wieder aus der Schutzgruppe entfernen.
  - d. Wenn die Schutzgruppe für kurzfristigen festplattengestützten Schutz und langfristigen bandgestützten Schutz konfiguriert ist, wählen Sie die Option zum manuellen Erstellen des Replikats aus. So können Sie verhindern, dass ein nicht benötigtes Replikat für das vorübergehend zur Schutzgruppe hinzugefügte Volume erstellt wird.
  - e. Schließen Sie den Assistenten ab.
7. Entfernen Sie Server1 aus der Schutzgruppe, und wählen Sie die dabei die Option zum Beibehalten der Replikate auf Festplatte und Band.
8. Wählen Sie die Schutzgruppe aus, zu der die Serverfarm gehört, und klicken Sie auf **Schutzgruppe ändern**.

9. Erweitern Sie im Assistenten zum Ändern von Gruppen im Fenster **Gruppenmitglieder auswählen** Server2, und wählen Sie die Serverfarm aus. Stellen Sie den Assistenten dann fertig.  
Es wird eine Konsistenzprüfung gestartet.
10. Falls Sie Schritt 6 ausgeführt haben, können Sie das Volume jetzt aus der Schutzgruppe entfernen.

## Hinzufügen von Datenbanken zu einer Windows SharePoint Services-Farm

Wenn eine Datenbank zu einer Windows SharePoint Services-Farm hinzugefügt bzw. daraus entfernt wird, kennzeichnet DPM das Replikats als inkonsistent und alarmiert den Administrator.

Wird eine Datenbank hinzugefügt, enthält die Warnung einen Link zum Ändern der Schutzgruppe. Nach Abschluss des Assistenten zum Ändern von Gruppen führt DPM eine Konsistenzprüfung aus. Der Schutz der Farm, einschließlich der hinzugefügten Datenbank, wird fortgesetzt.

Wird eine Datenbank entfernt, sollten Sie den Schutz der Serverfarm unter Verwendung der Option zum Beibehalten des Replikats beenden und die Farm dann erneut der Schutzgruppe hinzufügen.

## Hinzufügen oder Entfernen von Servern in einer Windows SharePoint Services-Farm

DPM verwendet einen einzelnen Front-End-Webserver, um die Farm zu schützen. Wenn Sie zusätzliche Front-End-Webserver hinzufügen oder andere Front-End-Webserver als den von DPM verwendeten entfernen, hat dies keine Auswirkungen auf den Schutz der Farm.

Wenn Sie den von DPM verwendeten Front-End-Webserver entfernen und den Schutz der Serverfarm aufrecht erhalten möchten, lesen Sie [Ändern des Front-End-Webservers](#).

## Wiederherstellen von Windows SharePoint Services-Daten

Bei der Wiederherstellung von Windows SharePoint Services-Daten gilt Folgendes:

- Die Details zu den Elementen werden auf der Zusammenfassungsseite des Wiederherstellungsassistenten für Windows SharePoint Services-Sites und -Elemente nicht angezeigt. Wenn Sie eine Windows SharePoint Services-Farm wiederherstellen, stellt DPM die Konfigurationsdatenbank der Farm wieder her, listet diese Datenbank jedoch nicht auf der Zusammenfassungsseite des Wiederherstellungsassistenten auf.

- Die Administrationsinhaltsdatenbank ist die erste Inhaltsdatenbank, die mit der Zentraladministration erstellt wird, wenn Sie die Farm einrichten. Stellen Sie die Administrationsinhaltsdatenbank nicht direkt wieder her, da dies zu einer Datenbeschädigung in der Windows SharePoint Services-Farm führen kann.
- Die Zeitpunkte der Wiederherstellungspunkte auf der Registerkarte Durchsuchen können sich von den Zeitpunkten auf der Registerkarte Suchen für Windows SharePoint Services-Daten unterscheiden. Auf der Registerkarte Suchen werden die richtigen Zeitpunkte der Wiederherstellungspunkte für Sites, Dokumente und Ordner angezeigt. Auf der Registerkarte Durchsuchen werden die Sicherungszeiten für die Farm angezeigt.
- Dokumente in Windows SharePoint Services können einen der folgenden Status aufweisen, wenn die Dokumentversionskontrolle aktiviert ist:
  - Erstellt, nicht eingereicht - nur für den Ersteller sichtbar
  - Eingereicht - sichtbar für den Administrator und Benutzer mit Berechtigung zum Veröffentlichen
  - Veröffentlicht - sichtbar für Benutzer mit Berechtigung zum Genehmigen
  - Genehmigt - sichtbar für alle Betrachter

Wenn Sie Windows SharePoint Services-Daten wiederherstellen, werden nur Dokumente wiederhergestellt, die eingereicht, veröffentlicht oder genehmigt wurden. Dokumente, die nicht eingereicht wurden, werden im Rahmen einer Websitesammlung- oder Dokumentwiederherstellung nicht wiederhergestellt. Dokumente, die sich im Papierkorb eines Benutzers oder der Websitesammlung befinden, werden im Rahmen einer Websitesammlung- oder Dokumentwiederherstellung nicht wiederhergestellt.

## In diesem Abschnitt

[Wiederherstellen von Windows SharePoint Services-Farmen](#)

[Wiederherstellen von Windows SharePoint Services-Sites](#)

[Wiederherstellen von Windows SharePoint Services-Elementen](#)

## Wiederherstellen von Windows SharePoint Services-Farmen

Um eine Windows SharePoint Services-Farm wiederherzustellen, muss das Wiederherstellungsziel die folgenden Anforderungen erfüllen:

- Die Front-End-Webserver weisen dieselbe Konfiguration wie beim Erstellen des Wiederherstellungspunkts auf.
- Die Farmstruktur muss auf dem Front-End-Webserver erstellt werden; die Farmdaten werden in der vorhandenen Struktur wiederhergestellt.
- Die Instanzen von SQL Server sind mit denselben Namen konfiguriert, die beim Erstellen des Wiederherstellungspunkts verwendet wurden.

▶ **So stellen Sie Farmdaten in einer funktionierenden Farm wieder her**

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Erweitern Sie im Bereich **Protected data** (Geschützte Daten) den Server, der die wiederherzustellende Farm enthält, und klicken Sie auf **All Protected SharePoint Data** (Alle geschützten SharePoint-Daten).  
Die Farm wird im Bereich **Recoverable item** (Wiederherstellbares Element) als *Servername\Farmname* angezeigt.
3. Wählen Sie mithilfe des Kalenders und des Menüs **Wiederherstellungszeit** einen Wiederherstellungspunkt aus.
4. Klicken Sie im Bereich **Recoverable item** (Wiederherstellbares Element) auf das Farmelement.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.
6. Schließen Sie den Assistenten ab.

▶ **So stellen Sie Farmdaten wieder her, wenn die geschützte Farm nicht verfügbar ist**

1. Erstellen Sie eine neue Farm, die dieselbe Instanz von SQL Server und denselben Front-End-Webserver wie die ursprünglich geschützte Farm verwendet.
2. Registrieren Sie auf dem Front-End-Webserver, den DPM zum Schutz der ursprünglichen Farm verwendet hat, den Windows SharePoint Services VSS Writer-Dienst (WSS Writer-Dienst), indem Sie in einer Befehlszeile den folgenden Befehl ausführen:  
**stsadm -o registerwsswriter**
3. Klicken Sie auf dem DPM-Server in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
4. Erweitern Sie im Bereich **Protected data** (Geschützte Daten) den Server, der die wiederherzustellende Farm enthält, und klicken Sie auf **All Protected SharePoint Data** (Alle geschützten SharePoint-Daten).  
Die Farm wird im Bereich **Recoverable item** (Wiederherstellbares Element) als *Servername\Farmname* angezeigt.
5. Wählen Sie mithilfe des Kalenders und des Menüs **Wiederherstellungszeit** einen Wiederherstellungspunkt aus.
6. Klicken Sie im Bereich **Recoverable item** (Wiederherstellbares Element) auf das Farmelement.
7. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.
8. Schließen Sie den Assistenten ab.
9. Führen Sie auf dem Haupt-Front-End-Webserver der Serverfarm den Konfigurationsassistenten für SharePoint-Produkte und -Technologien aus, und trennen Sie den Front-End-Webserver von der Farm.

 **Hinweis**

Wenn der Haupt-Front-End-Webserver der Serverfarm nicht der Front-End-Webserver ist, den DPM zum Schutz der Farm verwendet, müssen Sie auch den Front-End-Webserver abtrennen, den DPM zum Schutz der Farm verwendet.

10. Öffnen Sie Internet Information Services (IIS), und löschen Sie alle Website- und Anwendungspoleinträge, die die Farm betreffen.
11. Führen Sie den Konfigurationsassistenten für SharePoint-Produkte und -Technologien aus, wählen Sie die Option für die Verbindung mit einer vorhandenen Serverfarm, und geben Sie den Servernamen und den Datenbanknamen für die in Schritt 1 erstellte Farm an.

 **Hinweis**

Führen Sie Schritt 11 für alle Front-End-Webserver der Serverfarm aus.

12. Klicken Sie auf der Seite **Completing the SharePoint Products and Technologies Configuration Wizard** (Assistenten abschließen) auf **Advanced Settings** (Erweiterte Einstellungen) und dann auf **Weiter**.
13. Wählen Sie auf der Seite **Advanced Settings** (Erweiterte Einstellungen) die Option **Use this machine to host the web site** (Diesen Computer zum Hosten der Website verwenden), und schließen Sie den Assistenten ab.

## Siehe auch

[Wiederherstellen von Windows SharePoint Services-Sites](#)

[Wiederherstellen von Windows SharePoint Services-Elementen](#)

## Wiederherstellen von Windows SharePoint Services-Sites

Um eine Microsoft Windows SharePoint Services-Site wiederherzustellen, müssen Sie Folgendes ausführen:

1. Erstellen Sie eine Farm, die für die Wiederherstellung verwendet werden kann.
2. Erstellen Sie eine Webanwendung für die Wiederherstellung.
3. Verwenden Sie DPM, um die Site in der Wiederherstellungsfarm wiederherzustellen.

Die folgenden Anforderungen gelten für eine Sitewiederherstellung:

- Die Farm, die für die Wiederherstellung verwendet wird, sollte eine Farm mit nur einem Server sein.
- Wenn Sie eine MOSS-Farm schützen, muss es sich bei der Wiederherstellungsfarm ebenfalls um eine MOSS-Farm handeln.
- Die auf der Wiederherstellungsfarm installierten Funktionen und Vorlagen müssen mit denen auf der Zielfarm übereinstimmen.

- Wenn auf der geschützten Farm Service Packs oder Updates installiert wurden, müssen auf der Wiederherstellungsfarm dieselben Service Packs und Updates installiert sein; andernfalls können Wiederherstellungsvorgänge auf Elementebene fehlschlagen.
- Die Wiederherstellungs- und Zielfarmen müssen dieselbe Sprache verwenden und müssen dieselben Sprachpacks installiert haben.
- Die Zielfarm muss eine Websitesammlung mit demselben Pfad wie die ursprüngliche geschützte Website enthalten. Wenn die Websitesammlung nicht vorhanden ist, können Sie eine leere Websitesammlung unter dem richtigen Pfad auf der Zielfarm erstellen, bevor Sie die Wiederherstellung ausführen.

Wenn Sie eine Website wiederherstellen, stellt DPM die Datenbank in der Wiederherstellungsfarm wieder her, extrahiert die Website aus der Wiederherstellungsfarm und importiert sie in die Zielfarm. Während dieses Prozesses erstellt DPM eine temporäre Datei auf der Wiederherstellungsfarm an einem im Wiederherstellungsassistenten festgelegten Speicherort. Sie sollten die temporären Dateien an diesem Speicherort regelmäßig löschen.

#### So stellen Sie eine Website wieder her

1. Erstellen Sie eine Farm, die DPM für die Wiederherstellung verwenden kann. Anleitungen zum Erstellen einer Wiederherstellungsfarm finden Sie, in englischer Sprache, unter „[Deploy in a simple server farm](http://go.microsoft.com/fwlink/?LinkId=95150)“ (http://go.microsoft.com/fwlink/?LinkId=95150).
2. Erstellen Sie eine Webanwendung, und nennen Sie sie DPMRecoveryWebApplication. Anleitungen zum Erstellen einer Webanwendung finden Sie, in englischer Sprache, unter „[Create or extend Web applications \(Windows SharePoint Services\)](http://go.microsoft.com/fwlink/?LinkId=94374)“ (http://go.microsoft.com/fwlink/?LinkId=94374).
3. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Wiederherstellung**.
4. Erweitern Sie im Bereich **Protected data** (Geschützte Daten) den Server, der die wiederherzustellende Farm enthält, und klicken Sie auf **All Protected SharePoint Data** (Alle geschützten SharePoint-Daten).  
Die Farm wird im Bereich **Recoverable item** (Wiederherstellbares Element) als *Servername\Farmname* angezeigt.
5. Doppelklicken Sie auf das Farmelement.  
Die Datenbanken für die Farm werden im Bereich **Recoverable item** (Wiederherstellbares Element) angezeigt.
6. Wählen Sie einen Wiederherstellungspunkt für die Website, die Sie wiederherstellen möchten, und klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.
7. Wählen Sie im Fenster **Select Recovery Type** (Wiederherstellungstyp wählen) die Option **Recover to original site** (Auf Originalwebsite wiederherstellen).

8. Geben Sie im Fenster **Specify Recovery Farm** (Wiederherstellungsfarm festlegen) die Informationen für die in Schritt 1 erstellte Wiederherstellungsfarm ein, und schließen Sie den Assistenten ab.

DPM stellt die Website in der ursprünglichen Farm wieder her.

## Siehe auch

[Wiederherstellen von Windows SharePoint Services-Farmen](#)

[Wiederherstellen von Windows SharePoint Services-Elementen](#)

## Wiederherstellen von Windows SharePoint Services-Elementen

Sie können Windows SharePoint Services-Elemente, zum Beispiel Listen und Dokumente, von einem DPM-Wiederherstellungspunkt auf der ursprünglichen Website oder auf einer anderen Website wiederherstellen.

### So stellen Sie ein Element wieder her

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Wiederherstellung**.
2. Erweitern Sie im Bereich **Protected data** (Geschützte Daten) den Server, der die wiederherzustellende Farm enthält, doppelklicken Sie auf **All Protected SharePoint Data** (Alle geschützten SharePoint-Daten), und doppelklicken Sie auf den Namen der Serverfarm.  
  
Inhaltsdatenbanken werden im Bereich **Recoverable item** (Wiederherstellbares Element) angezeigt.
3. Wählen Sie mithilfe des Kalenders und des Menüs **Wiederherstellungszeit** einen Wiederherstellungspunkt aus.
4. Doppelklicken Sie im Bereich **Recoverable item** (Wiederherstellbares Element) auf die Inhaltsdatenbank, doppelklicken Sie auf die Website, und doppelklicken Sie dann auf die angezeigten Elemente, um zu dem wiederherzustellenden Element zu navigieren.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**, und schließen Sie den Assistenten ab.

## Siehe auch

[Wiederherstellen von Windows SharePoint Services-Farmen](#)

[Wiederherstellen von Windows SharePoint Services-Sites](#)

# Verwalten von geschützten virtuellen Servern

---

In diesem Abschnitt finden Sie Richtlinien zum Ausführen allgemeiner Wartungsaufgaben auf geschützten Servern. Außerdem enthält dieser Abschnitt einen Leitfaden zum Ändern der Computerkonfiguration, wenn der Computer durch DPM geschützt wird.

## In diesem Abschnitt

[Allgemeine Wartung von Servern, auf denen Virtual Server ausgeführt wird](#)

[Ausführen von Virtual Server-Verwaltungsaufgaben](#)

[Wiederherstellen von Virtual Server-Daten](#)

## Allgemeine Wartung von Servern, auf denen Virtual Server ausgeführt wird

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- und Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßigen Sicherungen. Es gibt jedoch einige Besonderheiten, die zu berücksichtigen sind, wenn Sie auf Computern mit Virtual Server, die von System Center Data Protection Manager (DPM) geschützt werden, Serververwaltungsaufgaben ausführen.

Wenn Sie Wartungsaufgaben für einen geschützten Servers ausführen müssen und für den Zeitraum der Wartungsarbeiten keine Schutzaufträge fortgesetzt werden sollen, können Sie den Schutz-Agent mit dem folgenden Verfahren deaktivieren.



### Hinweis

Wenn Sie einen Schutz-Agent für einen Server deaktivieren, der ein Clusterknoten ist, sollten Sie den Schutz-Agent für jeden Knoten des Clusters deaktivieren.

### ► So deaktivieren Sie einen Schutz-Agent

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Wählen Sie auf der Registerkarte **Agents** im Anzeigebereich den Namen des Computers mit dem zu deaktivierenden Schutz-Agent aus.
3. Klicken Sie im Bereich **Aktionen** auf **Schutz-Agent deaktivieren**.
4. Klicken Sie im Dialogfeld auf **OK**, um zu bestätigen, dass Sie den Vorgang fortsetzen möchten.

## In diesem Abschnitt

[Verwenden von Windows-Wartungstools auf virtuellen Servern](#)

[Anwenden von Betriebssystem-Updates auf Virtual Server](#)

[Ausführen von Antivirusprogrammen auf Virtual Server](#)



## Verwenden von Windows-Wartungstools auf Virtual Server

Das Ausführen der Datenträgerbereinigung, der Datenträgerdefragmentierung oder von Chkdsk.exe sollte keine negativen Auswirkungen auf die Leistung oder den Schutz von Daten haben.

### Siehe auch

[Verwenden von Windows-Wartungstools auf dem DPM-Server](#)

[Verwenden von Windows-Wartungstools für Dateiserver und Workstations](#)

[Verwenden von Windows-Wartungstools auf Exchange-Servern](#)

[Verwenden von Windows-Wartungstools auf SQL-Servern](#)

[Verwenden von Windows-Wartungstools auf Windows SharePoint Services-Servern](#)

## Anwenden von Betriebssystem-Updates auf Virtual Server

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Updates, „Fixes“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können für Computer, auf denen Virtual Server ausgeführt wird und die von DPM geschützt werden sowie auf virtuellen Rechnern, die von DPM geschützt werden, die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Server Update Services. Da für einige Softwareupdates der Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

## Ausführen von Antivirusprogrammen auf Virtual Server

Um Datenbeschädigung in Replikaten und Wiederherstellungspunkten zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von DPM nicht erkannt werden. Anleitungen zur Konfiguration, damit das Antivirusprogramm infizierte Dateien löscht, finden Sie im Produkthandbuch des Antivirusprogramms.

# Ausführen von Virtual Server-Verwaltungsaufgaben

In diesem Abschnitt finden Sie Anleitungen und Richtlinien für die Verwaltung eines geschützten virtuellen Servers und zum Vornehmen von Änderungen nach der erstmaligen DPM-Konfiguration.

## In diesem Abschnitt

[Verschieben von Virtual-Servern zwischen Domänen](#)

[Umbenennen von Virtual-Servern](#)

[Umbenennen von virtuellen Rechnern](#)

[Verschieben von virtuellen Rechnern oder virtuellen Festplatten](#)

[Schützen von Anwendungsdaten auf virtuellen Rechnern](#)

## Verschieben von Virtual-Servern zwischen Domänen

Folgendes ist für geschützte Computer nicht möglich:

- Domäne eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Domäne eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem Computer zuordnen, wenn der Computer wieder geschützt wird.

Es wird empfohlen, die Domäne eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie zwei Aufgaben ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen, während der Computer seine ursprüngliche Domänenmitgliedschaft beibehält.
- Die Datenquellen auf dem Computer schützen, nachdem er Mitglied einer anderen Domäne geworden ist.

### So ändern Sie die Domänenmitgliedschaft eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie die Domänenmitgliedschaft des Computers.

4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Umbenennen von Virtual-Servern

DPM verwendet den Namen des Computers als eindeutigen Bezeichner für Replikate, Wiederherstellungspunkte, DPM-Datenbankeinträge, Berichtsdatenbankeinträge usw.

Folgendes ist nicht möglich:

- Namen eines geschützten Computers ändern und den Schutz der Daten ohne Störung fortsetzen.
- Namen eines geschützten Computers ändern und die vorhandenen Replikate und Wiederherstellungspunkte dem neuen Computernamen zuordnen.

Es wird empfohlen, den Namen eines geschützten Computers nicht zu ändern. Lässt sich dies jedoch nicht umgehen, müssen Sie Folgendes ausführen:

- Die Datenquellen auf dem Computer aus dem Schutz nehmen (alter Computernamen).
- Die Datenquellen auf dem Computer schützen (neuer Computernamen).

### So ändern Sie den Namen eines geschützten Computers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.  
Wenn Sie die Replikate und Wiederherstellungspunkte beibehalten, ist der Zugriff auf die Daten bei einer Administratorwiederherstellung möglich, bis Sie die Replikate löschen. Für die Endbenutzerwiederherstellung sind die Replikate jedoch nicht zugänglich.
2. Deinstallieren Sie den Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie den Namen des Computers.
4. Installieren Sie einen Schutz-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Datenquellen den Schutzgruppen auf dem DPM-Server hinzu.  
Informationen zu Aufgaben, die Schutz-Agents und Schutzgruppen betreffen, finden Sie, in englischer Sprache, in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Umbenennen von virtuellen Rechnern

Beim Umbenennen eines virtuellen Rechners wird der Name der Konfigurationsdatei für den virtuellen Rechner (.vmc), der Name des virtuellen Rechners, wie er auf der Administrationswebsite angezeigt wird, und der Anzeigename des Fensters für den virtuellen Rechner geändert, nicht jedoch der Name des Ordners, der den virtuellen Rechner enthält.

Wenn Sie den Namen eines virtuellen Rechners ändern, der als Gast auf einem Virtual Server geschützt wird, setzt DPM den Schutz fort und erfasst die Änderung so wie auch alle anderen Änderungen an geschützten Daten erfasst werden.

## Verschieben von virtuellen Rechnern oder virtuellen Festplatten

### Verschieben eines virtuellen Rechners

► **So verschieben Sie einen virtuellen Rechner, der von DPM geschützt wird**

1. Kopieren Sie den virtuellen Rechner auf den neuen Host. Anleitungen hierzu finden Sie, in englischer Sprache, unter „[Copying, managing, and renaming virtual machines](http://go.microsoft.com/fwlink/?LinkId=95298)“ (<http://go.microsoft.com/fwlink/?LinkId=95298>).
2. Fügen Sie den kopierten virtuellen Rechner einer Schutzgruppe hinzu.
3. Entfernen Sie den ursprünglichen virtuellen Rechner vom ursprünglichen Host. Anleitungen hierzu finden Sie, in englischer Sprache, unter „[Removing virtual machines](http://go.microsoft.com/fwlink/?LinkId=95299)“ (<http://go.microsoft.com/fwlink/?LinkId=95299>).
4. Beenden Sie den Schutz des ursprünglichen virtuellen Rechners.

### Verschieben einer virtuellen Festplatte

Wenn Sie große Datenmengen speichern oder die Datenträgerleistung verbessern möchten, können Sie eine virtuelle Festplatte verschieben. Eine virtuelle Festplatte für einen virtuellen Rechner wird als .vhd-Datei gespeichert. Um den Schutz für eine virtuelle Festplatte, die auf ein neues Volume verschoben wird, aufrechtzuerhalten, starten Sie den Assistenten zum Ändern von Gruppen für die entsprechende Schutzgruppe, und führen eine Konsistenzprüfung aus.

## Schützen von Anwendungsdaten auf virtuellen Rechnern

Wenn Sie einen virtuellen Rechner einer Schutzgruppe hinzufügen, schützen Sie die vollständige Konfiguration des virtuellen Rechners, einschließlich Betriebssystem, Anwendungen und Anwendungsdaten. Es ist jedoch nicht möglich, ausschließlich Anwendungsdaten aus den Wiederherstellungspunkten für den virtuellen Rechner wiederherzustellen; Sie können nur den gesamten virtuellen Rechner wiederherstellen. Wenn Sie den virtuellen Rechner wiederherstellen, werden Anwendungen mit allen Daten, die zum Zeitpunkt der Erstellung des Wiederherstellungspunktes vorhanden waren, wiederhergestellt.

Es ist nicht nötig, einen DPM-Schutz-Agent auf einem virtuellen Rechner zu installieren, um ihn als virtuellen Rechner auf dem Virtual Server-Host zu schützen.

Um nur Anwendungsdaten für Anwendungen, die auf virtuellen Rechnern ausgeführt werden, wiederherzustellen, müssen Sie einen Schutz-Agent auf dem virtuellen Rechner installieren und die Anwendungsdaten explizit als Schutzgruppenmitglieder auswählen.

Sie können sowohl die virtuellen Rechner als Gäste auf dem Virtual Server-Host als auch die Anwendungsdaten auf den virtuellen Rechnern als Anwendungen schützen.

Weitere Informationen zum Schutz von Anwendungsdaten finden Sie, in englischer Sprache, unter den Themen zum Schutz bestimmter Datentypen, zum Beispiel Exchange Server-Daten oder SQL Server-Daten in der [DPM-Hilfe](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## Wiederherstellen von Virtual Server-Daten

### In diesem Abschnitt

[Wiederherstellen des Virtual Server-Hosts](#)

[Wiederherstellen von virtuellen Rechnern](#)

[Wiederherstellen von virtuellen Rechnern als Dateien](#)

### Wiederherstellen des Virtual Server-Hosts

Wenn Sie einen Virtual Server-Host und seine virtuellen Rechner schützen, sind die wiederherstellbaren Elemente die Virtual Server-Konfiguration und die einzelnen virtuellen Rechner. Sie sollten die Virtual Server-Konfiguration wiederherstellen, bevor Sie einzelne virtuelle Rechner wiederherstellen.

#### So stellen Sie einen virtuellen Rechner wieder her

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Suchen Sie den Namen des virtuellen Servers, den Sie wiederherstellen möchten, und wählen Sie die Daten im Ergebnisfenster aus.
3. Wählen Sie das fett formatierte Datum für den Wiederherstellungspunkt, den Sie wiederherstellen möchten. Verfügbare Wiederherstellungspunkte werden im Kalender des Abschnitts mit den Wiederherstellungspunkten in Fettschrift angezeigt.
4. Klicken Sie im Bereich **Recoverable item** (Wiederherstellbares Element) auf das Element der Virtual Server-Konfiguration.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**. Der Wiederherstellungsassistent wird gestartet.
6. Überprüfen Sie die Auswahl für die Wiederherstellung, und klicken Sie auf **Weiter**.

7. Wählen Sie **Recover to original instance** (Auf ursprünglicher Instanz wiederherstellen), und klicken Sie auf **Weiter**. Die aktuellen Dateien werden bei der Wiederherstellung überschrieben.
8. Legen Sie die Wiederherstellungsoptionen fest, und klicken Sie auf **Weiter**. Es stehen folgende Wiederherstellungsoptionen zur Verfügung:
  - a. Wählen Sie **Enable SAN-based recovery using hardware snapshots** (SAN-basierte Wiederherstellung mit Hardware-Snapshots aktivieren), um zur schnelleren Wiederherstellung SAN-basierte Hardware-Snapshots zu verwenden.

Diese Option ist nur gültig, wenn in Ihrem SAN die Hardware-Snapshot-Funktion aktiviert ist, das SAN Klone erstellen und einen Klon aufteilen kann, damit er schreibfähig ist, und wenn der geschützte Computer und der DPM-Server an dasselbe SAN angeschlossen sind.
  - b. Klicken Sie im Bereich **Benachrichtigung** auf die Option **Send an e-mail when the recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden), und geben Sie die Empfänger der Benachrichtigung an. Trennen Sie die E-Mail-Adressen durch Kommas.
9. Überprüfen Sie die Wiederherstellungseinstellungen, und klicken Sie auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen von virtuellen Rechnern](#)

[Wiederherstellen von virtuellen Rechnern als Dateien](#)

## Wiederherstellen von virtuellen Rechnern

Wenn Sie einen Virtual Server-Host und seine virtuellen Rechner schützen, sind die wiederherstellbaren Elemente die Virtual Server-Konfiguration und die einzelnen virtuellen Rechner. Sie sollten die Virtual Server-Konfiguration wiederherstellen, bevor Sie einzelne virtuelle Rechner wiederherstellen.

Wenn Sie den virtuellen Rechner wiederherstellen, werden Anwendungen mit allen Daten, die zum Zeitpunkt der Erstellung des Wiederherstellungspunktes vorhanden waren, wiederhergestellt.

### So stellen Sie einen virtuellen Rechner wieder her

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Suchen Sie den Namen des virtuellen Rechners, den Sie wiederherstellen möchten, und wählen Sie die Daten im Ergebnisfenster aus.

3. Verfügbare Wiederherstellungspunkte werden im Kalender des Abschnitts mit den Wiederherstellungspunkten in Fettschrift angezeigt. Wählen Sie das fett formatierte Datum für den Wiederherstellungspunkt, den Sie wiederherstellen möchten.
4. Klicken Sie im Bereich **Recoverable item** (Wiederherstellbares Element) auf den virtuellen Rechner, den Sie wiederherstellen möchten.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**. DPM startet den Wiederherstellungsassistenten.
6. Überprüfen Sie die Auswahl für die Wiederherstellung, und klicken Sie auf **Weiter**.
7. Wählen Sie **Recover to original instance** (Auf ursprünglicher Instanz wiederherstellen), und klicken Sie auf **Weiter**. Die aktuellen Dateien werden bei der Wiederherstellung überschrieben.
8. Legen Sie die Wiederherstellungsoptionen fest, und klicken Sie auf **Weiter**.
  - a. Wählen Sie **Enable SAN-based recovery using hardware snapshots** (SAN-basierte Wiederherstellung mit Hardware-Snapshots aktivieren), um zur schnelleren Wiederherstellung SAN-basierte Hardware-Snapshots zu verwenden.  
Diese Option ist nur gültig, wenn in Ihrem SAN die Hardware-Snapshot-Funktion aktiviert ist, das SAN Klone erstellen und einen Klon aufteilen kann, damit er schreibfähig ist, und wenn der geschützte Computer und der DPM-Server an dasselbe SAN angeschlossen sind.
  - b. Klicken Sie im Bereich **Benachrichtigung** auf die Option **Send an e-mail when the recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden), und geben Sie die Empfänger der Benachrichtigung an. Trennen Sie die E-Mail-Adressen durch Kommas.
9. Überprüfen Sie die Wiederherstellungseinstellungen, und klicken Sie auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen des Virtual Server-Hosts](#)

[Wiederherstellen von virtuellen Rechnern als Dateien](#)

## Wiederherstellen von virtuellen Rechnern als Dateien

Sie können die Virtual Server-Konfiguration und virtuelle Rechner als Dateien in einem Netzwerkordner wiederherstellen, sodass Sie diese Dateien auf einen alternativen Virtual Server-Host kopieren können.

Die folgenden Dateien werden im Netzwerkordner wiederhergestellt:

- Für die Virtual Server-Konfiguration options.xml
- Für jeden virtuellen Rechner alle zugeordneten .vhd-, .vmc- und .vsv-Dateien

Wenn Sie einen virtuellen Rechner in einem Netzwerkordner wiederherstellen und die Dateien dann auf einen neuen Virtual Server-Host kopieren und den virtuellen Rechner starten, wird möglicherweise eine Fehlermeldung angezeigt, dass der Server unerwartet heruntergefahren wurde. Dies kann auftreten, da DPM die Wiederherstellungsdateien nicht als „erwarteter Shutdown“ kennzeichnen kann. Die wiederhergestellten Dateien sind ansonsten anwendungskonsistent.

Wenn die .vhd-Datei für einen virtuellen Rechner im Stammverzeichnis eines Volumes gespeichert ist und Sie den virtuellen Rechner an einem anderen Speicherort wiederherstellen, wird die .vhd-Datei mit den Verzeichnisattributen „versteckt“ und „System“ wiederhergestellt. Um die wiederhergestellte .vhd-Datei anzuzeigen, müssen Sie die Verzeichnisattribute entfernen.

### So stellen Sie virtuelle Rechner als Dateien wieder her

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Wiederherstellung**.
2. Wählen Sie mithilfe der Durchsuchen-Funktion die Speichergruppe aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf dem Kalender auf ein beliebiges fettformatiertes Datum, um die für dieses Datum verfügbaren Wiederherstellungspunkte zu erhalten. Im Menü **Wiederherstellungszeit** sind die Zeitpunkte aller verfügbaren Wiederherstellungspunkte aufgeführt.
4. Wählen Sie im Menü **Wiederherstellungszeit** den Wiederherstellungspunkt, den Sie verwenden möchten.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird gestartet.
6. Klicken Sie im Fenster **Review recovery selection** (Auswahl für die Wiederherstellung überprüfen) auf **Weiter**.
7. Wählen Sie **Copy files to network location** (Dateien in Netzwerkordner kopieren), und klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **Specify destination** (Ziel festlegen) den Netzwerkordner an, in den die Dateien kopiert werden sollen.



9. Geben Sie die Wiederherstellungsoptionen an:
  - a. Wählen Sie **Apply security settings of the destination computer** (Sicherheitseinstellungen des Zielcomputers anwenden) oder **Apply the security settings of the recovery point version** (Sicherheitseinstellungen der Wiederherstellungspunktversion anwenden).
  - b. Wählen Sie **Enable SAN-based recovery using hardware snapshots** (SAN-basierte Wiederherstellung mit Hardware-Snapshots aktivieren), um zur schnelleren Wiederherstellung SAN-basierte Hardware-Snapshots zu verwenden.

Diese Option ist nur gültig, wenn in Ihrem SAN die Hardware-Snapshot-Funktion aktiviert ist, das SAN Klone erstellen und aufteilen kann, damit der Klon schreibfähig ist, und wenn der geschützte Computer und der DPM-Server an dasselbe SAN angeschlossen sind.
  - c. Klicken Sie im Bereich **Benachrichtigung** auf die Option **Send an e-mail when the recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden), und geben Sie die Empfänger der Benachrichtigung an. Trennen Sie die E-Mail-Adressen durch Kommas.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Wiederherstellungseinstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Siehe auch

[Wiederherstellen des Virtual Server-Hosts](#)

[Wiederherstellen von virtuellen Rechnern](#)

# Leistungsverwaltung

---

In den einzelnen Themen dieses Abschnitts werden Leistungserwartungen definiert und es wird erläutert, wie die Leistung von Data Protection Manager (DPM) optimiert werden kann. Die tatsächlichen Ergebnisse sind von der Netzwerkgeschwindigkeit, den Leistungsmerkmalen der geschützten Computer, der Größe der geschützten Daten und der Änderungsrate der geschützten Daten abhängig.

## In diesem Abschnitt

[Auswirkungen von DPM auf die Leistung](#)

[DPM und Arbeitsspeicher](#)

[Leistungsindikatoren](#)

[Verbessern der Leistung](#)

[Verwalten der DPM-Leistung in einem WAN](#)

[Auswirkungen von Schutzgruppenänderungen auf Aufträge](#)

## Siehe auch

[Wiederherstellung im Notfall](#)

[Verwalten von DPM-Servern](#)

[Verwalten von geschützten Dateiservern und Workstations](#)

[Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird](#)

[Verwalten von geschützten virtuellen Servern](#)

[Verwalten von Bandbibliotheken](#)

## Auswirkungen von DPM auf die Leistung

Eines der Themen, mit denen Sie sich als Administrator auseinandersetzen müssen, ist die Auswirkung von DPM auf System- und Netzwerkressourcen. Die primären Datenübertragungsvorgänge sind die folgenden:

- **Replikaterstellung.** Dieser Vorgang wird für jedes Schutzgruppenmitglied einmal ausgeführt.
- **Änderungsnachverfolgung.** Dies ist ein fortlaufender Prozess auf jedem geschützten Dateiserver.
- **Synchronisierung.** Dieser Vorgang wird nach einem regelmäßigen Zeitplan ausgeführt.
- **Konsistenzprüfung.** Dieser Vorgang wird im Fall eines inkonsistenten Replikats ausgeführt.
- **Vollständige Schnellsicherungen.** Dieser Vorgang wird nach einem regelmäßigen Zeitplan ausgeführt.
- **Sicherung auf Band.** Dieser Vorgang wird nach einem regelmäßigen Zeitplan ausgeführt.

Ein Verständnis dieser Vorgänge und DPM-Prozesse erweist sich beim Ermitteln realistischer Erwartungen für die Leistung als nützlich.

## In diesem Abschnitt

[Replikaterstellung](#)

[Änderungsnachverfolgung](#)

[Synchronisierung](#)

[Konsistenzprüfung](#)

[Vollständige Schnellsicherung](#)

[Sicherung auf Band](#)

[DPM-Prozesse](#)

## Siehe auch

[Leistungsverwaltung](#)

## Replikaterstellung

In DPM ist ein Replikat eine vollständige Kopie der geschützten Daten auf einem Volume, in einer Datenbank oder in einer Speichergruppe. Der DPM-Schutz-Agent auf dem geschützten Computer sendet die zu schützenden Daten an den DPM-Server. Von jedem Mitglied der Schutzgruppe wird ein Replikat erstellt. Die Replikaterstellung ist einer der DPM-Vorgänge, für die die meisten Ressourcen erforderlich sind, und benötigt in besonderem Maße Netzwerkressourcen.

Typischerweise wird die Leistung der Replikaterstellung durch die Geschwindigkeit der Netzwerkverbindung zwischen DPM-Server und den geschützten Computern begrenzt. Mit anderen Worten, der Zeitaufwand für die Übertragung einer Datenmenge von 1 GB von einem geschützten Computer an den DPM-Server wird durch die Datenmenge festgelegt, die im Netzwerk pro Sekunde übertragen werden kann.

In der folgenden Tabelle wird der Zeitaufwand für die Übertragung verschiedener Datenmengen bei unterschiedlichen Netzwerkgeschwindigkeiten unter optimalen Bedingungen dargestellt. Die Zeit wird in Stunden angegeben, sofern nicht ausdrücklich Minuten angegeben sind.

### Zeitaufwand für die Datenübertragung über ein Netzwerk bei verschiedenen Geschwindigkeiten

Datengröße	Netzwerkgeschwindigkeit 1 Gbit/s	Netzwerkgeschwindigkeit 100 Mbit/s	Netzwerkgeschwindigkeit 32 Mbit/s	Netzwerkgeschwindigkeit 8 Mbit/s	Netzwerkgeschwindigkeit 2 Mbit/s	Netzwerkgeschwindigkeit 512 Kbit/s
1 GB	< 1 Minute	< 1 Stunde	< 1	< 1	1,5	6
50 GB	<10 Minuten	1,5 Stunden	5	18	71	284
200 GB	<36 Minuten	6 Stunden	18	71	284	1137
500 GB	<1,5 Stunden	15	45	178	711	2844



#### Hinweis

- Gbit/s = Gigabit pro Sekunde, Mbit/s = Megabit pro Sekunde, Kbit/s = Kilobit pro Sekunde. Bei den Zahlen für eine Netzwerkgeschwindigkeit von 1 Gbit/s wird davon ausgegangen, dass die Datenträgergeschwindigkeit auf dem DPM-Server und auf dem geschützten Computer keinen Engpass verursacht. Die Dauer für die Fertigstellung der ersten Replikaterstellung (ER) kann typischerweise wie folgt berechnet werden:
- ER: Stunden = ((Datengröße in MB) / (0,8 x Netzwerkgeschwindigkeit in MB/s)) / 3600
- Hinweis 1: Die Netzwerkgeschwindigkeit wird durch Division mit 8 von Bit in Byte umgerechnet.
- Hinweis 2: Die Netzwerkgeschwindigkeit wird mit 0,8 multipliziert, da die maximale Netzwerkeffizienz ungefähr 80 % beträgt.

In einem äußerst schnellen Netzwerk, z. B. einer Gigabitverbindung, wird die Geschwindigkeit der Replikaterstellung durch die Datenträgergeschwindigkeit des DPM-Servers oder des geschützten Computers bestimmt – je nachdem, welche geringer ist.

Die Auswirkungen der Replikaterstellung auf die Netzwerkleistung können durch Verwenden der Netzwerk-Bandbreitenbeschränkung verringert werden. Weitere Informationen finden Sie unter [Verwenden der Netzwerk-Bandbreitenbeschränkung](#).

Um die Netzwerkauslastung durch Replikaterstellung zu vermeiden, können Sie Replikate manuell vom Band oder anderen Wechselmedien erstellen. Weitere Informationen finden Sie unter [Manuelles Erstellen von Replikaten](#).

### **Siehe auch**

[Auswirkungen von DPM auf die Leistung](#)

[Leistungsverwaltung](#)

## **Änderungsnachverfolgung**

Nach Erstellen des Replikats startet der DPM-Schutz-Agent auf dem Computer die Nachverfolgung von geschützten Daten auf diesem Computer. Änderungen an Dateien werden gefiltert, bevor sie auf das Volume geschrieben werden. Dieser Prozess ähnelt dem Filtern von Dateien durch ein Antivirusprogramm, der Leistungsaufwand ist jedoch geringer.

### **Siehe auch**

[Auswirkungen von DPM auf die Leistung](#)

[Leistungsverwaltung](#)

## **Synchronisierung**

Bei der Synchronisierung überträgt DPM Daten vom geschützten Computer an den DPM-Server und wendet die Änderungen dann auf die Replikate der geschützten Dateien an.

Bei Dateivolumes oder Freigaben verfolgt der Schutz-Agent auf dem geschützten Computers die Änderungen an Blöcken. Dabei wird anhand des Volumefilters und des Änderungslogs, die Teil des Betriebssystems sind, festgestellt, ob geschützte Dateien geändert wurden. DPM verwendet den Volumefilter und das Änderungslog auch, um die Erstellung neuer Dateien sowie das Löschen oder Umbenennen geschützter Dateien zu verfolgen.

Für Anwendungsdaten werden Änderungen an Volumeblöcken, die zu Anwendungsdateien gehören, nach der Replikaterstellung vom Volumefilter verfolgt.

Wie Änderungen auf den DPM-Server übertragen werden, richtet sich nach der Anwendung und nach dem Synchronisierungstyp. Für geschützte Microsoft Exchange-Daten wird bei der Synchronisierung ein inkrementeller Volumeschattenkopie-Dienst (VSS)-Snapshot übertragen. Für geschützte Microsoft SQL Server-Daten wird bei der Synchronisierung eine Transaktionsprotokollsicherung übertragen.

DPM basiert darauf, dass durch die Synchronisierung Replikate mit den geschützten Daten aktualisiert werden. Jeder Synchronisierungsauftrag verwendet Netzwerkressourcen und kann aus diesem Grund die Netzwerkleistung beeinträchtigen.

Die Auswirkungen der Synchronisierung auf die Netzwerkleistung können durch Verwenden der Netzwerk-Bandbreitenbeschränkung und Komprimierung verringert werden. Weitere Informationen finden Sie unter [Verwenden der Netzwerk-Bandbreitenbeschränkung](#) und [Verwenden der Komprimierung über das Netzwerk](#).

## **Siehe auch**

[Auswirkungen von DPM auf die Leistung](#)

[Leistungsverwaltung](#)

## **Konsistenzprüfung**

Eine Konsistenzprüfung ist die Suche nach Inkonsistenzen zwischen einer geschützten Datenquelle und deren Replikat sowie die Korrektur dieser Inkonsistenzen.

Die Leistung des geschützten Computers, des DPM-Servers und des Netzwerks wird durch die Ausführung einer Konsistenzprüfung beeinträchtigt; dies wurde jedoch optimiert, da nur die Änderungen und Prüfsummen übertragen werden.

Die Auswirkungen einer Konsistenzprüfung auf das Netzwerk sind nach der erfolgreichen Erstellung eines Replikats deutlich geringer als bei der ersten Replikaterstellung. Wenn die erste Replikaterstellung unterbrochen wird oder nicht erfolgreich ist, kann die erste Konsistenzprüfung zu ähnlichen Beeinträchtigungen führen wie die Replikaterstellung.

Es wird empfohlen, Konsistenzprüfungen außerhalb der Hauptgeschäftszeiten durchzuführen.

DPM führt in den folgenden Fällen automatisch eine Konsistenzprüfung durch:

- Beim Ändern einer Schutzgruppe durch Ändern der Ausschlussliste
- Wenn eine tägliche Konsistenzprüfung geplant ist und das Replikat inkonsistent ist

## **Siehe auch**

[Auswirkungen von DPM auf die Leistung](#)

[Leistungsverwaltung](#)

## **Vollständige Schnellsicherung**

Eine vollständige Schnellsicherung ist ein Synchronisierungstyp, bei dem der Schutz-Agent einen Snapshot aller seit der vorigen vollständigen Schnellsicherung (bzw. für die erste vollständige Schnellsicherung seit der ersten Replikaterstellung) geänderten Blöcke überträgt und das Replikat entsprechend aktualisiert. Es wird davon ausgegangen, dass die Auswirkung einer vollständigen Schnellsicherung auf die Leistung sowie die Dauer des Vorgangs einer vollständigen Schnellsicherung geringer ist als bei einer vollständigen Sicherung, da DPM nur die seit der letzten vollständigen Schnellsicherung geänderten Blöcke überträgt.

## Siehe auch

[Auswirkungen von DPM auf die Leistung](#)  
[Leistungsverwaltung](#)

## Sicherung auf Band

Wenn DPM Daten vom Replikat auf Band sichert, entsteht kein Netzwerkverkehr, und somit gibt es auch keine Auswirkungen auf die Leistung des geschützten Computers.

Wenn DPM Daten vom geschützten Computer direkt auf Band sichert, wirkt sich dies auf die Datenträgerressourcen und die Leistung des geschützten Computers aus. Die Auswirkungen auf die Leistung sind beim Sichern von Dateidaten geringer als beim Sichern von Anwendungsdaten.

## Siehe auch

[Auswirkungen von DPM auf die Leistung](#)  
[Leistungsverwaltung](#)

## DPM-Prozesse

Auf dem DPM-Server können drei Prozesse die Leistung beeinträchtigen:

- **DPM-Schutz-Agent (MsDpmProtectionAgent.exe).** DPM-Aufträge wirken sich sowohl auf die Speicher- als auch auf die CPU-Auslastung durch den DPM-Schutz-Agent aus. Es ist normal, dass die CPU-Auslastung durch MsDpmProtectionAgent.exe während Konsistenzprüfungen ansteigt.
- **DPM-Dienst (MsDpm.exe).** Der DPM-Dienst wirkt sich sowohl auf die Speicher- als auch die CPU-Auslastung aus.
- **DPM-Verwaltungskonsole (eine Instanz von Mmc.exe).** Die DPM-Verwaltungskonsole kann für eine hohe Speicherauslastung ausschlaggebend sein. Sie können diese Konsole schließen, wenn sie gerade nicht verwendet wird.



### Hinweis

Es ist damit zu rechnen, dass die Speicherauslastung für die DPM-Instanz des SQL Server-Dienstes (Microsoft\$DPM\$Acct.exe) vergleichsweise hoch ist. Dies deutet nicht auf ein Problem hin. Der Dienst verwendet normalerweise eine große Menge an Arbeitsspeicher zum Zwischenspeichern, gibt diesen jedoch bei wenig freiem Arbeitsspeicher wieder frei.

## Siehe auch

[Auswirkungen von DPM auf die Leistung](#)  
[Leistungsverwaltung](#)

## DPM und Arbeitsspeicher

Wenn der von allen stattfindenden Prozessen genutzte Speicher die Menge des verfügbaren RAMs übersteigt, verschiebt das Betriebssystem Seiten (4-KB-Teile) von einer oder mehreren virtuellen Adressräumen auf die Festplatte des Computers, sodass der entsprechende RAM für andere Zwecke frei wird. Auf Microsoft Windows-Systemen werden diese Seiten in einer oder mehreren so genannten Auslagerungsdateien (pagefile.sys) im Stammverzeichnis einer Partition gespeichert.

DPM benötigt eine Größe der Auslagerungsdatei, die 0,2 Prozent der Gesamtgröße aller Wiederherstellungspunktvolumes beträgt, zusätzlich zur empfohlenen Größe (im Allgemeinen das 1,5-Fache des Computer RAMs). Wenn die Wiederherstellungspunktvolumes auf einem DPM-Server zum Beispiel insgesamt 3 TB groß sind, sollten Sie die Größe der Auslagerungsdatei um 6 GB erhöhen.

Informationen zum Ändern der Größe von Auslagerungsdateien finden Sie, in englischer Sprache, unter „[Change the size of the virtual memory paging pool](http://go.microsoft.com/fwlink/?LinkId=95116)“ (<http://go.microsoft.com/fwlink/?LinkId=95116>).

Auf x86 32-Bit-Betriebssystemen gibt es eine Volumeschattenkopie-Dienst (VSS)-Begrenzung für Nicht-Auslagerungsspeicher. Wenn Sie mehr als 10 TB Daten schützen, muss auf dem DPM-Server deshalb ein 64-Bit-Betriebssystem ausgeführt werden.

### Siehe auch

[Leistungsverwaltung](#)

## Leistungsindikatoren

Eine Methode zum Überwachen der Leistung von DPM-Servern bietet die Option „Leistung“ unter „Verwaltung“. Sie können festlegen, dass die überwachten Daten als Protokoll gespeichert werden. Sie können „Leistung“ außerdem so konfigurieren, dass Warnungen generiert werden. Informationen zum Erstellen und Konfigurieren von Leistungswarnungen finden Sie, in englischer Sprache, im Microsoft Knowledge Base-Artikel 324752, [How to create and configure performance alerts in Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=47881), (<http://go.microsoft.com/fwlink/?LinkId=47881>).



### Hinweis

Sie können mit dem DPM Management Pack für Microsoft Operations Manager 2005 (MOM) oder System Center Operations Manager 2007 von einem Operations Management-Verwaltungsserver aus Status, Zustand und Leistung von mehreren DPM-Servern zentral überwachen. Informationen zum Herunterladen des DPM Management Packs finden Sie im [Microsoft Management Pack and Product Connector Catalog](http://go.microsoft.com/fwlink/?LinkId=47215) (<http://go.microsoft.com/fwlink/?LinkId=47215>).

In der Tabelle **Leistungsindikatoren zur Überwachung von DPM** sind Indikatoren aufgeführt, die beim Überwachen der Leistung des DPM-Servers nützlich sind. Weitere Informationen zu bestimmten Leistungsindikatoren finden Sie in der Hilfe zu Leistungsprotokollen und Warnungen. Um das Leistungstool zu öffnen, klicken Sie auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie auf **Leistung**. Klicken Sie im Menü **Aktion** auf **Hilfe**.

#### Leistungsindikatoren zur Überwachung von DPM

Leistungsobjekt und - indikator	Beschreibung	Auf ein mögliches Problem hindeutender Wert	Mögliche Ursachen
Arbeitsspeicher: Verfügbare MB	Gibt den freien Arbeitsspeicher für Prozesse an, die auf dem angegebenen DPM-Server ausgeführt werden. Der Wert „Verfügbare MB“ stellt den gesamten Arbeitsspeicher dar, der für Standbylisten (zwischen- gespeicherte Listen), freie Listen und ausgelagerte Nulllisten reserviert ist.	< 50 MB Weist auf wenig freien Arbeitsspeicher auf dem DPM-Server hin.	<ul style="list-style-type: none"> <li>• Eine oder mehrere Anwendungen verwenden große Mengen an Arbeitsspeicher.</li> <li>• Mehrere DPM-Aufträge werden gleichzeitig ausgeführt.</li> <li>• Der DPM-Server verfügt nicht über genügend Arbeitsspeicher für die aktuelle DPM-Arbeitsauslastung.</li> </ul>



Leistungsobjekt und - indikator	Beschreibung	Auf ein mögliches Problem hindeutender Wert	Mögliche Ursachen
Prozessor: Prozessorzeit (%)	Gibt den prozentualen Anteil der Zeit an, die der Prozessor während des Samplingintervalls ausgelastet ist.	> 95 % für länger als 10 Minuten Weist auf eine sehr hohe CPU-Auslastung auf dem DPM-Server hin.	<ul style="list-style-type: none"> <li>• Mehrere DPM-Aufträge werden gleichzeitig ausgeführt. Synchronisierungsaufträge mit Konsistenzprüfung führen zu einer besonders hohen CPU-Auslastung.</li> <li>• Auf dem DPM-Server ist die Komprimierung über das Netzwerk aktiviert. Die Komprimierung über das Netzwerk ermöglicht einen höheren Datendurchsatz, ohne die Netzwerkleistung zu beeinträchtigen. Für dieses Verfahren müssen jedoch sowohl auf dem geschützten Computer als auch auf dem DPM-Server große Datenmengen verarbeitet werden.</li> <li>• Ein außer Kontrolle geratener Prozess erschöpft Systemressourcen.</li> <li>• Der DPM-Server verfügt nicht über genügend Verarbeitungskapazität für die aktuelle DPM-Arbeitsauslastung.</li> </ul>

Leistungsobjekt und - indikator	Beschreibung	Auf ein mögliches Problem hindeutender Wert	Mögliche Ursachen
Physikalischer Datenträger: Aktuelle Warteschlangenlänge (für alle Instanzen)	Gibt die Anzahl von Datenträgeranforderungen an, die aktuell ausstehen, und Anforderungen, die zurzeit verarbeitet werden.	> 80 Anforderungen für mehr als 6 Minuten Weist auf eine zu hohe Warteschlangenlänge von Datenträgern hin.	<ul style="list-style-type: none"> <li>• Mehrere gleichzeitig ausgeführte DPM-Aufträge fordern große Mengen an Datenträgerressourcen an.</li> <li>• Die Datenträgerleistung muss optimiert werden.</li> <li>• Die Datenträgerressourcen auf dem DPM-Server sind für die aktuelle DPM-Arbeitsauslastung nicht ausreichend.</li> </ul>

## Siehe auch

[Leistungsverwaltung](#)

## Verbessern der Leistung

Leistung wird durch Arbeitsauslastung und Kapazität bestimmt. Ein langsamer Computer kann eine ausreichende Leistung erbringen, wenn die Arbeitsauslastung gering ist. Im Gegensatz dazu kann die tatsächliche Leistung eines äußerst leistungsstarken Computers beeinträchtigt sein, wenn dieser mit einer übermäßigen Arbeitsauslastung konfrontiert wird. Bei Vorgängen zwischen zwei Computern in einem Netzwerk wird die Arbeitsauslastung, die effektiv bewältigt werden kann, durch die Komponente mit der niedrigsten Kapazität begrenzt. Bei dieser Komponente kann es sich um einen der Computer oder um die Netzwerkverbindung selbst handeln.

Im Allgemeinen können Sie die Leistung steigern, indem Sie Änderungen an Arbeitsauslastung, Kapazität oder beidem vornehmen.

## In diesem Abschnitt

[Ändern von Arbeitsauslastungen](#)

[Erhöhen der Kapazität](#)

## Siehe auch

[Leistungsverwaltung](#)

## Ändern von Arbeitsauslastungen

DPM bietet verschiedene Methoden, mit denen Sie die Schutzarbeitslasten ändern und die Leistung verbessern können. In der folgenden Tabelle sind die Methoden aufgeführt, mit denen die entsprechenden Auslastungen geändert werden können, sowie deren zu erwartende Auswirkungen.

### Methoden zum Ändern von Auslastungen beim Schutz von Daten

Methoden	Auswirkung
Netzwerk-Bandbreitenbeschränkung	Aufträge verwenden weniger Bandbreite, benötigen jedoch mehr Zeit
Komprimierung über das Netzwerk	Verringert die Größe der Datenübertragung, erhöht jedoch die CPU-Nutzung auf dem DPM-Server und den geschützten Computern
Staffeln von Startzeiten für die Synchronisierung	Gleicht die Auslastung von Synchronisierungsaufträgen zwischen Schutzgruppen aus
Planen von Konsistenzprüfungen außerhalb der Hauptgeschäftszeit	Verhindert, dass die reguläre geschäftliche Verwendung von geschützten Dateiservern durch DPM beeinträchtigt wird
Manuelles Erstellen von Replikaten	Beschleunigt unter Umständen die Replikaterstellung. Kein Leistungsaufwand auf dem geschützten Computer oder Netzwerkressourcen. Die erste Konsistenzprüfung beeinträchtigt jedoch die Leistung des geschützten Computers.

### In diesem Abschnitt

[Verwenden der Netzwerk-Bandbreitenbeschränkung](#)

[Verwenden der Komprimierung über das Netzwerk](#)

[Staffeln von Startzeiten für die Synchronisierung](#)

[Planen von Konsistenzprüfungen](#)

[Manuelles Erstellen von Replikaten](#)

### Siehe auch

[Erhöhen der Kapazität](#)

[Leistungsverwaltung](#)

## Verwenden der Netzwerk-Bandbreitenbeschränkung

Mithilfe der Netzwerk-Bandbreitenbeschränkung wird die von DPM zum Erstellen und Synchronisieren von Replikaten verwendete Netzwerkbandbreite begrenzt. Die Netzwerk-Bandbreitenbeschränkung dient dazu, anderen Anwendungen als DPM Netzwerkbandbreite zur Verfügung zu stellen.

Der Vorteil einer Verwendung der Netzwerk-Bandbreitenbeschränkung besteht darin, dass die von einem Synchronisierungsauftrag maximal verwendeten Netzwerkressourcen eingeschränkt werden können. Der Nachteil der Netzwerk-Bandbreitenbeschränkung besteht darin, dass der Zeitaufwand für die Fertigstellung von Synchronisierungsaufträgen erhöht werden kann.

Die Netzwerk-Bandbreitenbeschränkung wird für jeden geschützten Computer konfiguriert. Sie wird über einen absoluten Höchstwert von pro Sekunde zu übertragenden Daten angegeben.

### So aktivieren Sie die Netzwerk-Bandbreitenbeschränkung

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Agents**.
3. Wählen Sie im Bereich **Anzeige** einen Server aus.
4. Klicken Sie im Bereich **Aktionen** auf **Throttle computer** (Computer beschränken).
5. Klicken Sie auf **Enable network bandwidth usage** (Netzwerk-Bandbreitenbeschränkung aktivieren).

Sie können die Netzwerk-Bandbreitenbeschränkung separat für Geschäftszeiten und andere Zeiten konfigurieren, und Sie können die Geschäftszeiten für den geschützten Computer definieren. Geschäftszeiten und Nicht-Geschäftszeiten verwenden die Zeitzone des geschützten Computers.

Die Netzwerkbandbreite kann auch durch Gruppenrichtlinien eingeschränkt werden. Die Einschränkung reservierbarer Bandbreite durch Gruppenrichtlinien auf dem lokalen Computer legt die gemeinsame reservierbare Bandbreite aller Programme fest, die den Paketplaner verwenden, DPM eingeschlossen. Durch die DPM-Netzwerk-Bandbreitenbeschränkung wird die Netzwerkbandbreite festgelegt, die von DPM während der Replikaterstellung, Synchronisierung und Konsistenzprüfungen verwendet werden kann. Wenn die DPM-Bandbreitenbeschränkung allein oder zusammen mit Einschränkungen durch andere Programme die Einschränkung reservierbarer Bandbreite durch Gruppenrichtlinien überschreitet, wird die DPM-Bandbreitenbeschränkung unter Umständen nicht angewendet.

Wenn beispielsweise ein DPM-Computer mit einer Netzwerkverbindungsgeschwindigkeit von 1 Gbit/s durch Gruppenrichtlinien über eine Einschränkung reservierbarer Bandbreite von 20 % verfügt, werden von der Bandbreite für alle Programme, die den Paketplaner verwenden, 200 Mbit/s reserviert. Wenn in diesem Fall die DPM-Bandbreitennutzung auf maximal 150 Mbit/s und die Bandbreitennutzung durch Internetinformationsdienste (IIS – Internet Information Services) auf maximal 100 Mbit/s festgelegt wird, übersteigt die Summe der Bandbreitenbeschränkungen von DPM und IIS die durch die Gruppenrichtlinie vorgegebene Einschränkung reservierbarer Bandbreite, und der DPM-Höchstwert findet möglicherweise keine Anwendung.

Um dieses Problem zu beheben, verringern Sie in DPM die Einstellung für die maximale Netzwerk-Bandbreitennutzung.

#### **Siehe auch**

[Verbessern der Leistung](#)

[Ändern von Arbeitsauslastungen](#)

### **Verwenden der Komprimierung über das Netzwerk**

Durch Komprimierung wird die Größe übertragener Daten während der Replikaterstellung und Synchronisierung verringert und ein größerer Datendurchsatz bei geringeren Auswirkungen auf die Netzwerkleistung ermöglicht. Durch diese Option wird jedoch die CPU-Auslastung sowohl auf dem DPM-Server als auch auf den geschützten Computern erhöht. Der Umfang der Komprimierung und die Steigerung der Netzwerkleistung sind von der Arbeitsauslastung abhängig.

Die Komprimierung wird für geschützte Computer aktiviert und bei der Replikaterstellung, der Synchronisierung und bei Konsistenzprüfungen angewendet. Für Wiederherstellungsaufträge wird die Komprimierung ebenfalls verwendet.

#### **► So aktivieren Sie die Komprimierung über das Netzwerk**

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
2. Klicken Sie im Bereich **Aktionen** auf **Optimize performance** (Leistung optimieren).
3. Wählen Sie auf der Registerkarte **Netzwerk** die Option **Enable on-the-wire compression** (Komprimierung über das Netzwerk aktivieren).
4. Um die Änderungen anzuwenden, klicken Sie auf **OK**.

#### **Siehe auch**

[Verbessern der Leistung](#)

[Ändern von Arbeitsauslastungen](#)

### **Staffeln von Startzeiten für die Synchronisierung**

Sie können für Synchronisierungsaufträge einzelner Schutzgruppen eine Startzeit in Minuten nach der vollen Stunde angeben. Wenn Sie die Startzeiten staffeln, werden die Auswirkungen auf die Netzwerkleistung durch die Ausführung mehrerer großer Aufträge zum Schutz von Daten minimiert.

Um zu ermitteln, ob Sie die Startzeiten von Synchronisierungsaufträgen staffeln sollten, sammeln Sie in der DPM-Verwaltungskonsole zunächst Informationen zu geplanten Datenschutzaufträgen:

- Überprüfen Sie Aufträge im Aufgabenbereich **Überwachung** auf der Registerkarte **Aufträge**, die für Zeiten geplant sind, in denen auf dem DPM-Server lange Datenträgerwarteschlangen vorhanden sind.
- Überprüfen Sie im Aufgabenbereich **Schutz** Schutzgruppendetails, um die Größe und Häufigkeit von Schutzaufträgen zu ermitteln.

Durch das Versetzen der Synchronisierungsstartzeiten können Sie auch den sekundären Schutz eines anderen DPM-Servers optimieren. Als sekundärer Schutz wird es bezeichnet, wenn ein DPM-Server die Datenbank und die Replikate eines anderen DPM-Servers schützt, der primärer DPM-Server genannt wird. Sie können die Synchronisierung des primären DPM-Servers in Bezug zum sekundären DPM-Server versetzen, damit sie nach dem Synchronisieren der Datenquellen auf den primären DPM-Server erfolgt.

### ► So staffeln Sie Startzeiten für die Synchronisierung

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
2. Wählen Sie im Anzeigebereich eine Schutzgruppe aus.
3. Klicken Sie im Bereich **Aktionen** auf **Optimize performance** (Leistung optimieren).
4. Wählen Sie auf der Registerkarte **Netzwerk** im Feld **Offset <Zeit> start time by** (Startzeit <Zeit> verschieben um) die Stunden und Minuten, um die der Start des Synchronisierungsauftrags verschoben werden soll.

Der maximale zulässige Wert für die Verschiebung entspricht der Synchronisierungsfrequenz.

5. Um die Änderungen anzuwenden, klicken Sie auf **OK**.  
Das Ändern der Startzeiten verschiebt Wiederherstellungspunkte für Dateien um die entsprechende Zeitdauer.

Sie können zwischen zwei Synchronisierungsmodi wählen: in regelmäßigen Abständen oder direkt vor dem Erstellen eines Wiederherstellungspunkts.

Die Synchronisierung in regelmäßigen Intervallen verteilt die Arbeitsauslastung des Netzwerks über den Tag. Bei der Synchronisierung direkt vor einem Wiederherstellungspunkt ist der Netzwerkverkehr zum Zeitpunkt der Synchronisierung potenziell stärker, aber die Daten werden nicht den ganzen Tag über übertragen.

Wenn dem Unternehmen nur eine eingeschränkte Netzwerkbandbreite zwischen dem geschützten Computer und dem DPM-Server zur Verfügung steht, und wenn diese eingeschränkte Bandbreite auch für die normalen Geschäftsvorgänge genutzt wird, sollten Sie in Betracht ziehen, nur direkt vor einem Wiederherstellungspunkt zu synchronisieren und diesen Vorgang außerhalb der Geschäftszeiten zu planen.

Die Auswirkungen auf den Netzwerkverkehr und die Leistung sind zwar wichtig, Sie müssen jedoch auch bedenken, wie sich die Wahl des Synchronisierungsmodus auf die Möglichkeit der Datenwiederherstellung auswirkt. Wenn Sie nur einmal am Tag synchronisieren, können Sie im schlimmsten Fall Daten aus den letzten 24 Stunden verlieren. Wenn Sie jedoch einmal pro Stunde synchronisieren, verlieren Sie im schlimmsten Fall Daten aus der letzten Stunde.

## **Siehe auch**

[Verbessern der Leistung](#)

[Ändern von Arbeitsauslastungen](#)

## **Planen von Konsistenzprüfungen**

Da Konsistenzprüfungen sowohl die Leistung des DPM-Servers als auch des geschützten Computers beeinträchtigen, sollten Sie diese zu Zeiten planen, in denen eine verringerte Reaktionszeit des geschützten Computers die wenigsten Auswirkungen auf Geschäftsvorgänge hat und der wenigste Netzwerkverkehr zu erwarten ist.

Nachdem eine Schutzgruppe manuell erstellt wurde oder aufgrund eines Netzwerkausfalls, eines Überlaufs des Synchronisierungsprotokolls oder aus einem anderen Grund ein inkonsistentes Replikat vorhanden ist, müssen Sie eine manuelle Konsistenzprüfung durchführen. Anleitungen hierzu finden Sie, in englischer Sprache, unter [How to Synchronize a Replica](#) in der DPM-Hilfe (<http://go.microsoft.com/fwlink/?LinkId=102162>).

Sie können auch eine tägliche Konsistenzprüfung planen, um sicherzustellen, dass inkonsistente Replikate automatisch repariert werden.

In den Planungsoptionen können Sie eine Zeitdauer oder Zeitspanne konfigurieren, in der Konsistenzprüfungsaufträge ausgeführt werden. Sie können den Beginn der Konsistenzprüfung beispielsweise auf 20:00 Uhr festlegen, wenn die meisten Mitarbeiter des Unternehmens nicht mehr im Haus sind, und eine maximale Dauer von 10 Stunden angeben.

## **Siehe auch**

[Verbessern der Leistung](#)

[Ändern von Arbeitsauslastungen](#)

## **Manuelles Erstellen von Replikaten**

Beim Erstellen einer Schutzgruppe können Sie auswählen, ob Replikate manuell von Band oder anderen Wechselmedien erstellt werden, um so die Auslastung von Dateiservern und dem Netzwerk zu verringern.

Die automatische Replikaterstellung ist einfacher. Je nach Größe der geschützten Daten kann die manuelle Replikaterstellung jedoch schneller sein. Bei kleineren Datensets wird die automatische Erstellung empfohlen. Für große Datensets und langsame Netzwerke ist die manuelle Option wahrscheinlich die bessere Wahl.

Nachdem das Replikat erstellt wurde, müssen Sie eine Synchronisierung mit Konsistenzprüfung ausführen.

Eine Anleitung zum manuellen Erstellen eines Replikats finden Sie, in englischer Sprache, unter [How to Manually Create a Replica](#) in der DPM-Hilfe (<http://go.microsoft.com/fwlink/?LinkId=102160>).

### **Siehe auch**

[Verbessern der Leistung](#)

[Ändern von Arbeitsauslastungen](#)

## **Erhöhen der Kapazität**

Sie können die Leistung auch steigern, indem Sie die Kapazität des DPM-Servers durch Hardwareaktualisierungen erhöhen:

- Durch Hinzufügen von Datenträgern zum Speicherpool und Neuweisung der Replikate im Speicherpool kann die Warteschlangenlänge der Datenträger verringert werden.
- Die Verwendung von Stripesetvolumes kann den Datenträgerdurchsatz beim Umgang mit Datenträgerengpässen verbessern.
- Eine Erweiterung des Arbeitsspeichers ist eine vergleichsweise kostengünstige Aktualisierung, die zu einer spürbaren Verbesserung der Leistung führt, wenn der Server häufig über wenig freien Arbeitsspeicher verfügt.
- Durch Hinzufügen weiterer Prozessoren oder Aktualisieren auf schnellere Prozessoren können einige CPU-Probleme vermieden werden.

Berücksichtigen Sie außerdem die Datenschutzerfordernungen: Möglicherweise müssen Sie zusätzliche DPM-Server einsetzen, um die Arbeitsauslastung auszugleichen.

### **Siehe auch**

[Verbessern der Leistung](#)

[Leistungsverwaltung](#)

[Ändern von Arbeitsauslastungen](#)

## **Verwalten der DPM-Leistung in einem WAN**

Überlegungen hinsichtlich der Leistung sind eine ernstzunehmende Angelegenheit, wenn der DPM-Server und die entsprechenden geschützten Computer über langsame WAN-Links (Wide Area Network) miteinander verbunden sind. Das gilt insbesondere für Replikaterstellungen oder Konsistenzprüfungen, die viele Ressourcen benötigen. Beispielsweise würde es mindestens 120 Stunden dauern, ein Volume von 20 GB über einen Link mit einer Verbindungsgeschwindigkeit von 512 Kbit/s zu übertragen.

Bei dieser Netzwerkkonfiguration sollten Sie die Komprimierung für alle Schutzgruppen aktivieren. Es wird empfohlen, Replikate von Volumes, die größer sind als 5 GB, manuell zu erstellen.

### **Siehe auch**

[Leistungsverwaltung](#)



# Auswirkungen von Schutzgruppenänderungen auf Aufträge

Änderungen an der Konfiguration einer DPM-Schutzgruppe können dazu führen, dass einige aktive Aufträge abgebrochen werden. Eine Änderung kann sich auf Replikaterstellungsaufträge, auf Archivierungsaufträge oder auf beides auswirken. In der folgenden Tabelle sind die Aufträge aufgeführt, die in den einzelnen Kategorien abgebrochen werden.

## Auftragstypen

Replikataufträge	Archivierungsaufträge
<ul style="list-style-type: none"> <li>• Replikaterstellung</li> <li>• Konsistenzprüfung</li> <li>• Synchronisierung</li> <li>• Wiederherstellungspunkt auf Datenträger erstellen</li> <li>• Wiederherstellung vom Datenträger</li> </ul>	<ul style="list-style-type: none"> <li>• Wiederherstellungspunkt auf Band erstellen</li> <li>• Überprüfung von Daten auf Band</li> <li>• Daten auf Band kopieren</li> <li>• Sicherung auf Band</li> <li>• Wiederherstellen vom Band</li> </ul>

In der folgenden Tabelle sind die Auswirkungen von Schutzgruppenänderungen auf aktive Aufträge aufgelistet. Aufträge können für alle Mitglieder der Schutzgruppe abgebrochen werden („Schutzgruppe“), für alle Datenquellen auf dem geschützten Computer („geschützter Computer“) oder für alle geschützten Computer in derselben Zeitzone wie der Computer, der die Datenquellen in der geänderten Schutzgruppe hostet („Zeitzone“).

## Schutzgruppenänderungen und aktive Aufträge

Änderung an der Schutzgruppe	Abgebrochene Aufträge
Bandgestützten Schutz entfernen	Archivierungsaufträge für die Schutzgruppe
Datenträgergestützten Schutz hinzufügen	Archivierungsaufträge für die Schutzgruppe, falls bandgestützter Schutz konfiguriert wurde
Datenträgergestützten Schutz entfernen	Replikat- und Archivierungsaufträge für die Schutzgruppe
Datenquellen hinzufügen oder entfernen	Replikate für den geschützten Computer und Archivierungsaufträge für die Zeitzone
Geschützte Objekte ändern, einschließlich Ordnerausschlüsse	Replikat- und Archivierungsaufträge für den geschützten Computer und für die Zeitzone
Ausgeschlossene Dateitypen ändern	Replikat- und Archivierungsaufträge für die Schutzgruppe

<b>Änderung an der Schutzgruppe</b>	<b>Abgebrochene Aufträge</b>
Schutzgruppe löschen	Replikat- und Archivierungsaufträge für die Schutzgruppe
Bevorzugten Server für Exchange Server-Clusterdaten ändern	Replikat- und Archivierungsaufträge für den geschützten Computer und für die Zeitzone
Schutz eines bereitgestellten Volumens zu einem anderen Bereitstellungspunkt ändern	Replikat- und Archivierungsaufträge für den geschützten Computer und für die Zeitzone
Schutz beenden und Daten auf Band löschen	Archivierungsaufträge für die Zeitzone
Schutz beenden und Daten auf Datenträger löschen	Replikat- und Archivierungsaufträge für den geschützten Computer
Bandbibliothek ändern, die von der Schutzgruppe verwendet wird	Archivierungsaufträge für die Schutzgruppe, falls die Datenüberprüfung aktiviert ist
Auswahl der Banddatenübertragung ändern	Archivierungsaufträge für die Schutzgruppe
Anzahl der Bandkopien ändern	Archivierungsaufträge für die Schutzgruppe
Bandgestützten Schutz hinzufügen oder entfernen	Archivierungsaufträge für die Schutzgruppe
Datenüberprüfungseinstellungen für bandgestützten Schutz ändern	Archivierungsaufträge für die Schutzgruppe
Datenüberprüfungseinstellungen für datenträgergestützten Schutz ändern	Replikataufträge für die Schutzgruppe
Komprimierungseinstellungen für bandgestützten Schutz ändern	Archivierungsaufträge für die Schutzgruppe
Verschlüsselungseinstellungen für bandgestützten Schutz ändern	Archivierungsaufträge für die Schutzgruppe
Einstellung der Netzwerk-Bandbreitenbeschränkung für kurzfristigen bandgestützten Schutz ändern	Archivierungsaufträge für die Schutzgruppe
Einstellungen der Komprimierung, Verschlüsselung oder Netzwerk-Bandbreitenbeschränkung für datenträgergestützten Schutz ändern	Replikataufträge für die Schutzgruppe

## **Siehe auch**

[Leistungsverwaltung](#)

# Verwalten von Bandbibliotheken

---

In diesem Abschnitt wird die Verwaltung von Bandbibliotheken und eigenständigen Bandlaufwerken beschrieben, die an den System Center Data Protection Manager 2007 (DPM)-Server angeschlossen sind, darunter auch routinemäßige Wartungsarbeiten.

Informationen zur Bedienung, Wartung und Fehlerbehebung für die Hardware entnehmen Sie bitte der Dokumentation für das Bandlaufwerk.

## In diesem Abschnitt

[Aktualisieren von Bandbibliotheksinformationen](#)

[Neuzuweisen von Bandlaufwerken](#)

[Deaktivieren von Bandbibliotheken und Bandlaufwerken](#)

[Entfernen von Bandbibliotheken](#)

[Verwalten des Bandkatalogs](#)

[Reinigen von Bandlaufwerken](#)

[Verwalten von Bändern](#)

[Wiederherstellen von auf Band gesicherten Daten](#)

## Aktualisieren von Bandbibliotheksinformationen

Sie können Bandbibliotheksinformationen aktualisieren, indem Sie die Option **Neu einlesen** auf der Registerkarte **Bibliotheken** im Aufgabenbereich **Verwaltung** verwenden. Beim Vorgang „Neu einlesen“ werden die folgenden Aufgaben aufgeführt:

- Überprüfen, ob neue Bandbibliotheken und eigenständige Bandlaufwerke an den DPM-Server angeschlossen wurden
- Aktualisieren des Status aller an den DPM-Server angeschlossenen Bandbibliotheken und eigenständigen Bandlaufwerke

Das Neueinlesen kann mehrere Minuten dauern. Alle Bibliotheksaufträge, die während des Neueinlesens beginnen, werden in eine Warteschlange gestellt, bis das Neueinlesen abgeschlossen ist. Wenn ein Bibliotheksauftrag beim Start des Neueinlesens bereits ausgeführt wird, schlägt der Neueinlesen-Vorgang fehl.

Wenn beim Neueinlesen neue Bandbibliotheken oder eigenständige Bandlaufwerke erkannt werden, fügt DPM die Informationen der Registerkarte **Bibliotheken** hinzu.

Wenn Sie neue Bandbibliotheken oder neue Bandlaufwerke an den DPM-Server anschließen und diese beim Neueinlesen nicht erkannt werden, versuchen Sie, das Problem mit folgenden Maßnahmen zu beheben:

1. Stellen Sie sicher, dass die Bandbibliothek und die Laufwerke korrekt angeschlossen sind.
2. Stellen Sie bei SCSI-Verbindungen sicher, dass die logische Gerätenummer (logical unit number, LUN) für jedes Gerät eindeutig ist.

3. Stellen Sie sicher, dass im Geräte-Manager alle an den DPM-Server angeschlossenen Bandbibliotheken und eigenständigen Bandlaufwerke aufgelistet sind.
4. Stellen Sie sicher, dass für jedes Gerät die richtigen Treiber installiert sind.

Verwenden Sie die Funktion „Neu einlesen“ nur, wenn Änderungen an der Hardware vorgenommen wurden, um den Status aller an den DPM-Server angeschlossenen Bandbibliotheken und eigenständigen Bandlaufwerke zu aktualisieren.

## Neuzuweisen von Bandlaufwerken

Die Aktion **Neu einlesen** auf der Registerkarte **Bibliotheken** im Aufgabenbereich **Verwaltung** veranlasst DPM, die an den DPM-Server angeschlossenen Bandlaufwerke zu untersuchen und die auf der Registerkarte **Bibliotheken** angezeigten Informationen zu aktualisieren. Auf der Registerkarte **Bibliotheken** ist jedes eigenständige Laufwerk sowie jede Bandbibliothek mit ihren Laufwerken aufgeführt.

Wenn der physische Zustand eines Bandlaufwerks in der DPM-Verwaltungskonsole nicht korrekt angezeigt wird, müssen Sie die Bandlaufwerksinformationen neu zuweisen. Beispiele für falsche Anzeigen: Laufwerke aus einer Bandbibliothek werden als eigenständige Bandlaufwerke angezeigt, ein Laufwerk aus Bibliothek 1 wird als Teil von Bibliothek 2 angezeigt, ein eigenständiges Bandlaufwerk wird als Laufwerk in einer Bandbibliothek angezeigt.

### **Hinweis**

Wenn ein Bandlaufwerk nicht richtig zugewiesen ist, können Aufträge, die das falsch zugewiesene Bandlaufwerk verwenden, nicht richtig ausgeführt werden.

Um die Zuweisung der Bandlaufwerke zu korrigieren, müssen Sie eine Datei namens DPMLA.xml mit den korrekten Informationen erstellen und dann auf **Neu einlesen** klicken. Eine Vorlage für die Laufwerkneuzuweisung, LADriveRemappingTemplate.xml, wird bei der Installation von DPM auf dem DPM-Server gespeichert.

Um die Datei DPMLA.xml zu erstellen, öffnen Sie die Datei LADriveRemappingTemplate.xml aus dem Ordner Microsoft Data Protection Manager\DPM\Config in einem XML-Editor oder in Editor (Notepad), folgen Sie den Anleitungen in der Vorlagendatei, und speichern Sie die Datei als DPMLA.xml im Ordner Microsoft Data Protection Manager\DPM\Config.

### **Wichtig**

An der Vorlagendatei LADriveRemappingTemplate.xml sollten Sie keine Änderungen vornehmen, da spätere Updates von DPM diese Datei möglicherweise aktualisieren. Wenn Sie LADriveRemappingTemplate.xml ändern, können Updates für DPM die Vorlagendatei nicht ersetzen.

Nachstehend finden Sie ein Beispiel für den Inhalt einer DPMLA.xml-Datei, mit der ein Laufwerk, das als eigenständiges Bandlaufwerk angezeigt wird, einer Bibliothek im Laufwerkschacht 0 in der Bibliothek zugewiesen wird:

```
<?xml version="1.0" encoding="utf-16"?>
<LAConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.microsoft.com/2003/dls/LAConfig.xsd">
  <DriveReMapInfo IsManuallyMapped="true">
    <DriveLibraryAssociation>
      <Drive SerialNumber="HUL4B06579" SCSIPort="10" SCSIBus="23" SCISITargetId="80"
SCSILun="4" DriveBayIndex="0" />
      <Library SerialNumber="2B41146637" SCSIPort="6" SCSIBus="5" SCISITargetId="0"
SCSILun="1" />
    </DriveLibraryAssociation>
  </DriveReMapInfo>
</LAConfig>
```

## Deaktivieren von Bandbibliotheken und Bandlaufwerken

Sie können eine Bandbibliothek oder ein eigenständiges Bandlaufwerk in DPM vorübergehend deaktivieren, um Wartungsarbeiten oder Reparaturen vorzunehmen.

### So deaktivieren Sie eine Bandbibliothek oder ein eigenständiges Bandlaufwerk

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken**.
3. Wählen Sie im Bereich **Anzeige** die Bandbibliothek oder das eigenständige Bandlaufwerk aus, die bzw. das Sie entfernen möchten, und klicken Sie dann im Bereich **Aktionen** auf **Deaktivieren**.

Falls die Bandbibliothek oder das eigenständige Bandlaufwerk gerade von einem Auftrag verwendet wird, deaktiviert DPM das Gerät nicht, solange der Auftrag noch nicht abgeschlossen ist.

Wenn Sie das einzige Bandlaufwerk deaktivieren, das auf dem DPM-Server installiert ist, schlagen alle geplanten Aufträge, die für das Bandlaufwerk konfiguriert wurden, fehl.

### Siehe auch

[Entfernen von Bandbibliotheken](#)

## Entfernen von Bandbibliotheken

Wenn Sie Bandbibliotheken oder eigenständige Bandlaufwerke physisch trennen oder ein Laufwerk physisch aus einer Bibliothek entfernen, die einer Schutzgruppe zugeordnet ist, zeigt die DPM-Verwaltungskonsole die abgetrennte oder entfernte Bandbibliothek oder das eigenständige Bandlaufwerk als offline an.

Wenn Sie Bandbibliotheken oder eigenständige Bandlaufwerke trennen oder entfernen, die keiner Schutzgruppe zugeordnet sind, wird der Eintrag für die Bandbibliothek oder das eigenständige Bandlaufwerk aus der DPM-Verwaltungskonsole entfernt. Dies erfolgt entweder bei der täglichen Inventarisierung oder beim Neueinlesen, je nachdem, was zuerst ausgeführt wird.

Wenn Sie eine Bandbibliothek entfernen, die einer Schutzgruppe zugeordnet ist, und Sie die Bandbibliothek nicht wieder online bringen werden, sollten Sie die Schutzgruppe ändern und eine andere Bandbibliothek verwenden. Wenn alle Schutzgruppen, die der entfernten Bandbibliothek zugeordnet waren, einer anderen Bandbibliothek zugewiesen wurde, wird der Eintrag für die Bandbibliothek oder das eigenständige Bandlaufwerk aus der DPM-Verwaltungskonsole entfernt. Dies erfolgt entweder bei der täglichen Inventarisierung oder beim Neueinlesen, je nachdem, was zuerst ausgeführt wird.

### Siehe auch

[Deaktivieren von Bandbibliotheken und Bandlaufwerken](#)

## Verwalten des Bandkatalogs

DPM bewahrt die Metadaten für jedes Band, als *Bandkatalog* bezeichnet, in einer Datenbank. Sie können die Aufbewahrungseinstellungen für den Bandkatalog verwalten, um festzulegen, wann der Katalog *gekürzt* wird, d. h. wann Einträge aus dem Katalog entfernt werden.

DPM kürzt den Katalog automatisch, wenn der Aufbewahrungszeitraum für die Schutzgruppe abgelaufen ist. Sie können DPM jedoch auch anweisen, den Katalog für alle Schutzgruppen schon eher zu kürzen, um die Größe der Datenbank zu beschränken.

### ► So legen Sie Einstellungen für die Aufbewahrung des Bandkatalogs fest

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
2. Wählen Sie eine Schutzgruppe aus
3. Klicken Sie im Bereich **Aktionen** auf **Specify tape catalog retention** (Aufbewahrung des Bandkatalogs festlegen).
4. Wählen Sie **For** (Für) und legen Sie die Dauer fest. Um die Standardeinstellung für die Aufbewahrung zu verwenden, wählen Sie **For the duration of retention period specified for each protection group** (Für die Dauer des Aufbewahrungszeitraums der einzelnen Schutzgruppen).
5. Klicken Sie auf **OK**.

Im Dialogfeld **Tape Catalog Retention** (Bandkatalogaufbewahrung) wird auch die aktuelle Größe des Katalogs in der Datenbank angezeigt. Sie können den Schwellenwert, bei dessen Erreichen DPM eine Warnung zur Größe der Datenbank ausgibt, ändern.

## Reinigen von Bandlaufwerken

Wenn Sie ein eigenständiges Bandlaufwerk reinigen, laden Sie ein Reinigungsband und folgen Sie den Anleitungen des Hardwareherstellers. Wenn Sie ein Band in einer Bandbibliothek mit DPM reinigen, legen Sie fest, welches Band zum Reinigen verwendet wird, und starten Sie den Reinigungsauftrag. Beginnt der Strichcode auf einem Band mit „CLN“ (zum Beispiel CLN0000812), erkennt DPM das Band nach einer schnellen Inventarisierung als Reinigungsband; Sie brauchen kein Band als Reinigungsband anzugeben.

Wenn das Reinigungsband jedoch keinen Strichcode aufweist oder dieser nicht mit „CLN“ beginnt, müssen Sie das Band als Reinigungsband kennzeichnen und dann eine schnelle Inventarisierung ausführen.

Wenn Sie ein Reinigungsband ohne Strichcode oder mit einem Strichcode, der nicht mit „CLN“ beginnt, einer Bibliothek hinzufügen und eine ausführliche Inventarisierung ausführen, bevor Sie das Band als Reinigungsband kennzeichnen und eine schnelle Inventarisierung ausführen, wird ein Reinigungsauftrag gestartet, wenn DPM dieses Band bei der ausführlichen Inventarisierung bereitstellt.

Folgen Sie bei der Reinigung den Richtlinien des Bandgerätherstellers.

### So legen Sie das Reinigungsband fest

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken**.
3. Wählen Sie im Bereich **Anzeige** das Band aus, das zum Reinigen verwendet werden soll, und klicken Sie dann im Bereich **Aktionen** auf **Mark as cleaning tape** (Als Reinigungsband kennzeichnen).

### So reinigen Sie ein Bandlaufwerk

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken**.
3. Wählen Sie im Bereich **Anzeige** das zu reinigende Laufwerk aus, und klicken Sie dann im Bereich **Aktionen** auf **Clean drive** (Laufwerk reinigen).

### Hinweis

Wenn ein Reinigungsband online und als Reinigungsband gekennzeichnet ist, brauchen Sie nur den Reinigungsauftrag auszuführen.

## Verwalten von Bändern

Für ein eigenständiges Bandlaufwerk verwendet DPM dasselbe Band für die täglichen Sicherungen einer bestimmten Schutzgruppe, bis nicht mehr genügend Speicherplatz auf dem Band vorhanden ist.

Wenn ein Sicherungsauftrag mehr Speicherplatz benötigt als auf einem einzelnen Band verfügbar ist, wird der Auftrag gestartet, und DPM zeigt eine Warnung an, dass ein Auftrag auf ein Band wartet, wenn Sie das volle Band entfernen und ein leeres Band einlegen müssen.

DPM hängt keine Sicherungen aus anderen Schutzgruppen auf demselben Band an.

### In diesem Abschnitt

[Hinzufügen und Entfernen von Bändern](#)

[Identifizieren von Bändern](#)

[Importieren von Bändern](#)

[Anzeigen von Bandinhalten](#)

[Austauschen von ausgelagerten Bändern](#)

[Kopieren von Bändern](#)

[Inventarisieren von Bändern](#)

### Hinzufügen und Entfernen von Bändern

Falls die Bandbibliothek über einen Insert/Eject (IE)-Port verfügt, verwenden Sie die Aktionen **Add tape (IE port)** (Band hinzufügen (IE-Port)) und **Remove tape (IE port)** (Band entfernen (IE-Port)) auf der Registerkarte **Bibliothek** im Aufgabenbereich **Verwaltung**, um Bänder zu Bibliotheksschächten hinzuzufügen bzw. daraus zu entfernen.

Wenn das Bandlaufwerk nicht über einen IE-port verfügt, müssen Sie die Bibliothek auf der Registerkarte **Bibliothek** im Aufgabenbereich **Verwaltung** auswählen, auf **Unlock library door** (Bibliothekstür entsperren) klicken, das Band physisch hinzufügen oder entfernen, und dann auf **Lock library door** (Bibliothekstür sperren) klicken.

Wenn Sie Bänder zur Bandbibliothek hinzufügen bzw. daraus entfernen und dabei die Aktionen **Unlock door** (Tür entsperren) oder **Add tape** (Band hinzufügen) verwenden, inventarisiert DPM die Bibliothek automatisch. Wenn Sie Bänder zur Bandbibliothek hinzufügen bzw. daraus entfernen und dabei nicht die Aktionen **Unlock door** (Tür entsperren) oder **Add tape** (Band hinzufügen) verwenden, müssen Sie die Aktion **Inventory library** (Bibliothek inventarisieren) ausführen, um die Informationen in der DPM-Verwaltungskonsole zu aktualisieren.

Das Hinzufügen oder Entfernen eines Bandes zu einem bzw. aus einem eigenständigen Bandlaufwerk erfolgt manuell den Hardwareanweisungen entsprechend ohne die DPM-Verwaltungskonsole.



## Identifizieren von Bändern

DPM erkennt Bändern anhand der Bandbezeichnung. Bandbezeichnungen für Bänder, die für den langfristigen Schutz verwendet werden, werden beim Erstellen einer Schutzgruppe zugewiesen. DPM weist eine Standardbandbezeichnung im folgenden Format zu: **DPM - <Schutzgruppenname> - long-term tape <Nummer>**. Sie können diese Bezeichnung im Assistenten zum Erstellen neuer Schutzgruppe ändern.

Jedes Band verfügt über einen Kennzeichner (On Media Identifier, OMID), der sich am Anfang des Bandes befindet. DPM liest den Band-OMID, bevor ein Vorgang mit dem Band ausgeführt wird, um sicherzustellen, dass es sich um das richtige Band handelt.

Wenn Ihr Bandlaufwerk über ein Strichcodelesegerät verfügt, zeigt DPM den Strichcode der einzelnen Bänder in der DPM-Verwaltungskonsolle an. Beginnt der Strichcode eines Bandes mit „CLN“, zum Beispiel Strichcode CLN0000812, identifiziert DPM das Band nach einer schnellen Inventarisierung als Reinigungsband.

## Identifizieren unbekannter Bänder

Wenn ein Band, das Daten enthält, der Bandbibliothek hinzugefügt wird, und die Bandbezeichnung wird als „Unbekannt“ angezeigt, können Sie das Band mit DPM identifizieren.

Wenn DPM das Band erkennt, wird der Bandheader gelesen, und die Bandbezeichnung wird wie folgt aktualisiert:

- Ein vom DPM-Server erstelltes Band zeigt die zugewiesene Bandbezeichnung an.
- Ein von einem anderen DPM-Server erstelltes Band zeigt **Imported** (Importiert) als Bandbezeichnung an.
- Ein Band, das Inhalte enthält, die nicht von DPM erstellt wurde, wird mit der Bandbezeichnung **Unrecognized** (Nicht erkannt) angezeigt.
- Für ein Band mit widersprüchlichen Identifikationsinformationen, zum Beispiel Strichcode oder OMID, zeigt DPM **Suspect** (Zweifelhaft) als Bandbezeichnung an.

### So identifizieren Sie unerkannte Bänder

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**, und klicken Sie dann auf die Registerkarte **Bibliotheken**.
2. Erweitern Sie im Anzeigebereich die Bandbibliothek oder das eigenständige Bandlaufwerk, und wählen Sie das nicht erkannte Band aus.
3. Klicken Sie im Bereich **Aktionen** auf **Identify unknown tape** (Unbekanntes Band identifizieren).
4. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**.
5. Wählen Sie das nicht erkannte Band auf der Registerkarte **Bibliotheken** aus.
6. Klicken Sie im Bereich **Aktionen** auf **Identify unknown tape** (Unbekanntes Band identifizieren).

## Verwalten zweifelhafter Bänder

Ein *zweifelhaftes* Band ist ein Band mit widersprüchlichen Identifikationsinformationen. In den folgenden Fällen werden Bänder als zweifelhaft markiert:

- Zwei Bänder weisen denselben Strichcode aber unterschiedliche On-Media-Identifizierer (OMID) auf
- Zwei Bänder weisen denselben OMID aber unterschiedliche Strichcodes auf
- Zwei Bänder weisen denselben OMID auf, und eines der Bänder hat keinen Strichcode
- Es wird ein anderes Band als ein Reinigungsband zum Reinigen verwendet

DPM kann zweifelhafte Bänder nicht verwenden. Um den zweifelhaften Zustand des Bandes zu beheben, führen Sie die entsprechenden Schritte in der folgenden Tabelle aus.

Grund für den zweifelhaften Status	Lösung
Zwei Bänder weisen den gleichen Strichcode aber unterschiedliche OMIDs auf	Ändern Sie den Strichcode für eines der zweifelhaften Bänder. Nachdem Sie alle Probleme für alle zweifelhaften Bänder behoben haben, öffnen Sie eine Befehlszeile, und führen Sie das Skript <code>ResolveSuspectMedia.cmd</code> aus.
Zwei Bänder weisen denselben OMID aber unterschiedliche Strichcodes auf oder Zwei Bänder weisen denselben OMID auf, und eines der Bänder hat keinen Strichcode	<p>Dies weist darauf hin, dass eines der Bänder gültig ist, während das ungültige Band denselben OMID aufweist, was dazu führt, dass beide Bänder als zweifelhaft markiert werden.</p> <ol style="list-style-type: none"> <li>1. Entfernen Sie beide als zweifelhaft markierten Bänder aus der Bandbibliothek.</li> <li>2. Öffnen Sie ein Befehlszeilenfenster und führen Sie das Skript <code>ResolveSuspectMedia.cmd</code> aus. Ab diesem Zeitpunkt werden die zweifelhaften Bänder nicht mehr als <b>zweifelhaft</b> markiert.</li> <li>3. Legen Sie eines der Bänder in die Bibliothek ein.</li> <li>4. Klicken Sie im Aufgabenbereich Verwaltung auf der Registerkarte Bibliotheken auf <b>Inventory library</b> (Bibliothek inventarisieren).</li> </ol> <p>Wird das Band nach der Inventarisierung als <b>zweifelhaft</b> angezeigt, ist dies das ungültige Band und Sie sollten es auswerfen. Führen Sie das Skript <code>ResolveSuspectMedia.cmd</code> erneut aus, legen Sie das andere Band ein, und klicken Sie auf <b>Inventory library</b> (Bibliothek inventarisieren).</p> <p>Wird das Band nach der Inventarisierung nicht als <b>zweifelhaft</b> angezeigt, ist das andere Band ungültig.</p> <p>Nachdem Sie festgestellt haben, welches Band ungültig ist, verwenden Sie es nicht mehr mit diesem DPM-Server, ohne es zu löschen.</p>

Grund für den zweifelhaften Status	Lösung
Es wird ein anderes Band als ein Reinigungsband zum Reinigen verwendet	Öffnen Sie ein Befehlszeilenfenster, und führen Sie das Skript ResolveSuspectMedia.cmd aus. Markieren Sie dieses Band nicht mehr als Reinigungsband.
Der Strichcode eines Bandes wird geändert, nachdem der OMID geschrieben wurde.	Verwenden Sie wieder den ursprünglichen Strichcode, und führen Sie ResolveSuspectMedia.cmd aus.
Der OMID des Bandes wurde geändert, oder das Band wurde von einem anderen Programm als DPM gelöscht.	Versehen Sie das Band mit einem neuen Strichcode, und führen Sie ResolveSuspectMedia.cmd aus.

Sie können das Skript ResolveSuspectMedia.cmd von der folgenden Website herunterladen:  
<http://go.microsoft.com/fwlink/?LinkId=96738>.

## Importieren von Bändern

Ein *importiertes Band* enthält Inhalte, die von einem anderen DPM-Server erstellt wurden. Wenn Sie der Bandbibliothek ein importiertes Band hinzufügen, müssen Sie das Band neu katalogisieren, um den Inhalt des Bandes zu identifizieren.

Während der Katalogisierung liest DPM vom Band und fügt der Datenbank Informationen zu den auf dem Band enthaltenen Daten hinzu. Nach Abschluss der Katalogisierung können Sie Daten von dem Band wiederherstellen, indem Sie einen Wiederherstellungspunkt von den Daten auf dem Band auswählen.

### So importieren Sie Bänder

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken**, und wählen Sie das zu importierende Band aus.
3. Klicken Sie im Bereich **Aktionen** auf **Recatalog imported tape** (Importiertes Band neu katalogisieren).

## Anzeigen von Bandinhalten

Wenn Sie ein Band finden, das Sie nicht identifizieren können, und über die weitere Verwendung unsicher sind, können Sie den Inhalt anzeigen.

Wenn Sie den Inhalt anzeigen, können Sie die Daten, die sich auf dem Band befinden, kopieren, indem Sie im Dialogfeld mit den Bandinhalten auf **Kopieren** klicken. Die Verwendung der Option **Kopieren** ist hilfreich, wenn Sie die Daten nicht mit DPM vom Band wiederherstellen können, zum Beispiel, wenn Daten zwei Bänder umfassen, aber nur eines verfügbar ist.

### ► So zeigen Sie Bandinhalte an

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken** und wählen Sie das anzuzeigende Band aus.
3. Klicken Sie im Bereich **Aktionen** auf **View tape contents** (Bandinhalt anzeigen).

### ► So zeigen Sie die Bänder an, die einer Schutzgruppe zugeordnet sind

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
2. Klicken Sie im Bereich **Anzeige** auf eine Schutzgruppe.
3. Klicken Sie im Bereich **Aktionen** auf **View tape list** (Bandliste anzeigen).

## Austauschen von ausgelagerten Bändern

In der DPM-Verwaltungskonsole wird angezeigt, wenn ein Band in der Bibliothek entfernt und im Archiv gespeichert werden sollte, indem ein grünes Symbol in der Spalte **Offsite Ready** (Bereit für Auslagerung) angezeigt wird. Sie können alle Bänder, die bereit für die Auslagerung sind, auch im Bandverwaltungsbericht anzeigen. Im Bandverwaltungsbericht sind die Bänder aufgelistet, die in dem für den Bericht ausgewählten bevorstehenden Zeitraum für die Archivierung an einem externen Ort bereit sind.

Wenn die Daten auf dem Band abgelaufen sind, fügen Sie das Band wieder in die Bandbibliothek ein. Abgelaufene Bänder, die nicht wieder in die Bandbibliothek eingefügt werden, erscheinen im Bandverwaltungsbericht als „overdue“ (überfällig). Überfällige Bänder sind bereits in einem früheren Berichtszeitraum abgelaufen. Abgelaufene Bänder sollten zur erneuten Verwendung wieder in die Bandbibliothek eingegliedert werden.

## Kopieren von Bändern

Sie können mit DPM Daten vom Band auf einen Datenträger oder von einem Datenträger oder Band auf Band kopieren.

### ▶ So kopieren Sie Bandinhalte auf einen Datenträger

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken**, erweitern Sie die Bandbibliothek oder das eigenständige Bandlaufwerk, wählen Sie das zu kopierende Band aus, und klicken Sie auf **View tape contents** (Bandinhalt anzeigen).
3. Wählen Sie im Dialogfeld mit den Bandinhalten die zu kopierenden Daten aus, und klicken Sie auf **Kopieren**.
4. Geben Sie im Dialogfeld **Specify Alternate Recovery Destination** (Alternatives Wiederherstellungsziel festlegen) ein Ziel auf einem Server mit installiertem Schutz-Agent an, und klicken Sie auf **OK**.
5. Klicken Sie auf **Ja**, um den Kopiervorgang fortzusetzen.
6. Klicken Sie auf **OK**, um die Meldung zu schließen.

Im Aufgabenbereich **Überwachung** auf der Registerkarte **Aufträge** wird der Fortschritt des Kopierauftrags angezeigt.

### ▶ So kopieren Sie Daten von einem Datenträger oder Band auf Band

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Wählen Sie die Daten aus, die Sie auf Band kopieren möchten, und klicken Sie auf **Wiederherstellen**.  
Der Wiederherstellungsassistent wird geöffnet.
3. Auf der Seite **Review Recovery Selection** (Auswahl für die Wiederherstellung überprüfen) können Sie überprüfen, auf welchem Band bzw. auf welchen Bändern sich die Daten befinden. Klicken Sie zum Fortfahren auf **Weiter**.
4. Wählen Sie auf der Seite **Specify Recovery Type** (Wiederherstellungstyp wählen) die Option zum Kopieren auf Band, und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Specify Library** (Bibliothek festlegen) im Dialogfeld **Primary library** (Primäre Bibliothek) eine Bibliothek aus, die für die Wiederherstellung verwendet wird. **Copy library** (Kopiebibliothek) ist nur verfügbar, wenn der Auftrag nur mit der in **Primary library** ausgewählten Bandbibliothek nicht abgeschlossen werden kann.
  - Wenn die Daten von der Festplatte kopiert werden, kopiert die unter **Primary library** ausgewählte Bibliothek auf Band.
  - Wenn die Daten vom Band kopiert werden und die Bandbibliothek über mehrere Bandlaufwerke verfügt, liest die Bibliothek, die Sie unter **Primary library** (Primärbibliothek) ausgewählt haben, vom Quellband und kopiert die Daten auf ein anderes Band.

- Wenn die Daten vom Band kopiert werden und die Bandbibliothek nur über ein Bandlaufwerk verfügt, liest die Bibliothek, die Sie unter **Primary library** (Primärbibliothek) ausgewählt haben, vom Quellband, und die Bibliothek, die Sie unter **Copy library** (Kopiebibliothek) ausgewählt haben, kopiert die Daten auf Band.
6. Auf der Seite **Specify Recovery Options** (Wiederherstellungsoptionen festlegen) können Sie die E-Mail-Adressen angeben, an die nach Abschluss der Wiederherstellung eine Benachrichtigung gesendet wird. Klicken Sie zum Fortfahren auf **Weiter**.
  7. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen, und klicken Sie dann auf **Wiederherstellen**.

## Inventarisieren von Bändern

Die Inventarisierung dient dazu, neue Bänder zu identifizieren und bekannte Bänder zu erkennen.

Bei einer *schnellen Inventarisierung* werden die Strichcodes der einzelnen Bänder in der Bibliothek gelesen. DPM kann eine schnelle Inventarisierung ausführen, wenn die Bänder und die Bandbibliothek, in der sich die Bänder befinden, über Strichcodes verfügen.

Bei einer *ausführlichen Inventarisierung* werden die Headerbereiche der Bänder in der Bibliothek gelesen, um den On-Media-Identifizier (OMID) der einzelnen Bänder zu identifizieren. DPM muss eine ausführliche Inventarisierung ausführen, wenn ein Band keinen Strichcode aufweist oder wenn die Bandbibliothek nicht über ein Strichcodelesegerät verfügt.

Bei einer schnellen Inventarisierung wird jedes Band (mit oder ohne Strichcode) in einer Bibliothek erkannt. Um die Medien eindeutig zu identifizieren, ist jedoch eine ausführliche Inventarisierung erforderlich.



### Hinweis

Wenn Sie ein Reinigungsband ohne Strichcode oder mit einem Strichcode, der nicht mit „CLN“ beginnt, einer Bibliothek hinzufügen und eine ausführliche Inventarisierung ausführen, bevor Sie das Band als Reinigungsband kennzeichnen und eine schnelle Inventarisierung ausführen, wird ein Reinigungsauftrag gestartet, wenn DPM dieses Band bei der ausführlichen Inventarisierung bereitstellt.

### ► So inventarisieren Sie Bänder in einer Bibliothek

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsolle auf **Verwaltung**.
2. Klicken Sie auf die Registerkarte **Bibliotheken** und wählen Sie eine Bibliothek aus.
3. Klicken Sie im Bereich **Aktionen** auf **Inventarisieren**.
4. Wählen Sie im Dialogfeld **Inventory** (Inventarisieren) die Option **Fast inventory** (Schnelle Inventarisierung) oder **Detailed inventory** (Ausführliche Inventarisierung), und klicken Sie dann auf **Start**.

Die Option für die schnelle Inventarisierung ist deaktiviert, wenn das Band keinen Strichcode aufweist oder die Bandbibliothek nicht über ein Strichcodelesegerät verfügt.

# Wiederherstellen von auf Band gesicherten Daten

## Wiederherstellen von Daten von Bändern, die von einem anderen DPM-Server erstellt wurden

Es kann vorkommen, dass Sie Daten von Bändern, die von einem anderen DPM-Server erstellt wurden, wiederherstellen müssen, zum Beispiel wenn ein DPM-Server ausfällt und wichtige Informationen wiederhergestellt werden müssen, bevor der Server wiederhergestellt werden kann. In diesem Fall müssen Sie das Band physisch einem DPM-Server hinzufügen und dann die Aktion **Recatalog imported tape** (Importiertes Band neu katalogisieren) verwenden.

Während der Neukatalogisierung liest DPM vom Band und fügt der Datenbank Informationen zu den auf dem Band enthaltenen Daten hinzu. Nach Abschluss der Katalogisierung können Sie Daten von dem Band wiederherstellen, indem Sie einen Wiederherstellungspunkt von den Daten auf dem Band auswählen.

## Wiederherstellen von Daten, wenn ein Band eines Bandsets fehlt

Wenn geschützte Daten, zum Beispiel ein Volume oder eine SQL Server-Datenbank, mehrere Bänder umfassen, müssen alle Bänder aus dem Bandset verfügbar sein, damit DPM die Daten wiederherstellen kann. Fehlt ein Band aus dem Bandset, führen Sie die folgenden Schritte aus, um auf die übrigen Daten zuzugreifen:

1. Fügen Sie das Band der Bandbibliothek hinzu. Möglicherweise müssen Sie das Band neu katalogisieren.
2. Zeigen Sie den Inhalt des Bandes an.
3. Kopieren Sie den Inhalt des Bands an den gewünschten Speicherort.

Nachdem Sie den Inhalt der übrigen Bänder kopiert haben, können Sie die kopierten Daten wie gewünscht verwenden.

## Siehe auch

[Hinzufügen und Entfernen von Bändern](#)

[Importieren von Bändern](#)

[Anzeigen von Bandinhalten](#)

[Kopieren von Bändern](#)

# Wiederherstellung im Notfall

---

Microsoft System Center Data Protection Manager 2007 (DPM) gibt Ihnen die Möglichkeit, Dateien und Anwendungsdaten zu schützen und schnell und effizient wiederherzustellen, wenn die Originaldaten verloren gehen, beschädigt werden oder versehentlich gelöscht werden. Was aber geschieht, wenn das gesamte Datacenter mit allen wichtigen Servern teilweise oder vollständig zerstört wird? Oder wenn der DPM-Server, der die Daten schützt, beschädigt wird oder ausfällt?

Als *Notfall-Wiederherstellung* bezeichnet man das Wiederherstellen der Systeme und Daten nach einem teilweisen oder vollständigen Ausfall eines Computers aufgrund natürlicher oder technischer Ursachen. In diesem Abschnitt wird beschrieben, wie Sie sich auf die Wiederherstellung im Notfall vorbereiten und wie Sie geschützte Server und den DPM-Server nach einem Serverausfall wieder aufbauen, indem Sie eine Kombination der Funktionen von DPM und vom DPM-Hilfsprogramm für die Systemwiederherstellung verwenden.

Die Verfahren für die routinemäßige Wiederherstellung von Daten mit DPM sind in der DPM-Hilfe und in den Abschnitten zum Betrieb der einzelnen Servertypen aufgeführt.

## In diesem Abschnitt

[Vorbereiten auf die Notfall-Wiederherstellung](#)

[Wiederherstellung](#)

[Verwenden von Skripten vor und nach Sicherungen](#)

## Siehe auch

[Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird](#)

[Verwalten von geschützten virtuellen Servern](#)

## Vorbereiten auf die Notfall-Wiederherstellung

Ob Sie die Funktionen und Daten eines Computers nach dessen Beschädigung oder Ausfall wiederherstellen können, ist davon abhängig, welche Aktionen Sie vor diesem Notfall ergriffen haben.

Wenn Sie DPM für den routinemäßigen Schutz von Datei- und Anwendungsdaten verwenden und ansonsten keine weiteren Vorbereitungen für die Wiederherstellung im Notfall treffen, können Sie mit DPM die Daten wiederherstellen, nachdem ein geschützter Computer beschädigt wurde oder ausgefallen ist. Zunächst müssen Sie den Computer jedoch manuell wieder aufbauen, indem Sie das Betriebssystem, die Anwendungen und die Serverkonfiguration neu installieren.



Wenn der DPM-Server beschädigt wird oder ausfällt, müssen Sie den DPM-Server manuell wieder aufbauen und dann den Schutz neu konfigurieren. Festplattengestützte Wiederherstellungspunkte können nicht wiederhergestellt werden, Sie können jedoch vorhandene Bänder für die Datenwiederherstellung importieren. Weitere Informationen finden Sie, in englischer Sprache, unter [Importing Tapes](http://go.microsoft.com/fwlink/?LinkId=102163) (<http://go.microsoft.com/fwlink/?LinkId=102163>).

Wenn sowohl der geschützte Computer als auch der DPM-Server beschädigt werden oder ausfallen, können Sie die letzte Sicherung von importierten Bändern wiederherstellen, nachdem Sie die Computer wieder aufgebaut haben.

Wenn sowohl der geschützte Computer als auch der DPM-Server beschädigt werden oder ausfallen und Sie nur den kurzfristigen festplattengestützten Schutz verwendet haben, sind möglicherweise alle Ihre Daten verloren.

#### **Bereiten Sie sich mit den folgenden Methoden auf die Notfall-Wiederherstellung vor:**

1. **Sichern Sie den Systemstatus des geschützten Computers.** Sie können den Systemstatus von geschützten Computern in einer Schutzgruppe mit DPM sichern. Systemstatussicherungen ermöglichen Ihnen die Wiederherstellung der Computerkonfiguration, nachdem Sie das Betriebssystem und die Anwendungen neu installiert haben.
2. **Sichern Sie kritische Daten auf Festplatte und auf Band.** Zu einem durchdachten Plan für die Wiederherstellung im Notfall gehört die Speicherung kritischer Informationen außerhalb des Unternehmensstandorts, damit Sie auch im Fall einer Beschädigung oder Zerstörung des Firmengebäudes die Unternehmensdaten wiederherstellen können. Bänder sind weit verbreitete Medien für die ausgelagerte Speicherung.
3. **Fügen Sie einen zweiten DPM-Server hinzu.** Ein *sekundärer DPM-Server* dient zum Schutz und zur Wiederherstellung eines *primären DPM-Server*, welcher Datei- und Anwendungsdaten direkt schützt. Der sekundäre Server schützt die Datenbanken des primären DPM-Servers und die Replikate der Datenquellen, die auf dem primären DPM-Server gespeichert werden. Wenn der primäre DPM-Server ausfällt, können Sie die Datenbanken und Replikate auf dem wiederaufgebauten primären DPM-Server vom sekundären DPM-Server wiederherstellen. Sie können Daten direkt vom sekundären DPM-Server auf den geschützten Computern wiederherstellen, wenn der primäre DPM-Server nicht verfügbar ist. Der sekundäre DPM-Server kann auch Server schützen, bis der primäre DPM-Server wieder einsatzbereit ist.
4. **Sichern Sie DPM-Datenbanken auf Band.** Sie können einen DPM-Server verwenden, um dessen eigene Datenbanken in der Bandbibliothek zu speichern, oder Sie verwenden Software von einem Dritthersteller, um die Datenbanken auf Band oder anderen Wechselmedien zu speichern. Eine Sicherung der DPM-Datenbanken ermöglicht Ihnen die Konfiguration von Schutzgruppen wiederherzustellen, nachdem Sie DPM erneut installiert haben.



#### **Wichtig**

Das Hinzufügen eines sekundären DPM-Servers bietet von den oben aufgeführten Optionen den besten Schutz. Als Mindestmaßnahme wird die regelmäßige Sicherung der DPM-Datenbanken mit DPM oder einer Drittherstellersoftware dringend empfohlen.

## In diesem Abschnitt

[Bewährte Verfahren für die Notfall-Wiederherstellung](#)

[Sichern des Systemstatus der geschützten Computer](#)

[Sichern von DPM-Servern](#)

[Sichern für die Bare-Metal-Recovery](#)

## Siehe auch

[Wiederherstellung](#)

## Bewährte Verfahren für die Notfall-Wiederherstellung

Datensicherungen, sei es durch DPM oder Drittanbietersoftware, sind von der Integrität der geschützten Daten abhängig. Um das Risiko der Datenbeschädigung zu minimieren, wird die Einhaltung der folgenden Richtlinien empfohlen:

- Führen Sie regelmäßig Tools aus, die die Integrität von Anwendungen überprüfen, zum Beispiel DBCC in SQL Server.
- Überwachen Sie Ereignisprotokolle auf den geschützten Computern und auf dem DPM-Server, um Hardware- und Dateisystemfehler zu erkennen.
- Führen Sie regelmäßig Testwiederherstellungen der geschützten Daten aus.
- Führen Sie häufig Konsistenzprüfungen für wichtige Daten aus.
- Verwenden Sie einen sekundären DPM-Server, um zusätzlichen Schutz und Redundanz zu gewährleisten.

DPM führt die Prä-Sicherungs- und Post-Sicherungsskripts unter Verwendung des lokalen Systemkontos aus. Es hat sich bewährt, sicherzustellen, dass die Skripts nur für das Administratorkonto und das lokale Systemkonto Lese- und Schreibberechtigungen haben. Diese Berechtigungsstufe verhindert, dass unbefugte Benutzer die Skripts ändern.

Auf jedem geschützten Computer sollten Sie die Skriptdatei, ScriptingConfig.xml, unter \Programme\Microsoft DPM\DPM\Scripting, und alle Prä- und Post-Sicherungsskripts sichern.

## Siehe auch

[Sichern von DPM durch einen sekundären DPM-Server](#)

[Verwenden von Skripts vor und nach Sicherungen](#)

## **Sichern des Systemstatus der geschützten Computer**

Der Systemstatus ist eine Sammlung systemspezifischer Daten, die vom Betriebssystem gepflegt werden, die als eine Einheit gesichert werden muss. Es handelt sich nicht um eine Sicherung des gesamten Systems. Die Sicherung eines Computersystemstatus kann verwendet werden, wenn Sie den Computer in einen bekannten Zustand versetzen müssen, zum Beispiel nach einer Installation, die zu unerwünschten Ergebnissen führt.

DPM kann den Systemstatus für jeden Computer schützen, auf dem ein DPM-Schutz-Agent installiert ist, ausgenommen Computer, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird.

Der Systemstatus eines geschützten Computers kann einer Schutzgruppe hinzugefügt werden. DPM nutzt das Windows-Sicherungsdienstprogramm auf dem geschützten Computer, um den Systemstatus in einer Backupdatei (.bkf) zu sichern, die auf dem DPM-Medium gespeichert wird, das Sie für diese Schutzgruppe festgelegt haben (Festplatte, Band oder beides).

Da sich der Systemstatus eher selten ändert, ziehen Sie in Betracht, den Systemstatus in einer Schutzgruppe getrennt von den Datei- und Anwendungsdaten zu platzieren, damit Sie für jede Datenquelle den effizientesten Schutzzeitplan einrichten können.

### **Systemstatus von Mitgliedsservern und Desktops**

Wenn DPM den Systemstatus eines Mitgliedsservers oder Desktops sichert, werden die folgenden Komponenten geschützt:

- die Startdateien
- die COM+-Klassenregistrierungsdatenbank
- die Registry

### **Systemstatus von Domänencontrollern**

Wenn DPM den Systemstatus eines Domänencontrollers sichert, werden die folgenden Komponenten geschützt:

- Active Directory (NTDS)
- die Startdateien
- die COM+-Klassenregistrierungsdatenbank
- die Registry
- das Systemvolumen (SYSVOL)

Weitere Informationen zum Sichern und Wiederherstellen des Systemstatus eines Domänencontrollers finden Sie, in englischer Sprache, unter „[Introduction to Administering Active Directory Backup and Restore](http://go.microsoft.com/fwlink/?LinkId=90626)“ (<http://go.microsoft.com/fwlink/?LinkId=90626>).

### **Systemstatus von Servern, auf denen Zertifikatdienste ausgeführt werden**

Wenn DPM den Systemstatus eines Mitgliedsservers oder Domänencontrollers, auf dem Zertifikatdienste installiert sind, sichert, werden zusätzlich zu den Systemstatuskomponenten für den Mitgliedsserver oder Domänencontroller auch die Zertifikatdienste geschützt.

## Systemstatus von Clusterservern

Wenn DPM den Systemstatus eines Clusterservers sichert, werden zusätzlich zu den Systemstatuskomponenten der Mitgliedserver auch die Clusterservice-Metadaten geschützt.

## Ändern des Speicherorts der Sicherungsdatei

Die Sicherungsdatei des Systemstatus wird unter %Systemlaufwerk%\DPM\_SYSTEM\_STATE erstellt.

### ► So ändern Sie den Speicherort der Sicherungsdatei für den Systemstatus

1. Öffnen Sie auf dem geschützten Computer die Datei PSDatasourceConfig.xml in einem XML- oder Text-Editor. PSDatasourceConfig.xml befindet sich normalerweise unter *Installationspfad\Programme\Microsoft Data Protection Manager\DPM\Datasources*.
2. Ändern Sie den Wert von **<FilesToProtect>** von %Systemlaufwerk% zum gewünschten Speicherort.
3. Speichern Sie die Datei.
4. Führen Sie auf dem DPM-Server eine Konsistenzprüfung aus, wenn es eine Schutzgruppe gibt, die den Systemstatus des geschützten Computers aus Schritt 1 schützt.
5. Die Konsistenzprüfung schlägt fehl und gibt eine Warnung aus. Führen Sie die in der Warnung empfohlenen Aktionen wie folgt aus:
  - a. Klicken Sie in den Warnungsdetails auf den Link **Modify protection group** (Schutzgruppe ändern), und folgen Sie dem Assistenten.
  - b. Führen Sie eine Konsistenzprüfung durch.

## Sicherungsprotokolle für den Systemstatus

Die Protokolle für die Systemstatussicherung werden unter C:\Dokumente und Einstellungen\Default User\Anwendungsdaten\Microsoft\NTBackup gespeichert.

Protokolldateien erhalten den Namen NTBackup0.log, NTBackup1.log usw. Sie können diese Protokolle zur Unterstützung bei der Behebung von Problemen, die mit der Systemstatussicherung auftreten, anzeigen.

## Siehe auch

[Wiederherstellen von geschützten Computern](#)

## Sichern von DPM-Servern

Sie sollten die folgenden Komponenten auf einem DPM-Server schützen:

- Die DPM-Datenbank, die für die DPM-Wiederherstellung benötigt wird.
- Replikate. Replikate sind nicht erforderlich, wenn die Datenquellen auf Band geschützt werden, da Bänder zum Wiederherstellen der Daten auf den geschützten Computern und zum Erstellen der ersten Replikate auf einem neu aufgebauten DPM-Server verwendet werden können.
- Der Ordner \Programme\Microsoft DPM\DPM\Config. Dieser Ordner wird benötigt, um die Neuzuordnungsdatei des Bandlaufwerks, DPMLA.xml, zu schützen.

Ein DPM-Server kann seine eigene Datenbank auf Band sichern. Sie können die empfohlenen Komponenten eines DPM-Servers sichern, indem Sie einen sekundären DPM-Server oder Software von einem anderen Hersteller als Microsoft verwenden.

### In diesem Abschnitt

[Sichern von DPM durch einen sekundären DPM-Server](#)

[Sichern von DPM-Datenbanken auf Band](#)

[Sichern von DPM durch Software von Drittanbietern](#)

### Siehe auch

[Sichern für die Bare-Metal-Recovery](#)

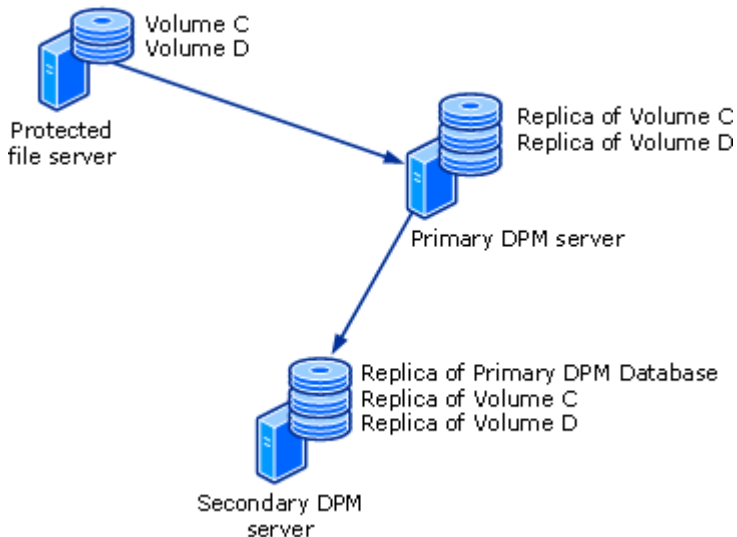
[Wiederherstellen von DPM-Servern](#)

## Sichern von DPM durch einen sekundären DPM-Server

Ein DPM-Server kann andere DPM-Server sichern. Ein DPM-Server, der Datenquellen direkt schützt, wird *primärer DPM-Server* genannt. Ein DPM-Server, der andere DPM-Server schützt, wird *sekundärer DPM-Server* genannt. Der sekundäre DPM-Server kann sowohl die Datenbanken als auch die Replikate auf dem primären DPM-Server schützen. Ein DPM-Server kann sowohl sekundären Schutz für einen anderen DPM-Server als auch primären Schutz für Datenquellen bieten.

In der folgenden Abbildung ist eine Beispieltopologie mit einem primären DPM-Server und einem sekundären DPM-Server dargestellt. In der Abbildung schützt der primäre DPM-Server die Volumes C und D des Dateiservers. Der sekundäre DPM-Server schützt die Datenbank des primären DPM-Servers und die Replikate der Volumes C und D des Dateiservers.

### Beispieltopologie für die DPM-Sicherung



Mit der in der Abbildung dargestellten Topologie können Sie die Daten vom primären DPM-Server wiederherstellen, wenn es auf dem Dateiserver zu Datenverlusten kommt. Wenn der primäre DPM-Server ausfällt, kann der sekundäre DPM-Server den Schutz des Dateiservers fortsetzen, während der primäre DPM-Server nicht verfügbar ist, und Sie können die Datenbanken und Replikate auf den wiederaufgebauten primären DPM-Server vom sekundären DPM-Server wiederherstellen.

Ein DPM-Server, der für den sekundären Schutz sorgt, kann nicht durch einen anderen DPM-Server geschützt werden. Beispiel: Server1 liefert primären Schutz für Computer1 und Server2 liefert sekundären Schutz für Server1. Server1 kann keinen sekundären Schutz für Server2 bieten.

Ein primärer DPM-Server kann nicht von mehreren sekundären DPM-Servern geschützt werden.

Überprüfen Sie Folgendes, bevor Sie den sekundären Schutz für Ihre Server konfigurieren:

- Die ausgewählten DPM-Server schützen keine weiteren DPM-Server.
- Der DPM-Server bzw. die ausgewählten DPM-Server werden nicht von anderen DPM-Servern geschützt.

#### **Wichtig**

Bevor Sie die Datenbank des primären DPM-Servers schützen können, müssen Sie den SQL Server VSS Writer-Dienst auf dem primären DPM-Server starten. Um den SQL Server VSS Writer-Dienst zu starten, klicken Sie in **Dienste** mit der rechten Maustaste auf **SQL Server VSS Writer**, und klicken Sie dann auf **Start**.

► **So sichern Sie einen primären DPM-Server mithilfe eines sekundären DPM-Servers**

1. Installieren Sie vom zweiten DPM-Server einen Schutz-Agent auf jedem primären DPM-Server, den Sie schützen möchten. Ein Neustart ist nicht erforderlich.
2. Um den Schutz der Replikate zu aktivieren, müssen Sie die Kommunikation zwischen dem sekundären DPM-Server und den vom primären DPM-Server geschützten Datenquellen sicherstellen. Wenn lokale Datenquellen auf einem Clusterknoten geschützt werden, sollten Sie zusätzlich zum Clusterschutz den Schutz für jeden Clusterknoten aktivieren. Führen Sie die folgenden Schritte aus, um die Kommunikation einzurichten:
  - a. Wählen Sie auf der Registerkarte **Agents** im Aufgabenbereich **Verwaltung** einen primären DPM-Server aus.
  - b. Klicken Sie im Bereich **Details**, neben **Protected servers enabled for protection** (Für den Schutz aktivierte geschützte Server) auf **Ändern**.
  - c. Wählen Sie im Dialogfeld **View details of protected computers** (Details zum geschützten Computer anzeigen) einen oder mehrere Computer aus, und klicken Sie auf **Enable protection** (Schutz aktivieren).
  - d. Geben Sie den Benutzernamen und das Kennwort für ein Domänenkonto ein, das auf allen Computern Mitglied der lokalen Administratorengruppe ist, und klicken Sie auf **OK**.  
Die Spalte **Protection enabled** (Schutz aktiviert) im Dialogfeld **View details of protected computers** (Details zum geschützten Computer anzeigen) ändert sich zu **Ja**.
3. Sie können eine vorhandene Schutzgruppe verwenden oder eine neue Schutzgruppe für die primären DPM-Server erstellen. Auf der Seite **Gruppenmitglieder auswählen** werden die folgenden Datenquellen für jeden DPM-Server, auf dem ein Schutz-Agent installiert ist, angezeigt:
  - die Datenbanken in der Instanz von SQL Server auf dem primären DPM-Server
  - alle Volumes auf dem primären DPM-Server
  - Alle Replikate auf dem primären DPM-Server, aufgelistet unter **Protected computers** (Geschützte Computer)

Jede dieser Datenquellen kann als Schutzgruppenmitglied ausgewählt werden. Sie sollten wenigstens die Datenbanken, den Ordner \Programme\Microsoft DPM\DPM\Config und den Ordner \Programme\Microsoft DPM\DPM\Scripting auswählen.

 **Hinweis**

Für den Schutz eines Replikats können Sie keine Dateierweiterungen ausschließen.

4. Auf der Seite **Select Data Protection Method** (Datenschutzmethode wählen) können Sie den kurzfristigen festplattengestützten Schutz, den langfristigen bandgestützten Schutz oder beides wählen. Der kurzfristige bandgestützte Schutz ist nicht verfügbar, wenn ein primärer DPM-Server Mitglied einer Schutzgruppe ist.
5. Schließen Sie den Assistenten zum Erstellen neuer Schutzgruppen ab, indem Sie die gewünschten Schutzoptionen wählen.



#### **Hinweis**

Wenn ein Replikat als Mitglied einer Schutzgruppe ausgewählt wurde und Sie den kurzfristigen festplattengestützten Schutz wählen, müssen Sie eine Synchronisierungsfrequenz angeben; die Option zum Synchronisieren vor einem Wiederherstellungspunkt ist nicht verfügbar. Es wird empfohlen, alle 24 Stunden eine Synchronisierung auszuführen.

#### **Siehe auch**

[Wechseln des Schutzes, wenn der primäre DPM-Server ausfällt](#)

[Wiederherstellen von geschützten Computern](#)

[Wiederherstellen von DPM-Servern](#)

### **Sichern von DPM-Datenbanken auf Band**

Ein DPM-Server kann seine eigene Datenbank schützen, indem die Datenbank auf Band gesichert wird. Es wird empfohlen, für die Sicherung der DPM-Serverdatenbank eine separate Schutzgruppe zu verwenden, mindestens zwei Kopien der Sicherungsbänder anzulegen und beide Sicherungsbänder an unterschiedlichen externen Standorten zu lagern. Sie sollten auch in Erwägung ziehen, den DPM-Statusbericht zu abonnieren, der das Band mit der neuesten Datenbanksicherung anzeigt.

#### **► So sichern Sie DPM-Datenbanken auf Band, indem Sie den primären DPM-Server mit einer lokalen SQL Server-Installation verwenden**

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
2. Klicken Sie im Bereich **Aktionen** auf **Schutzgruppe erstellen**.
3. Erweitern Sie auf der Seite **Select group members** (Gruppenmitglieder auswählen) das DPM-Serverelement, und wählen Sie dann **DPMDB**.
4. Wählen Sie auf der Seite **Select data protection method** (Datenschutzmethode wählen) die Option **I want short-term protection using tape** (Kurzfristiger Schutz auf Band), und klicken Sie auf **Weiter**.
5. Legen Sie die Optionen für die Richtlinien für den kurzfristigen Schutz fest. Für DPM-Datenbanken wird ein Aufbewahrungszeitraum von zwei Wochen empfohlen.
6. Schließen Sie den Assistenten zum Erstellen neuer Schutzgruppen mit den gewünschten Schutzoptionen ab.



## **Wichtig**

Wenn DPM eine Remoteinstallation von SQL Server verwendet, müssen Sie den DPM-Schutz-Agent auf dem SQL Server-basierten Remotecomputer installieren, bevor Sie die DPM-Datenbanken auf diesem Server schützen können.

### **So sichern Sie DPM-Datenbanken auf Band, indem Sie den primären DPM-Server mit einer Remoteinstallation von SQL Server verwenden**

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Schutz**.
2. Klicken Sie im Bereich **Aktionen** auf **Schutzgruppe erstellen**.
3. Erweitern Sie auf der Seite **Select group members** (Gruppenmitglieder auswählen) das SQL Server-Element für die Remoteinstallation von SQL Server, die DPM verwendet, und wählen Sie dann **DPM-Datenbank**.
4. Wählen Sie auf der Seite **Select data protection method** (Datenschutzmethode wählen) die Option **I want short-term protection using tape** (Kurzfristiger Schutz auf Band), und klicken Sie auf **Weiter**.
5. Legen Sie die Optionen für die Richtlinien für den kurzfristigen Schutz fest. Für DPM-Datenbanken wird ein Aufbewahrungszeitraum von zwei Wochen empfohlen.
6. Schließen Sie den Assistenten zum Erstellen neuer Schutzgruppen mit den gewünschten Schutzoptionen ab.

### **Siehe auch**

[Wiederherstellen von DPM-Datenbanken](#)

[Verwenden von Berichten](#)

## **Sichern von DPM durch Software von Drittanbietern**

Die Vorgehensweise beim Archivieren von Replikaten und Datenbanken mit Software von einem anderen Hersteller als Microsoft unterscheidet sich je nachdem, ob die verwendete Sicherungssoftware DPM und den Volumeschattenkopie-Dienst (VSS) unterstützt.

Sicherungssoftware, die DPM unterstützt, wurde speziell für die Verwendung mit DPM entwickelt und unterstützt den DPM VSS Writer-Dienst (DPM Writer).

Sicherungssoftware, die VSS unterstützt, verwendet VSS-fähige Dateisystemschatenkopien, aber arbeitet nicht mit dem DPM Writer-Dienst zusammen. Verglichen mit Software, die DPM unterstützt, hat diese Software zwei Nachteile :

- Archivierungs- und Wiederherstellungsvorgänge sind komplexer als mit Software, die DPM unterstützt.
- Software, die VSS unterstützt, organisiert die archivierten Replikate so, dass sie als direkt vom DPM-Server gesichert angezeigt werden. Durch diese Art der Organisation wird der Datenwiederherstellungsprozess weniger intuitiv.

Wenn Sie Sicherungssoftware verwenden, die VSS nicht unterstützt, können Sie nicht direkt von den Replikaten sichern. Stattdessen müssen Sie mit dem Tool DpmBackup

Sicherungsschattenkopien von den Replikaten und Datenbanksicherungen von den DPM-Datenbanken erstellen und anschließend mit der Sicherungssoftware die Sicherungsschattenkopien und Datenbanksicherungen auf Band sichern.

### **In diesem Abschnitt**

[Sichern mit Software von Drittanbietern, die DPM unterstützt](#)

[Sichern mit Software von Drittanbietern, die VSS unterstützt](#)

[Sichern mit Software von Drittanbietern, die VSS nicht unterstützt](#)

### **Siehe auch**

[Wiederherstellen von DPM-Datenbanken](#)

[Wiederherstellen von DPM-Replikaten](#)

### **Sichern mit Software von Drittanbietern, die DPM unterstützt**

Wenn Sie die DPM-Replikate und -Datenbanken mit Software von einem anderen Anbieter als Microsoft sichern, verwenden Sie am besten Sicherungssoftware, die speziell die Zusammenarbeit mit DPM entwickelt wurde. Die beiden wichtigsten Vorteile von Software, die DPM unterstützt:

- Die archivierten Daten werden so organisiert, dass der Wiederherstellungsprozess intuitiv und vergleichsweise einfach wird.
- Die Anzahl notwendiger Arbeitsschritte für Archivierungs- und Wiederherstellungsvorgänge wird minimiert.

Nachstehend finden Sie allgemeine Anleitungen für das Archivieren von DPM-Datenbanken und -Replikaten mit Sicherungssoftware, die DPM unterstützt. Informationen zur Verwendung der Sicherungssoftware finden Sie in der dazugehörigen Dokumentation.

#### **► So sichern Sie Datenbanken mit Sicherungssoftware, die DPM unterstützt**

1. Navigieren Sie in der Konsolenstruktur des Sicherungsprogramms zu \Programme\Microsoft DPM\DPM\, und wählen Sie den Ordner DPMDB aus. Der Dateiname der DPM-Datenbankdatei lautet DPMDB2007.mdf.
2. Wählen Sie die Medien, auf denen Sie die Datenbank sichern möchten.
3. Starten Sie den Sicherungsvorgang.

#### **► So sichern Sie Replikate mit Sicherungssoftware, die DPM unterstützt**

1. Erweitern Sie in der Konsolenstruktur des Sicherungsprogramms den DPM-Server.
2. Wählen Sie den Computer, dessen Replikate Sie archivieren möchten, oder die einzelnen geschützten Volumes.
3. Wählen Sie den Sicherungstyp aus.
4. Wählen Sie die Medien, auf denen Sie die Dateien sichern möchten.
5. Starten Sie den Sicherungsvorgang.

## Siehe auch

[Wiederherstellen von DPM-Datenbanken](#)

[Wiederherstellen von DPM-Replikaten](#)

### **Sichern mit Software von Drittanbietern, die VSS unterstützt**

Wenn Ihre Sicherungssoftware VSS unterstützt, können Sie Daten direkt von den Replikaten unter \Programme\Microsoft DPM\DPM\Volumes\Replica wiederherstellen; Sie müssen jedoch sicherstellen, dass die Software die Daten auf den Replikativolumes nicht ändert. Wenn Sie Daten zum Beispiel mit Windows Backup archivieren, verwenden Sie nur den Sicherungstyp „Kopie“.

Um sicherzustellen, dass die Sicherungstypen für diese Software nicht die Daten auf Replikativolumes ändern, informieren Sie sich in der Dokumentation zur Sicherungssoftware oder fragen Sie den Anbieter.

Sie müssen die Datenbank für die DPM-Datenbank und die Berichtdatenbank sichern. Nachstehend finden Sie allgemeine Anleitungen für das Archivieren von DPM-Datenbanken und -Replikaten mit Sicherungssoftware, die DPM nicht unterstützt, VSS jedoch unterstützt. Informationen zur Verwendung der Sicherungssoftware finden Sie in der dazugehörigen Dokumentation.

### **► So sichern Sie die Datenbanken mit Sicherungssoftware, die VSS unterstützt**

1. Navigieren Sie in der Konsolenstruktur des Sicherungsprogramms zu \Programme\Microsoft DPM\DPM\, und wählen Sie den Ordner DPMDB aus. Der Dateiname der DPM-Datenbankdatei lautet DPMDB2007.mdf.
2. Navigieren Sie in der Konsolenstruktur des Sicherungsprogramms zu \Programme\Microsoft DPM\Prerequisites\, und wählen Sie den Ordner Data aus. Der Dateiname der Berichtdatenbankdatei lautet standardmäßig ReportServer.mdf.
3. Wählen Sie die Medien, auf denen Sie die Datenbanken sichern möchten.
4. Starten Sie den Sicherungsvorgang.



#### **Hinweis**

Einige VSS-fähige Sicherungsprogramme haben keinen SQL VSS-Anforderer zum Sichern der SQL Server-Datenbanken über die VSS-Infrastruktur und MSDE VSS Writer. Verwenden Sie in diesem Fall das Verfahren zum Sichern von Datenbanken mit Sicherungssoftware, die VSS nicht unterstützt.

### **► So sichern Sie Replikate mit Sicherungssoftware, die VSS unterstützt**

1. Navigieren Sie in der Konsolenstruktur des Sicherungsprogramms zu \Programme\Microsoft DPM\DPM\Volumes\Replica\ auf dem DPM-Server.
2. Wählen Sie den Computer für die Replikate, die Sie archivieren möchten, oder die einzelnen geschützten Volumes.

3. Wählen Sie den Sicherungstyp aus.

 **Wichtig**

Informieren Sie sich in der Dokumentation Ihrer Sicherungssoftware oder wenden Sie sich an den Softwareanbieter, um festzustellen, welche Sicherungstypen die Replikatdaten nicht verändern.

4. Wählen Sie die Medien, auf denen Sie die Dateien sichern möchten.
5. Starten Sie den Sicherungsvorgang.

**Siehe auch**

[Wiederherstellen von DPM-Datenbanken](#)

[Wiederherstellen von DPM-Replikaten](#)

**Sichern mit Software von Drittanbietern, die VSS nicht unterstützt**

Wenn Ihre Sicherungssoftware weder VSS noch DPM unterstützt, müssen Sie mit dem Befehlszeilen-Tool DPMBackup Sicherungsschattenkopien von den Replikaten und Datenbanksicherungskopien von den DPM-Datenbanken erstellen und anschließend mit der Sicherungssoftware die Sicherungsschattenkopien und Datenbanksicherungskopien auf Band sichern.

Verwenden Sie DPMBackup, um Dateien für die Sicherung vorzubereiten, wenn Sie nicht VSS-fähige Sicherungssoftware verwenden. DPMBackup ist ein in DPM enthaltenes Befehlszeilen-Tool, mit dem die folgenden Aufgaben ausgeführt werden können:

- Erstellen und Bereitstellen von Sicherungsschattenkopien der einzelnen Replikatvolumes auf dem DPM-Server.
- Erstellen von Datenbanksicherungen der DPM-Datenbank (DPMDB.mdf).

DPM erstellt einen Bereitstellungspunkt der Sicherungsschattenkopien der Replikate auf dem DPM-Server im Ordner \Programme\Microsoft DPM\DPM\Volumes\ShadowCopy\. Die Sicherungsschattenkopien der Replikate werden vom Computer organisiert.

Sie können entweder Ihr Bandsicherungsprogramm oder Windows Scheduler konfigurieren, um DPMBackup auszuführen, bevor die Bandsicherung ausgeführt wird. Wie lange das Erstellen der Sicherungsschattenkopien und Datenbanksicherungen durch DPMBackup dauert, richtet sich nach Faktoren wie Datenträger- und Datenbankaktivität, als allgemeine Richtlinie können Sie aber davon ausgehen, dass das Tool ungefähr 2 Minuten pro Replikatvolume benötigt, um den Vorgang abzuschließen.

Das Programm DPMBackup.exe befindet sich auf dem DPM-Server im Ordner \Programme\Microsoft DPM\DPM\bin. Für DPMBackup werden Administratorberechtigungen auf dem DPM-Server benötigt.

Die von DPMBackup erstellten Schattenkopien sind schreibgeschützte Kopien der Replikatvolumes. Sie können wie ein Dateisystem archiviert werden. Da die Sicherungsschattenkopien der Replikate bereitgestellt sind, müssen Sie die Bandsicherungssoftware so konfigurieren, dass Bereitstellungspunkte durchlaufen werden.

Sie müssen die Datenbank für die DPM-Datenbank sichern. Nachstehend finden Sie allgemeine Anleitungen für das Archivieren von DPM-Datenbanken und -Replikaten mit Sicherungssoftware, die DPM und VSS nicht unterstützt. Informationen zur Verwendung der Sicherungssoftware finden Sie in der dazugehörigen Dokumentation.

#### ► **So sichern Sie die Datenbanken mit Sicherungssoftware, die DPM und VSS nicht unterstützt**

1. Führen Sie DPMBackup.exe aus.  
Sie können das Tool DPMBackup manuell ausführen oder das Sicherungsprogramm so konfigurieren, dass das Tool automatisch ausgeführt wird.
2. Navigieren Sie in der Konsolenstruktur des Sicherungsprogramms zu \Programme\Microsoft DPM\DPM\Volumes\ShadowCopy\Database Backups. Der Dateiname der DPM-Datenbanksicherung lautet DPMDB.bak. Der Dateiname der Berichtsdatenbanksicherung lautet standardmäßig ReportServer.bak.
3. Wählen Sie die Medien, auf denen Sie die Datenbanken sichern möchten.
4. Starten Sie den Sicherungsvorgang.

#### ► **So sichern Sie die Replikate mit Sicherungssoftware, die DPM und VSS nicht unterstützt**

1. Führen Sie DPMBackup.exe aus. Sie können das Tool DPMBackup manuell ausführen oder das Sicherungsprogramm so konfigurieren, dass das Tool automatisch ausgeführt wird.
2. Navigieren Sie in der Konsolenstruktur des Sicherungsprogramms zu \Programme\Microsoft DPM\DPM\Volumes\ShadowCopy\. Die Sicherungsschattenkopien der Replikate werden vom Computer organisiert.
3. Wählen Sie die Schattenkopien, die Sie sichern möchten.
4. Wählen Sie den Sicherungstyp aus.
5. Wählen Sie die Medien, auf denen Sie die Dateien sichern möchten.
6. Starten Sie den Sicherungsvorgang.

#### **Siehe auch**

[Wiederherstellen von DPM-Datenbanken](#)

[Wiederherstellen von DPM-Replikaten](#)

## **Sichern für die Bare-Metal-Recovery**

Das DPM System Recovery Tool (SRT) ist mit DPM gelieferte Software, die die Wiederherstellung für den DPM-Server und die von DPM geschützten Computer vereinfacht. *Bare-Metal-Recovery* bezeichnet eine Funktion, die beim Wiederherstellen eines Systems hilft, das sich nicht starten lässt. DPM SRT sichert das Systemvolumen und den Master-Boot-Record, indem das gesamte Volumen kopiert wird und VSS-Writer verwendet werden, um sicherzustellen, dass alle Anwendungen in einem konsistenten Zustand für die Kopie sind.

## **Brauchen Sie eine Bare-Metal-Recovery-Sicherung?**

Die Entscheidung, ob Sie Schutz für die Bare-Metal-Recovery mit DPM SRT hinzufügen, richtet sich nach Ihren Geschäftsansprüchen. Ihre Sicherungsanforderungen werden möglicherweise bereits durch festplattengestützten und bandgestützten Schutz mit DPM und einem sekundären DPM-Server erfüllt. Anwendungsserver und Dateiserver können wiederhergestellt werden, indem das Betriebssystem und die erforderlichen Anwendungen neu installiert werden, und die Daten werden anschließend aus DPM-Wiederherstellungspunkten wiederhergestellt. Ein DPM-Server kann wiederhergestellt werden, indem das Betriebssystem und die erforderlichen Anwendungen neu installiert werden, und die DPM-Datenbank wird anschließend vom sekundären DPM-Server wiederhergestellt.

Die Verwendung von DPM SRT zur Sicherung ausgewählter Server macht zusätzlichen Speicherplatz erforderlich. DPM SRT bietet jedoch die Möglichkeit, für instabile Systeme eine Reparatur oder ein Rollback auszuführen. Dies gilt sogar für Systeme, die nicht gestartet werden können. DPM SRT kann den Master-Boot-Code eines Laufwerks, die Partitionstabelle, die Volumeinformationen und die Logical Disk Management-Datenbank sichern, sodass Sie physisch beschädigte oder fehlerhafte Systemlaufwerke wiederaufbauen können.

### **In diesem Abschnitt**

[Installieren des DPM System Recovery Tools](#)

[Konfigurieren für die Bare-Metal-Recovery](#)

### **Siehe auch**

[Ausführen einer Bare-Metal-Recovery](#)

## **Installieren des DPM System Recovery Tools**

DPM System Recovery Tool (SRT) kann auf einem DPM-Server oder auf einem separaten Server installiert werden.

Wenn Sie DPM SRT installieren, müssen Sie den Speicherort für den primären Dateispeicher angeben, der die DPM SRT-Wiederherstellungspunkte enthalten wird. Es wird empfohlen, den primären Dateispeicher nicht auf demselben Datenträger zu speichern, auf dem das Betriebssystem und DPM SRT installiert sind. Sollte dies nicht möglich sein, können Sie den primären Dateispeicher auf einem separaten Volume auf demselben Datenträger platzieren.

Wie viel Speicher vom primären Dateispeicher benötigt wird, ist von der Größe der Systemdateien abhängig, die Sie schützen möchten. Angenommen, Sie schützen die Systemvolumen von drei Computern, auf denen Windows Server 2003 ausgeführt wird; die durchschnittliche Größe der Systemvolumen beträgt 6 GB. Der erforderliche Speicherplatz beträgt 6 GB für einen Computer, plus weitere 2 bis 5 Prozent des Speicherplatzes für jeden der anderen Computer. Diese Anforderungen sind in der Speichermethode von DPM SRT begründet, wobei nur eine Kopie einer Datei beliebigen Inhalts mit einer eindeutigen Inhaltsadresse gespeichert wird, die durch einen kryptografischen 128-Bit MD5-Algorithmus berechnet wird.

Weitere Informationen zum Berechnen der Größe des primären Dateispeichers sowie Anleitungen zur Verwendung des SRT-Installationsassistenten finden Sie, in englischer Sprache, in der DPM SRT-Hilfe (DPMSRT.chm auf der Produkt-DVD) unter den Themen „How Much Space Should I Allocate for the File Store?“ und „Installation“.

**Siehe auch**

[Konfigurieren für die Bare-Metal-Recovery](#)

## Konfigurieren für die Bare-Metal-Recovery

Sie können mit dem DPM System Recovery Tool (SRT) DPM-Server, Datei- und Anwendungsserver sowie Workstations für die Bare-Metal-Recovery sichern.

Um Sicherungen für die Bare-Metal-Recovery eines Servers zu konfigurieren, erstellen Sie einen *Wiederherstellungspunktzeitplan*. Der Wiederherstellungspunktzeitplan legt fest, welche Computer gesichert werden und an welchen Tagen und zu welcher Uhrzeit die Sicherung erfolgen soll. Außerdem gibt er das Wiederherstellungsset an. Dies ist die Definition der Volumeeinträge, die in den Wiederherstellungspunkt einbezogen werden sollen.

Das DPM System Recovery Tool definiert zwei Wiederherstellungssets:

- **Systemvolumes**, womit Systemdateien, Systemeinstellungen und Startdateien geschützt werden
- **Datenträgerlayout**, womit Datenträgerinformationen, darunter Master-Boot-Code, Partitionstabelle und Volumeinformationen, geschützt werden

Sie können in DPM SRT benutzerdefinierte Wiederherstellungssets erstellen.

Der DPM SRT-Agent muss auf jedem Computer installiert sein, der durch DPM SRT gesichert wird. Sie können die automatische Installation des Agents konfigurieren, wenn Sie den Wiederherstellungspunktzeitplan erstellen, oder Sie können den Agent manuell installieren.

Anleitungen zur Verwendung von DPM SRT finden Sie, in englischer Sprache, in der DPM SRT-Hilfe. Dies ist die Datei DPMSRT.chm auf der Produkt-DVD.

### Benutzerdefinierte Wiederherstellungssets für Front-End-Webserver

Um einen Front-End-Webserver für eine Microsoft Windows SharePoint Services-Farm zu sichern, wird empfohlen, die Systemvolumes- und Datenträgerlayout-Wiederherstellungssets auszuwählen und ein benutzerdefiniertes Wiederherstellungsset zu erstellen, das die folgenden Daten schützt:

- virtuelle Verzeichnisse, die sich nicht auf dem Systemvolume befinden
- die Registry
- die Internet-Informationdienste (IIS)-Metabase
- Windows SharePoint Services-Installationsdateien, falls sie sich nicht auf dem Systemvolume befinden

**Siehe auch**

[Ausführen einer Bare-Metal-Recovery](#)

# Wiederherstellung

In diesem Abschnitt finden Sie Anleitungen für die Wiederherstellung nach einem Notfall, zum Beispiel nach dem Ausfall eines DPM-Servers oder eines geschützten Servers. Anleitungen zur routinemäßigen Wiederherstellung von Daten mit DPM finden Sie, in englischer Sprache, in der DPM-Hilfe und in den Abschnitten zum Betrieb der einzelnen Servertypen.

## In diesem Abschnitt

[Wechseln des Schutzes, wenn der primäre DPM-Server ausfällt](#)

[Wiederherstellen von geschützten Computern](#)

[Wiederherstellen von DPM-Servern](#)

[Ausführen einer Bare-Metal-Recovery](#)

[Verwenden von DpmSync](#)

## Siehe auch

[Verwalten von geschützten Servern, auf denen Exchange ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen SQL Server ausgeführt wird](#)

[Verwalten von geschützten Servern, auf denen Windows SharePoint Services ausgeführt wird](#)

[Verwalten von geschützten virtuellen Servern](#)

## Wechseln des Schutzes, wenn der primäre DPM-Server ausfällt

Wenn der primäre DPM-Server ausfällt, kann der sekundäre DPM-Server den Schutz der geschützten Computer fortsetzen. Dazu müssen Sie den Schutz der geschützten Computer auf den sekundären DPM-Server wechseln. Sie müssen den Schutz der geschützten Computer auch auf den sekundären DPM-Server wechseln, um Daten direkt vom sekundären DPM-Server auf den geschützten Computern wiederherzustellen.

### **Wichtig**

Um Windows SharePoint Services-Daten direkt vom sekundären DPM-Server auf dem geschützten Computer wiederherzustellen, wenn Windows SharePoint Services eine Instanz von SQL Server auf einem anderen Computer verwendet, müssen Sie den Schutz für den Windows SharePoint Services-Server und für den SQL Server-basierten Computer auf den sekundären DPM-Server wechseln.



► **So wechseln Sie den Schutz zum sekundären DPM-Server**

- Führen Sie auf dem sekundären DPM-Server in der DPM Management Shell das Cmdlet `Start-ProductionServerSwitchProtection` aus.  
oder
- Führen Sie auf dem sekundären DPM-Server in einer Befehlszeile das Skript `SwitchProtection.ps1` unter Einhaltung der folgenden Syntax aus:

**SwitchProtection.ps1** *dpmservername Name* **psname** *Name* **protectiontype** *Typ*  
**username** *Benutzer* **password** *Kennwort* **domain** *Domäne*

**SwitchProtection.ps1-Parameter**

Parameter	Beschreibung
<b>-dpmservername</b>	Der Name des Servers, zu dem Sie den Schutz wechseln
<b>-psname</b>	Der Name des geschützten Computers, für den Sie den Schutz wechseln
<b>-protectiontype</b>	Der Schutztyp, den der Server bietet: primär oder sekundär
<b>-username</b> <b>-password</b>	Anmeldedaten für ein Konto mit Domänenadministratorberechtigung
<b>-domain</b>	Die Domäne, zu der der Schutzcomputer gehört

Wenn der primäre DPM-Server wieder verfügbar ist, wechseln Sie den Schutz zurück zum primären DPM-Server, damit dieser den Schutz der Computer fortsetzen kann. Sie müssen auch den Schutz auf dem zweiten DPM-Server wechseln, damit dieser den sekundären Schutz der vom primären DPM-Server geschützten Datenquellen wiederaufnimmt.

Wenn der sekundäre Schutz wiederaufgenommen wird, werden die Replike für die geschützte Datenquellen inaktiv. Sie müssen die Datenquellen wieder einer Schutzgruppe auf dem sekundären DPM-Server hinzufügen. Verwenden Sie dabei die Option zum automatischen Erstellen von Replikaten. Die Replike sind dann wieder aktiv.



**Hinweis**

Wenn die Replike nach Wiederaufnahme des sekundären Schutzes nicht inaktiv sind, führen Sie erneut `SwitchProtection.ps1` auf dem sekundären DPM-Server aus.

## Beispiel

Im folgenden Beispiel wechseln Sie den primären Schutz für Computer SQL1 zur Wiederherstellung oder zum fortgesetzten Schutz zum sekundären DPM-Server DPM2, indem Sie auf DPM2 den folgenden Befehl ausführen:

```
SwitchProtection.ps1 dpmservername dpm2 psname sql1 protectiontype primary  
username administrator password Password-1 domain dc990
```

Im folgenden Beispiel wird der primäre Schutz für Computer SQL1 zurück zum primären DPM-Server DPM1 gewechselt.

Zunächst führen Sie auf DPM1 den folgenden Befehl aus:

```
SwitchProtection.ps1 dpmservername dpm1 psname sql1 protectiontype primary  
username administrator password Password-1 domain dc990
```

Als Nächstes führen Sie auf DPM2 den folgenden Befehl aus:

```
SwitchProtection.ps1 dpmservername dpm2 psname sql1 protectiontype secondary  
username administrator password Password-1 domain dc990
```



### Hinweis

Das Skript SwitchProtection.ps1 finden Sie auf der Produkt-DVD für DPM 2007. Beim DPM-Setup wird das Skript unter dem Installationspfad in \Microsoft DPM\DPM\bin installiert.

## Siehe auch

[Sichern von DPM durch einen sekundären DPM-Server](#)

[Wiederherstellen von geschützten Computern](#)

## Wiederherstellen von geschützten Computern

In diesem Abschnitt finden Sie Anleitungen zum Wiederherstellen des Systemstatus auf einem geschützten Computer und zum Wiederherstellen von Daten auf einem geschützten Computer vom sekundären DPM-Server.

### Wiederherstellen des Systemstatus auf geschützten Computern

Sie können den Systemstatus auf geschützten Computer in einem *betriebsfähigen Zustand* wiederherstellen, was bedeutet, dass das Betriebssystem und erforderliche Anwendungen installiert sind.

Wenn Sie den Systemstatus eines Computers schützen, verwendet DPM das Dienstprogramm Windows Backup auf dem geschützten Computer, um den Systemstatus in einer Backupdatei (.bkf) zu sichern, die auf dem DPM-Medium gespeichert wird, das Sie für diese Schutzgruppe festgelegt haben (Festplatte, Band oder beides).

Die Wiederherstellung des Systemstatus erfolgt in zwei Phasen:

1. Stellen Sie die .bkf-Datei mit dem dem DPM-Wiederherstellungsassistenten auf dem geschützten Computer wieder her.
2. Stellen Sie den Systemstatus auf dem geschützten Computer mit Backup aus der .bkf-Datei wieder her.

► **So stellen Sie die .bkf-Datei mit dem Systemstatus wieder her**

1. Klicken Sie in der Navigationsleiste der DPM-Verwaltungskonsole auf **Wiederherstellung**.
2. Suchen Sie nach dem geschützten Computer, und wählen Sie im Ergebnisfenster die Daten aus.
3. Verfügbare Wiederherstellungspunkte werden im Kalender des Abschnitts mit den Wiederherstellungspunkten in Fettschrift angezeigt. Wählen Sie das Datum für den Wiederherstellungspunkt, den Sie wiederherstellen möchten.
4. Klicken Sie im Bereich **Recoverable item** (Wiederherstellbares Element) auf die .bkf-Datei, die wiederhergestellt werden soll.
5. Klicken Sie im Bereich **Aktionen** auf **Wiederherstellen**. DPM startet den Wiederherstellungsassistenten.
6. Überprüfen Sie die Auswahl für die Wiederherstellung, und klicken Sie auf **Weiter**.
7. Legen Sie fest, die .bkf-Datei an einem anderen Speicherort auf dem geschützten Computer wiederherzustellen.
8. Klicken Sie auf **Weiter**.
9. Geben Sie die Wiederherstellungsoptionen an:
  - **Wiederherstellungsverhalten für vorhandene Dateiversionen**. Wählen Sie **Kopie erstellen**, **Überspringen** oder **Überschreiben**.
  - **Sicherheit wiederherstellen**. Wählen Sie **Inherit security settings of target when overwriting or of parent folder when creating copy** (Sicherheitseinstellungen des Ziels übernehmen (beim Überschreiben) oder des übergeordneten Ordners (beim Kopieren) oder **Apply the security settings of the recovery point version** (Sicherheitseinstellungen der Wiederherstellungspunktversion anwenden).
  - **Throttling** (Beschränkung). Klicken Sie auf **Ändern**, um die Beschränkung zu aktivieren.
  - **Benachrichtigung**. Klicken Sie auf **Send an e-mail when the recovery completes** (Nach Abschluss der Wiederherstellung E-Mail senden), und geben Sie die Empfänger der Benachrichtigung an. Trennen Sie die E-Mail-Adressen durch Kommas.
10. Klicken Sie auf **Weiter**.

11. Überprüfen Sie die Wiederherstellungseinstellungen, und klicken Sie auf **Wiederherstellen**.

Synchronisierungsaufträge für das ausgewählte Wiederherstellungselement werden abgebrochen, während die Wiederherstellung ausgeführt wird.

#### **So stellen Sie den Systemstatus aus der .bkf-Datei wieder her**

1. Klicken Sie auf dem Computer, auf dem Sie die bkf-Datei für den Systemstatus wiederherstellen möchten, auf **Start**, klicken Sie auf **Ausführen**, geben Sie **ntbackup** ein, und klicken Sie dann auf **OK**.
2. Wenn der Assistent zum Sichern oder Wiederherstellen angezeigt wird, klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Backup or Restore** (Sichern oder Wiederherstellen) auf **Restore files and settings** (Dateien und Einstellungen wiederherstellen), und klicken Sie auf **Weiter**.
4. Klicken Sie auf der Seite **What to Restore** (Wiederherzustellende Elemente) auf die Elemente, um ihren Inhalt einzublenden. Suchen Sie die .bkf-Datei, die Sie mit DPM wiederhergestellt haben, wählen Sie sie aus, und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite **Completing the Backup or Restore Wizard** (Sicherungs- oder Wiederherstellungsassistent abschließen) auf **Erweitert**, falls Sie erweiterte Wiederherstellungsoptionen ändern möchten, zum Beispiel Sicherheitseinstellungen und Abzweigungspunktdateien. Wenn Sie die gewünschten erweiterten Wiederherstellungsoptionen ausgewählt haben, klicken Sie auf **OK**. Überprüfen Sie, ob alle Einstellungen korrekt sind, und klicken Sie auf **Fertig stellen**.

### **Geschützten Computer von einem sekundären DPM-Server wiederherstellen**

Wenn der primäre DPM-Server nicht verfügbar ist, können Sie Daten für geschützte Computer vom sekundären DPM-Server wiederherstellen. Um Daten vom sekundären DPM-Server an einem neuen Speicherort wiederherzustellen, verwenden Sie den Wiederherstellungsassistenten in der DPM-Verwaltungskonsole auf dem sekundären DPM-Server. Es sind keine zusätzlichen Schritte erforderlich. Wenn Sie die Daten vom sekundären DPM-Server am ursprünglichen Speicherort wiederherstellen möchten, müssen Sie zunächst den Schutz zum sekundären DPM-Server wechseln.

► **So stellen Sie Daten vom sekundären DPM-Server am ursprünglichen Speicherort auf einem geschützten Computer wieder her**

1. Wechseln Sie den Schutz des geschützten Computers zum sekundären DPM-Server, indem Sie das Cmdlet Start-SwitchProductionServer oder das Skript SwitchProtection.ps1 verwenden. Anleitungen zum Wechseln des Schutzes finden Sie unter [Wechseln des Schutzes, wenn der primäre DPM-Server ausfällt](#).
2. Verwenden Sie die DPM-Verwaltungskonsole auf dem sekundären DPM-Server, um die Daten am ursprünglichen Speicherort wiederherzustellen.

**Siehe auch**

[Sichern des Systemstatus der geschützten Computer](#)

[Sichern von DPM durch einen sekundären DPM-Server](#)

**Wiederherstellen von DPM-Servern**

Wenn der Zugriff auf den Server nicht möglich ist, richten Sie einen Server ein, indem Sie entweder mit dem DPM System Recovery Tool (SRT) das DPM-Serverimage wiederherstellen oder indem Sie das Betriebssystem und die Anwendungen einschließlich DPM neu installieren und dann die DPM-Datenbanken und Replikate wiederherstellen.

Wenn Sie einen primären DPM-Server wiederherstellen, müssen Sie den Schutz für die Computer, die zuvor vom DPM-Server geschützt wurden, wiederherstellen.

Weitere Informationen zum Wiederherstellen eines DPM-Servers mit DPM SRT finden Sie, in englischer Sprache, unter „Bare Metal Recovery“ in der DPM SRT-Hilfe.

**In diesem Abschnitt**

[Wiederherstellen von DPM-Datenbanken](#)

[Wiederherstellen von DPM-Replikaten](#)

[Erneutes Einrichten des Schutzes nach dem Wiederherstellen des primären DPM-Servers](#)

**Siehe auch**

[Verwenden von DpmSync](#)

## Wiederherstellen von DPM-Datenbanken

Wenn Sie die DPM-Datenbankdateien wiederherstellen, vergewissern Sie sich, dass der Speicherort auf dem DPM-Computer, auf dem Sie die Dateien wiederherstellen, sicher ist.

### ► So stellen Sie die DPM-Datenbank wieder her, wenn sie beschädigt ist

1. Deinstallieren Sie DPM unter Beibehaltung der datenträgergestützten Replikate.
2. Löschen Sie die DPM-Datenbank.
3. Installieren Sie eine neue Instanz des DPM-Servers.
4. Importieren Sie die letzte DPM-Bandsicherung und stellen Sie die Datenbank an einem anderen Speicherort wieder her, oder stellen Sie die Datenbank als Datei vom sekundären DPM-Server wieder her.
5. Führen Sie **DPMSync dbrestore dbloc Speicherort** aus.
6. Führen Sie **DPMSync sync** aus.

DPMSync nimmt den DPM-Dienst offline und fügt die gesicherte Datenbank SQL Server hinzu.

### Siehe auch

[Verwenden von DpmSync](#)

## Wiederherstellen von DPM-Replikaten

Um ein DPM-Replikat wiederherzustellen, müssen Sie zunächst DpmSync ausführen, um es neu zuzuweisen. DpmSync markiert das Replikat als ausstehende manuelle Replikaterstellung. Sie können das Replikat nur wiederherstellen, wenn sein Status in der DPM-Verwaltungskonsole als ausstehende manuelle Replikaterstellung angegeben ist. Wenn eine Replikatwiederherstellung fehlschlägt, wird der Replikatstatus als inkonsistent angezeigt, wodurch wiederholte Wiederherstellungsversuche verhindert werden.

Wenn eine Replikatwiederherstellung fehlschlägt, müssen Sie den Schutz der Datenquelle mit der Option zum Löschen des Replikats beenden, die Datenquelle erneut einer Schutzgruppe zuweisen, wobei Sie die Option zur manuellen Replikaterstellung wählen, und dann erneut versuchen, das Replikat wiederherzustellen.

Wenn die Wiederherstellung fehlschlägt, sind erneute Wiederherstellungsversuche zwecklos, da das Replikat jetzt als ungültig markiert ist und nicht den Status zum manuellen Laden aufweist.

► **So stellen Sie Replikate wieder her, nachdem die DPM-Datenbank wiederhergestellt wurde**

1. Führen Sie **DpmSync -reallocateReplica** aus. Mit diesem Befehl werden fehlende Replikate neu zugewiesen und erhalten den Status der ausstehenden manuellen Replikaterstellung. Anleitungen finden Sie unter [Verwenden von DpmSync](#).
2. Erstellen Sie das Replikat manuell vom sekundären DPM-Server oder von einer Bandsicherung der Datenquelle, die dem Replikat entspricht.
  - Wenn Sie einen sekundären DPM-Server verwenden, ist die Option **Restore to replica** (In Replikat wiederherstellen) im Aufgabenbereich **Wiederherstellung** verfügbar.
  - Wenn Sie Bandsicherungen verwenden, verwenden Sie DPM Management Shell mit der Option **RestoreToReplica** (In Replikat wiederherstellen).
3. Führen Sie eine Konsistenzprüfung aus, um den Schutz fortzusetzen.

**Siehe auch**

[Sichern von DPM-Servern](#)

## **Erneutes Einrichten des Schutzes nach dem Wiederherstellen des primären DPM-Servers**

Nachdem Sie einen primären DPM-Server wiederhergestellt haben, müssen Sie den Schutz für die Computer, die vom DPM-Server geschützt wurden, erneut einrichten. Führen Sie die folgenden Schritte auf allen Computern aus, die vom primären DPM-Server geschützt wurden.

► **So richten Sie den Schutz nach dem Wiederaufbau des primären DPM-Servers wieder ein**

1. Führen Sie auf dem geschützten Computer in einer Befehlszeile den folgenden Befehl aus:  
**Setdpmserver.exe <Name des primären DPM-Servers>**
2. Öffnen Sie die Computerverwaltung, und führen Sie die folgenden Schritte aus:
  - a. Wählen Sie **Lokale Benutzer und Gruppen**.
  - b. Überprüfen Sie, dass der primäre DPM-Server mit dem Format *Domäne/Name* Mitglied der folgenden Gruppen ist:  
Distribute COM Users  
DPMRADCOMTrustedMachines  
DPMRADmTrustedMachines
  - c. Wenn der primäre DPM-Server in keiner der unter Schritt b genannten Gruppen aufgeführt wird, fügen Sie den Server manuell als Mitglied hinzu. Verwenden Sie das Format *Domäne/Name*.

Sollte der Schutz nach Abschluss der oben genannten Schritte fehlschlagen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der Verwaltung die Komponentendienste.
2. Erweitern Sie **Computer**, erweitern Sie **Eigener Computer**, und klicken Sie auf **DCOM-Konfiguration**.
3. Klicken Sie im Ergebnisfenster mit der rechten Maustaste auf **DPM RA Service**, und dann auf **Eigenschaften**.
4. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Sicherheit**.
5. Klicken Sie im Bereich **Start- und Aktivierungsberechtigungen** auf **Bearbeiten**, und führen Sie dann einen der folgenden Schritte aus:
  - Wenn der primäre DPM-Server aufgeführt wird, ist der Eintrag in der Zugangskontrollliste (ACL) möglicherweise falsch. Entfernen Sie den Eintrag, und fügen Sie den primären DPM-Server dann mit vollständigen Berechtigungen hinzu.
  - Wenn der primäre DPM-Server nicht aufgeführt ist, fügen Sie ihn mit vollständigen Berechtigungen hinzu.

## Ausführen einer Bare-Metal-Recovery

Wenn Sie den DPM-Server oder einen geschützten Computer mit dem DPM System Recovery Tool (SRT) sichern, können Sie im Fall eines Hardwareausfalls eine Bare-Metal-Recovery ausführen.

Anleitungen zum Wiederherstellen eines DPM-Servers mit DPM SRT finden Sie, in englischer Sprache, unter „Bare Metal Recovery“ in der DPM SRT-Hilfe.

### Siehe auch

[Sichern für die Bare-Metal-Recovery](#)

## Verwenden von DpmSync

**DpmSync** ist ein Befehlszeilenprogramm, das es Ihnen ermöglicht, die DPM-Datenbank mit dem Status der Datenträger im Speicherpool und mit den installierten Schutz-Agents zu synchronisieren. DpmSync stellt die DPM-Datenbank wieder her, synchronisiert die DPM-Datenbank mit den Replikaten im Speicherpool, stellt die Berichtsdatenbank wieder her und weist fehlende Replikate neu zu.

### DpmSync-Syntax

DpmSync **-Sync**

DpmSync **-DpmDbLoc** *Speicherort*

DpmSync **-DpmReportDbLoc** *Speicherort*

DpmSync **-ReallocateReplica**

DpmSync **-?**



## Parameter

Parameter	Beschreibung
<b>-Sync</b>	Synchronisiert wiederhergestellte Datenbanken und weist fehlende Replikativolumen neu zu. Sie müssen DpmSync –Sync ausführen, nachdem Sie die Datenbank wiederhergestellt haben. Nachdem Sie DpmSync –Sync ausgeführt haben, sind einige Replikate möglicherweise noch als fehlend gekennzeichnet. Entfernen Sie in der DPM-Verwaltungskonsole auf der Registerkarte <b>Datenträger</b> im Aufgabenbereich <b>Verwaltung</b> die fehlenden Datenträger aus DPM, und führen Sie DpmSync -reallocate replica aus.
<b>-DpmDbLoc</b> <i>Speicherort</i>	Identifiziert den Speicherplatz der DPM-Datenbanksicherung.
<b>-DpmReportDbLoc</b> <i>Speicherort</i>	Identifiziert den Speicherplatz der Berichtsdatenbanksicherung.
<b>-ReallocateReplica</b>	Weist alle fehlenden Replikativolumen ohne Synchronisierung neu zu.
<b>-?</b>	Beschreibt die Verwendung des Befehls.

### Beispiel

Um die DPM- und Berichtsdatenbanken aus einem lokalen Sicherungsmedium auf dem DPM-Server wiederherzustellen, führen Sie die folgenden Befehle aus:

**DpmSync -DpmDbLoc G:\DPM\Backups\2005\November\DPMDB.bak**

**DpmSync -DpmReportDbLoc G:\DPM\Backups\2005\November\ReportServer.bak**

Nach dem Wiederherstellen der DPM- und Berichtsdatenbanken führen Sie folgenden Befehl aus, um die Datenbanken zu synchronisieren:

**DpmSync -Sync**

Nach dem Wiederherstellen und Synchronisieren der DPM- und Berichtsdatenbanken und bevor Sie die Replikate wiederherstellen, führen Sie folgenden Befehl aus, um den Replikaten Festplattenspeicherplatz zuzuweisen:

**DpmSync -ReallocateReplica**

### Siehe auch

[Wiederherstellen von DPM-Datenbanken](#)

[Wiederherstellen von DPM-Replikaten](#)

# Verwenden von Skripten vor und nach Sicherungen

Ein *Prä-Sicherungsskript* ist ein Skript, das auf dem geschützten Computer gespeichert ist; es wird vor jedem DPM-Sicherungsauftrag ausgeführt und bereitet die geschützte Datenquelle auf die Sicherung vor.

Ein *Post-Sicherungsskript* ist ein Skript, das nach einem DPM-Sicherungsauftrag ausgeführt wird, um die Aufgaben nach dem Sichern auszuführen; zum Beispiel bringt dieses Skript einen virtuellen Rechner wieder online.

Wenn Sie einen Schutz-Agent auf einem Computer installieren, wird die Datei `ScriptingConfig.xml` unter `Installationspfad\Microsoft Data Protection Manager\DPM\Scripting` auf dem geschützten Computer hinzugefügt. Für jede geschützte Datenquelle auf dem Computer können Sie in der Datei `ScriptingConfig.xml` ein Prä-Sicherungsskript und ein Post-Sicherungsskript festlegen.

Wenn DPM einen Schutzauftrag ausführt, wird die Datei `ScriptingConfig.xml` auf dem geschützten Computer überprüft. Wenn ein Prä-Sicherungsskript festgelegt wurde, führt DPM das Skript aus und schließt dann den Auftrag ab. Wenn ein Post-Sicherungsskript festgelegt wurde, schließt DPM den Auftrag ab und führt dann das Skript aus.



## Hinweis

Zu den Schutzaufträgen gehören Replikaterstellungen, vollständige Schnellsicherungen, Synchronisierungen und Konsistenzprüfungen.

DPM führt die Prä-Sicherungs- und Post-Sicherungsskripts unter Verwendung des lokalen Systemkontos aus. Es hat sich bewährt, sicherzustellen, dass die Skripts nur für das Administratorkonto und das lokale Systemkonto Lese- und Schreibberechtigungen haben. Diese Berechtigungsstufe verhindert, dass unbefugte Benutzer die Skripts ändern.

## ScriptingConfig.xml

```
<?xml version="1.0" encoding="utf-8"?>
<ScriptConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.microsoft.com/2003/dls/ScriptingConfig.xsd">
  <DataSourceScriptConfig DataSourceName="Datenquelle">
    <PreBackupScript>"Pfad\Skript" </PreBackupScript>
    <PreBackupCommandLine>Parameter</PreBackupCommandLine>
    <PostBackupScript>"Pfad\Skript" </PostBackupScript >
    <PostBackupCommandLine>Parameter</PostBackupCommandLine>
    <Timeout>30</Timeout>
  </DataSourceScriptConfig>
</ScriptConfiguration>
```

### ▶ So legen Sie Prä-Sicherungs- und Post-Sicherungsskripts fest

1. Öffnen Sie auf dem geschützten Computer die Datei ScriptingConfig.xml in einem XML- oder Text-Editor.
2. Vervollständigen Sie das Element DataSourceScriptConfig für jede Datenquelle wie folgt:
  - a. Geben Sie für das DataSourceName-Attribut das Datenquellenvolume (für Dateidatenquellen) oder den Namen (für alle anderen Datenquellen) ein. Der Datenquellenname für Anwendungsdaten sollte das folgende Format aufweisen: *Instanz\Datenbank* für SQL, *Speichergruppenname* für Exchange, ? für Virtual Server, und ? für Windows SharePoint Services.
  - b. Geben Sie im PreBackupScript-Tag den Pfad und den Skriptnamen ein.
  - c. Geben Sie im PreBackupCommandLine-Tag die durch Leerzeichen getrennten Befehlszeilenparameter ein, die an die Skripts übergeben werden sollen.
  - d. Geben Sie im PostBackupScript-Tag den Pfad und den Skriptnamen ein.
  - e. Geben Sie im PostBackupCommandLine-Tag die durch Leerzeichen getrennten Befehlszeilenparameter ein, die an die Skripts übergeben werden sollen.
  - f. Geben Sie im TimeOut-Tag die Zeitspanne in Minute an, die DPM nach dem Aufrufen eines Skripts warten soll, bis ein Timeout eintritt und das Skript als fehlgeschlagen markiert wird.
3. Speichern Sie die Datei ScriptingConfig.xml.



#### **Hinweis**

DPM hängt zusätzliche Boolesche Parameter (true/false) an den Post-Sicherungsskript-Befehl an, um den Ausführungsstatus des DPM-Sicherungsauftrags anzuzeigen.

## Anhang A: Kurzreferenz für DPM-Aufgaben

In der folgenden Tabelle sind administrativen Aufgaben den Objekten zugeordnet, die Sie zur Ausführung der Aufgabe auswählen.

Aufgabe	Auswahl
<ul style="list-style-type: none"> <li>• Replikat manuell synchronisieren</li> <li>• Manuelle Konsistenzprüfung für ein Replikat ausführen</li> <li>• Wiederherstellungspunkt manuell erstellen</li> <li>• Mitglied aus einer Schutzgruppe entfernen</li> <li>• Replikat löschen</li> </ul>	Die geschützte Datenquelle im Aufgabenbereich <b>Schutz</b>
<ul style="list-style-type: none"> <li>• Zeitpläne für Synchronisierungen, vollständige Schnellsicherungen, Konsistenzprüfungen und Wiederherstellungspunkte ändern</li> <li>• Komprimierung aktivieren</li> <li>• Einer Schutzgruppe ein Mitglied hinzufügen</li> <li>• Liste der Bänder anzeigen</li> <li>• Schutz einer Gruppe beenden</li> </ul>	Die Schutzgruppe im Aufgabenbereich <b>Schutz</b>
<ul style="list-style-type: none"> <li>• Aufbewahrungszeitraum des Bandkatalogs konfigurieren</li> </ul>	Der geschützte Computer oder die Schutzgruppe im Aufgabenbereich <b>Schutz</b>
<ul style="list-style-type: none"> <li>• Datenträgerzuweisung ändern</li> </ul>	Die geschützte Datenquelle oder die Schutzgruppe im Aufgabenbereich <b>Schutz</b>
<ul style="list-style-type: none"> <li>• Netzwerk-Bandbreitenbeschränkung konfigurieren</li> <li>• Schutz-Agents aktualisieren, deaktivieren oder aktivieren</li> </ul>	Der geschützte Computer auf der Registerkarte <b>Agents</b> im Aufgabenbereich <b>Verwaltung</b>
<ul style="list-style-type: none"> <li>• Tür der Bandbibliothek sperren oder entsperren</li> <li>• Bandbibliothek neu einlesen</li> </ul>	Die Bandbibliothek oder das eigenständige Bandlaufwerk auf der Registerkarte <b>Bibliotheken</b> im Aufgabenbereich <b>Verwaltung</b>
<ul style="list-style-type: none"> <li>• Bandlaufwerk reinigen</li> </ul>	Das Bandlaufwerk auf der Registerkarte <b>Bibliotheken</b> im Aufgabenbereich <b>Verwaltung</b>
<ul style="list-style-type: none"> <li>• Schnelle oder ausführliche Inventarisierung ausführen</li> </ul>	Bandbibliothek, eigenständiges Bandlaufwerk, Laufwerk, Schacht oder Band auf der Registerkarte <b>Bibliotheken</b> im Aufgabenbereich <b>Verwaltung</b>
<ul style="list-style-type: none"> <li>• Band löschen</li> <li>• Band als frei kennzeichnen</li> <li>• Band als Reinigungsband kennzeichnen</li> <li>• Inhalt eines Bandes anzeigen</li> </ul>	Ein Band auf der Registerkarte <b>Bibliotheken</b> im Aufgabenbereich <b>Verwaltung</b>

# Anhang B: Schemaerweiterungen in DPM 2007

---

Das Tool DPMADSchemaExtension führt folgende Aufgaben zur Unterstützung der Endbenutzerwiederherstellung aus:

- Erweitert das Schema
- Erstellt einen Container (MS-ShareMapConfiguration)
- Gewährt dem DPM-Server Berechtigungen zum Ändern der Inhalte des Containers
- Fügt Zuordnungen zwischen Quellenfreigaben und Freigaben aus den Replikaten hinzu

In diesem Anhang werden die Klassen und Attribute beschrieben, die Data Protection Manager (DPM) zur Unterstützung der Endbenutzerwiederherstellung zu Active Directory hinzufügt.

Im Abschnitt [Von DPM hinzugefügte Klassen](#) werden die Klassen beschrieben, die zu Active Directory hinzugefügt werden, wenn Sie die Endbenutzerwiederherstellung in DPM aktivieren.

Im Thema [Von DPM hinzugefügte Attribute](#) werden die Attribute beschrieben, die zu Active Directory hinzugefügt werden, wenn Sie die Endbenutzerwiederherstellung in DPM aktivieren.

## Von DPM hinzugefügte Klassen

Wenn die Endbenutzerwiederherstellung aktiviert ist, fügt DPM die Klasse **ms-SrvShareMapping** zum Verzeichnisdienst Active Directory hinzu. Diese Klasse enthält die Zuordnung vom geschützten Computer (und Freigabe) zum DPM-Server (und Freigabe).

### **Vorsicht**

Es wird empfohlen, diese Klasse nicht zu ändern.

Die folgende Tabelle enthält eine detaillierte Beschreibung der Klasse **ms-SrvShareMapping**:

Attribut	Wert
objectClass	Top
objectClass	classSchema
instanceType	4
possSuperiors	Container
possSuperiors	organizationalUnit
subClassOf	Top
governsID	1.2.840.113556.1.6.33.1.22
mustContain	ms-backupSrvShare
mustContain	ms-productionSrvShare

Attribut	Wert
rDNAttID	Cn
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-SrvShareMapping
IDAPDisplayName	ms-SrvShareMapping
adminDescription	Führt Server mit freigegebenen Ressourcen auf.
objectClassCategory	1

## Von DPM hinzugefügte Attribute

Wenn die Endbenutzerwiederherstellung aktiviert ist, fügt DPM zwei Attribute zu Active Directory hinzu. In der folgenden Tabelle werden die hinzugefügten Attribute aufgelistet:

Attribut	Beschreibung
ms-BackupSrv-Share	Stellt den Namen der DPM-Freigabe und des DPM-Computers als Zeichenfolgen zur Verfügung.
ms-ProductionSrv-Share	Stellt den Freigabennamen des geschützten Computers und den Computernamen des geschützten Computers als Zeichenfolgen zur Verfügung.

## ms-BackupSrv-Share-Attribut

Die folgende Tabelle enthält eine ausführliche Beschreibung des **ms-BackupSrv-Share**-Attributs:

Attribut	Wert
objectClass	Top
objectClass	attributeSchema
attributID	1.2.840.113556.1.6.33.2.23
attributeSyntax	2.5.5.12
rangeUpper	260
isSingleValued	TRUE
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-BackupSrv-Share
adminDescription	Kennzeichnet einen Server mit freigegebenen Ressourcen.
oMSyntax	64
IDAPDisplayName	ms-backupSrvShare
objectCategory	CN=Attribute-Schema,<SchemaContainerDN>

## ms-ProductionSrv-Share-Attribut

Die folgende Tabelle enthält eine ausführliche Beschreibung des **ms-ProductionSrv-Share**-Attributs:

Attribut	Wert
objectClass	Top
objectClass	attributeSchema
attributID	1.2.840.113556.1.6.33.2.24
attributeSyntax	2.5.5.12
rangeUpper	260
isSingleValued	TRUE
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-ProductionSrv-Share
adminDescription	Kennzeichnet einen Computer mit freigegebenen Ressourcen.
oMSyntax	64
IDAPDisplayName	ms-productionSrvShare
objectCategory	CN=Attribute-Schema,<SchemaContainerDN>



# Anhang C: Benutzerdefinierte Berichtansichten

---

Data Protection Manager 2007 enthält verschiedene SQL-Ansichten, die Ihnen helfen, benutzerdefinierte Berichte zu erstellen.

SQL-Ansichten vereinfachen Ihre Abfragen, indem Spalten mit Daten gefüllt werden, die aus verschiedenen Tabellen in der Datenbank gesammelt werden. Diese Ansichten bieten verschiedene Vorteile gegenüber der direkten Abfrage der Tabellen:

- Sie benötigen keine weitreichenden Kenntnisse der gesamten Datenbank oder der Beziehungen zwischen Tabellen und Schlüsseln.
- Wenn die Datenbankstruktur in zukünftigen Versionen des Produkts geändert werden sollten, können die Ansichten aktualisiert werden, sodass sie sich gleich verhalten.

Für DPM-Installationen, die einen separaten, dedizierten Computer für die SQL Server-Datenbank verwenden, werden die Ansichten auf dem Datenbankcomputer abgefragt, nicht auf dem Computer, auf dem DPM ausgeführt wird. Auf diese Weise werden Ressourcen weniger belastet, wenn viele Ansichten innerhalb kurzer Zeit abgefragt werden.

Die potenziellen Nachteile von SQL-Ansichten sind:

- Da die Ansicht bei jeder Abfrage ausgeführt wird, kann die Serverleistung beeinträchtigt werden, wenn die Ansicht zu häufig verwendet wird.
- Die verfügbaren unterstützten Ansichten beinhalten möglicherweise nicht alle Spalten, die Sie benötigen.

In diesem Anhang sind die in DPM 2007 verfügbaren Ansichten aufgeführt.

**Vw\_DPM\_Agents:** Enthält die Liste der Computer, auf denen ein DPM-Schutz-Agent von diesem DPM-Server installiert wurde.

Feld	Datentyp	Beschreibung
ServerName	Zeichenkette	Der Name des Computers
Version	Zeichenkette	Die Version des DPM-Agents auf diesem Computer

**Vw\_DPM\_Alerts:** Liste aller Warnungen der letzten 30 Tage.

Feld	Datentyp	Beschreibung
Severity	Ganzzahl 0=Fehler 1=Warnung 2=Information	Der Schweregrad der Warnung
Resolution	Ganzzahl 0 = Aktiv 1 = Empfohlene Aktion wird ausgeführt 2 = Aufgelöst	Der Zustand der Warnung
OccurredSince	Datum und Uhrzeit	Das erste Auftreten dieser Warnung
ResolvedTime	Datum und Uhrzeit	Der Zeitpunkt, zu dem die Warnung aufgelöst wurde
Type	Ganzzahl Siehe „Warnungstypen“ in diesem Anhang	Der Typ der Warnung

**Vw\_DPM\_CurrentOnlineMedia:** Die Bänder, die zurzeit in den zu DPM gehörigen Bibliotheken online sind wie bei der letzten Inventarisierung erfasst.

Feld	Datentyp	Beschreibung
UserFriendlyName	Zeichenkette	Der Name des Computers
ImportPoolMediaCount	Ganzzahl	Auf diesen DPM-Server importierte Bänder
FreePoolMediaCount	Ganzzahl	Als frei oder leer gekennzeichnete Bänder
AdminPoolMediaCount	Ganzzahl	Bänder mit aktiven Daten. Abgelaufene Bänder werden als frei angezeigt, wenn das Band als frei gekennzeichnet wird oder wenn die Schutzgruppe gelöscht wird.

**Vw\_DPM\_Disk\_Usage\_Replica:** Datenträgerauslastungsstatistiken für Replikate im Speicherpool.

Feld	Datentyp	Beschreibung
PhysicalPath	Zeichenkette	Der Name der geschützten Datenquelle
ReplicaId	GUID	Eindeutiger Kennzeichner für das Replikat auf DPM-Datenträgern
PGId	GUID	Eindeutiger Kennzeichner für die Schutzgruppe, zu der die Datenquelle gehört
ProductionServerName	Zeichenkette	Der Name des Servers, auf dem sich die Datenquelle befindet
DiskAllocated	Große Ganzzahl	Der gesamte Festplattenspeicher, der dieser Datenquelle zugewiesen ist
DiskUsed	Große Ganzzahl	Der gesamte Festplattenspeicher, der von dieser Datenquelle verwendet wird
FreeSpace	Große Ganzzahl	DiskAllocated – DiskUsed
ReplicaAllocated	Große Ganzzahl	Der Teil von DiskAllocated, der für das Replikat der Datenquelle reserviert ist
ReplicaUsed	Große Ganzzahl	Der Teil von ReplicaAllocated, der tatsächlich verwendet wird
ShadowCopyAllocated	Große Ganzzahl	Der Teil von DiskAllocated, der für die Wiederherstellungspunkte der Datenquelle reserviert ist
ShadowCopyUsed	Große Ganzzahl	Der Teil von ShadowCopyAllocated, der tatsächlich verwendet wird
StartDateTime	Datum und Uhrzeit	Der Zeitpunkt, zu dem diese Statistik erfasst wurde
EndTime	Datum und Uhrzeit	Internes Feld
ScheduleType	Ganzzahl 0=Wöchentlich 1=Monatlich 2=Vierteljährlich 3=Jährlich	Der Zeitplanungszeitraum, den diese Daten repräsentieren

**Vw\_DPM\_DiskRecoveryPoints:** Zählt die Datenträger-Wiederherstellungspunkte, die für die einzelnen Datenquellen verfügbar sind.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Der Name der geschützten Datenquelle
PGId	GUID	Eindeutiger Kennzeichner für die Schutzgruppe, zu der die Datenquelle gehört
ServerId	GUID	Eindeutiger Kennzeichner für den Server, zu dem die Datenquelle gehört
Frequency	Ganzzahl	Die Anzahl verfügbarer Wiederherstellungspunkte

**Vw\_DPM\_LongRecoveries:** Liefert historische Informationen über Wiederherstellungen, die länger als 24 Stunden gedauert haben.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Die Datenquelle, die wiederhergestellt wurde
TargetServerName	Zeichenkette	Der Name des Servers, auf dem wiederhergestellt wurde
WriterId	GUID	Gibt den Typ der wiederhergestellten Datenquelle an
StartTime	Datum und Uhrzeit	Der Zeitpunkt, zu dem die Wiederherstellung gestartet wurde
EndTime	Datum und Uhrzeit	Der Zeitpunkt, zu dem die Wiederherstellung beendet war
RecoverySize	Große Ganzzahl	Die Größe der Daten, die bei dem Auftrag wiederhergestellt wurden
RecoverySource	Ganzzahl 0=Datenträger 1=Band	Die Wiederherstellungsquelle

**Vw\_DPM\_Media:** Liefert Informationen zum Zustand aller DPM bekannten Bänder.

Feld	Datentyp	Beschreibung
MediaLabel	Zeichenkette	Die Bezeichnung auf dem Band
MediaBarcode	Zeichenkette	Der Strichcode des Bandes
IsOnline	Ganzzahl	Gibt an, ob das Band online ist
LibraryName	Zeichenkette	Der Name der Bibliothek, in der das Band vorhanden ist. NULL, wenn das Band offline ist
MediaSlotNumber	Ganzzahl	Die Schachtnummer, in der das Band vorhanden ist. NULL, wenn das Band offline ist Befindet sich das Band in einem Laufwerk, gibt dies den ursprünglichen Schacht des Bandes an (in den das Band beim Aufheben der Bereitstellung zurückkehrt).
PGName	Zeichenkette	Der Name der Schutzgruppe, in der das Band vorhanden ist.
MediaExpiryDate	Datum und Uhrzeit	Der Zeitpunkt, zu dem alle Datensets auf diesem Band abgelaufen sind. Dies kann ein Datum in der Vergangenheit oder NULL sein, wenn das Band frei ist.

**Vw\_DPM\_MediaPool\_Media:** Bandzählung für eine bestimmte Bibliothek.

Feld	Datentyp	Beschreibung
LibraryName	Zeichenkette	Der Name der Bibliothek.
FreeMedia	Ganzzahl	Anzahl der freien Bänder in dieser Bibliothek
FreeMediaThreshold	Ganzzahl	Der Schwellenwert, unter dem die Bibliothek eine Warnung ausgibt

**Vw\_DPM\_ProtectedDataSource:** Aktuelle Datenträgerauslastung durch verschiedene Datenquellen.

Feld	Datentyp	Beschreibung
ReplicaId	GUID	Kennzeichner des Replikats
PGId	GUID	Kennzeichner der Schutzgruppe, zu der das Replikat gehört
AllocatedSize	Große Ganzzahl	Datenträgerspeicher, der der Datenquelle zugewiesen ist
UsedSize	Große Ganzzahl	Datenträgerspeicher, der zurzeit von der Datenquelle verwendet wird
ProductionServerName	Zeichenkette	Der Name des Computers, auf dem sich die Datenquelle befindet
StorageNode	Zeichenkette	Immer auf den DPM-Server eingestellt

**Vw\_DPM\_ProtectedGroup:** Tabelle mit Informationen zu allen Schutzgruppen.

Feld	Datentyp	Beschreibung
PGId	GUID	Eindeutiger Kennzeichner der Schutzgruppe
ProtectionGroupName	Zeichenkette	Name der Schutzgruppe
CreationTime	Datum und Uhrzeit	Der Zeitpunkt, zu dem die Schutzgruppe erstellt wurde

**Vw\_DPM\_RecoveryDuration:** Verlauf der Zählungen für Wiederherstellungsaufträge über verschiedene Zeitspannen.

Feld	Datentyp	Beschreibung
StartDateTime	Datum und Uhrzeit	Der Zeitpunkt, zu dem die Statistik erfasst wurde
EndDateTime	Datum und Uhrzeit	Intern
ScheduleType	Ganzzahl	Die Frequenz, für die diese Statistik erfasst wurde
RecoveryDuration	Ganzzahl	Gibt an, ob die Wiederherstellung weniger als 6 Stunden, zwischen 6 und 24 Stunden oder länger als 24 Stunden gedauert hat
RecoveryCount	Ganzzahl	Anzahl der Wiederherstellungen

**Vw\_DPM\_RecoveryJob:** Ausführliche Informationen über aktuelle Wiederherstellungsaufträge.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Die Datenquelle, für die die Wiederherstellung ausgeführt wurde
ServerName	Zeichenkette	Der Server, auf dem die Wiederherstellung ausgeführt wurde
CreationTime	Datum und Uhrzeit	Zeitpunkt, zum dem der Wiederherstellungsauftrag ausgeführt wurde
FailureCode	Ganzzahl	Fehlercode für den Fall, dass der Wiederherstellungsauftrag fehlgeschlagen ist
Status	Ganzzahl 0/1=Findet statt 2=Erfolgreich 3=Fehlgeschlagen	Status des Wiederherstellungsauftrags



**Vw\_DPM\_RecoveryPointDisk:** Status aktueller Wiederherstellungspunkterstellungen auf Datenträgern.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Die Datenquelle, für die die Sicherung erstellt wurde
ServerName	Zeichenkette	Der Server, auf dem sich die Datenquelle befindet
CreationTime	Datum und Uhrzeit	Zeitpunkt, zum dem die Wiederherstellungspunkterstellung ausgeführt wurde
Status	Ganzzahl 0/1=Findet statt 2=Erfolgreich 3=Fehlgeschlagen	Status des Wiederherstellungspunkterstellungsauftrags
ErrorCode	Ganzzahl	Null bei Erfolg. Andernfalls ein DPM-Fehlercode.

**Vw\_DPM\_RecoveryPointTape:** Status aktueller Wiederherstellungspunkterstellungen auf Band.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Die Datenquelle, für die die Sicherung erstellt wurde
ServerName	Zeichenkette	Der Server, auf dem sich die Datenquelle befindet
CreationTime	Datum und Uhrzeit	Zeitpunkt, zum dem die Wiederherstellungspunkterstellung ausgeführt wurde
Status	Ganzzahl 0/1=Findet statt 2=Erfolgreich 3=Fehlgeschlagen	Status des Wiederherstellungspunkterstellungsauftrags
ErrorCode	Ganzzahl	Null bei Erfolg. Andernfalls ein DPM-Fehlercode.

**Vw\_DPM\_Replica:** Auflistung aller von DPM verwalteten Replikate.

Feld	Datentyp	Beschreibung
ReplicaId	GUID	Eindeutiger Kennzeichner, der von DPM für das Replikatvolumen generiert wird
PhysicalPath	Zeichenkette	Der Name der Datenquelle im Replikat
ServerName	Zeichenkette	Name des Servers, zu dem die Datenquelle gehört
ValidFrom	Datum und Uhrzeit	Wann das Replikat erstellt wurde
ValidTo	Datum und Uhrzeit	Datum, an dem das Replikat inaktiv wurde
PGId	GUID	Eindeutiger Kennzeichner, der von DPM für die Schutzgruppe, zu der die Datenquelle gehört, generiert wird
StorageNode	Zeichenkette	Immer auf den DPM-Server eingestellt

**Vw\_DPM\_Server:** Liste aller geschützten Computer.

Feld	Datentyp	Beschreibung
ServerId	GUID	Eindeutiger Kennzeichner, der von DPM für den geschützten Computer generiert wird
ServerName	Zeichenkette	Vollständig qualifizierter Domänenname des Computers
NetBiosName	Zeichenkette	Name
DomainName	Zeichenkette	Domäne, zu der der Computer gehört
IsRG	Ganzzahl	Ob dieser Computer eine Ressourcengruppe repräsentiert

**Vw\_DPM\_TapeRecoveryPoints:** Zählt die Band-Wiederherstellungspunkte, die für die einzelnen Datenquellen verfügbar sind.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Der Name der geschützten Datenquelle
PGId	GUID	Eindeutiger Kennzeichner für die Schutzgruppe, zu der die Datenquelle gehört
ServerId	GUID	Eindeutiger Kennzeichner für den Server, zu dem die Datenquelle gehört
Frequency	Ganzzahl	Die Anzahl verfügbarer Wiederherstellungspunkte
Term	Ganzzahl 0=Kurzfristig 1=Langfristig	Der Zeitplan, dem dieser Wiederherstellungspunkt entspricht

**Vw\_DPM\_TapeStat:** Historische Informationen zu Bandauslastungszählungen.

Feld	Datentyp	Beschreibung
StartDateTime	Datum und Uhrzeit	
EndDateTime	Datum und Uhrzeit	
ScheduleType	Ganzzahl	Ganzzahl 0=Wöchentlich 1=Monatlich 2=Vierteljährlich 3=Jährlich
Free	Ganzzahl	Anzahl der freien Bänder zur Schlusszeit
Online	Ganzzahl	Anzahl der Bänder, die zur Schlusszeit online sind

**Vw\_DPM\_TapeUsagePerPG:** Historische Bandauslastungsdaten pro Schutzgruppe.

Feld	Datentyp	Beschreibung
StartDateTime	Datum und Uhrzeit	Startzeit
EndDateTime	Datum und Uhrzeit	Schlusszeit
PGName	Zeichenkette	Name der Schutzgruppe
ScheduleType	Ganzzahl	Ganzzahl 0=Wöchentlich 1=Monatlich 2=Vierteljährlich 3=Jährlich
Online	Ganzzahl	Anzahl der Bänder, die zur Schlusszeit online sind
Offline	Ganzzahl	Anzahl der Bänder, die zur Schlusszeit offline sind

**Vw\_DPM\_Total\_Disk\_Trend:** Historischer Trend für die gesamte Datenträgerspeicherplatznutzung.

Feld	Datentyp	Beschreibung
StartDateTime	Datum und Uhrzeit	
EndTime	Datum und Uhrzeit	
ScheduleType	Ganzzahl	Ganzzahl 0=Wöchentlich 1=Monatlich 2=Vierteljährlich 3=Jährlich
DiskSpaceCapacity	Große Ganzzahl	Der Gesamtspeicher im Speicherpool zur Schlusszeit
PreviousDiskSpaceCapacity	Große Ganzzahl	Gesamtspeicher im Speicherpool im entsprechenden früheren Zeitraum
DiskSpaceAllocated	Große Ganzzahl	Der Datenträgerspeicher des Speicherpools, der zugewiesen wurde
PreviousDiskSpaceAllocated	Große Ganzzahl	Der Datenträgerspeicher des Speicherpools, der im entsprechenden früheren Zeitraum zugewiesen wurde
DiskSpaceUsed	Große Ganzzahl	Der tatsächlich verwendete Datenträgerspeicherplatz
PreviousDiskSpaceUsed	Große Ganzzahl	Der im entsprechenden früheren Zeitraum verwendete Datenträgerspeicherplatz

**Vw\_DPM\_Total\_RecoveryPoint:** Informationen zu allen aktuellen Wiederherstellungspunktaufträgen.

Feld	Datentyp	Beschreibung
DataSourceName	Zeichenkette	Der Name der geschützten Datenquelle
ServerName	Zeichenkette	Der Server, zu dem die Datenquelle gehört
CreationTime	Datum und Uhrzeit	Zeitpunkt, zum dem die Wiederherstellungspunkterstellung ausgeführt wurde
Status	Ganzzahl 0/1=Findet statt 2=Erfolgreich 3=Fehlgeschlagen	Status des Wiederherstellungspunkterstellungsauftrags
ErrorCode	Ganzzahl	Fehlercode bei der Erstellung des Wiederherstellungspunkts

## Warnungstypen

-1	RestoreDBAlert
0	NullType
1	AgentIncompatibleAlert
2	AgentUnreachableAlert
5	MediaVerificationFailedAlert
6	MediaEraseFailedAlert
7	DetailedInventoryFailedAlert
8	MediaDecommissionedAlert
9	MediaDataEraseAlert
10	FreeMediaThresholdAlert
11	DataSetCopyFailedAlert
12	BackupToTapeFailedAlert
13	BackupToTapeCatalogFailedAlert
14	LibraryDriveAlert
15	LibraryNotAvailableAlert
16	LibraryNotWorkingEfficientlyAlert
17	MediaRequiredAlert
18	ReplicaInitializationInProgressAlert
19	SynchronizationFailedAlert
20	StopProtectionFailedAlert
21	RecoveryInProgressAlert
22	RecoveryPartiallySuccessfulAlert
23	RecoverySuccessfulAlert
24	RecoveryFailedAlert
25	ShadowCopyFailedAlert
26	ReplicaInMissingStateAlert
27	ReplicaInInvalidStateAlert

28	PartialDeployedClusterAlert
29	AgentTaskFailAlert
30	SqmOptInAlert
31	DiskThresholdCrossedAlert
32	VerificationInProgressAlert
33	DiskMissingAlert
34	CatalogThresholdCrossedAlert
35	DatasetDataVerificationFailed
36	SCDiskThresholdCrossedAlert
37	ConfigureProtectionFailedAlert
38	ReplicaManualLoadPendingAlert
39	ReplicaInitializationPendingAlert
40	CertificateExpiringAlert
41	EvalShareInquiryAlert
42	ShadowCopyConsolidationRequired

**Deutsche Übersetzung © Dell Inc. 2007 - Originalversion in englischer Sprache © 2007 Microsoft Corporation. Alle Rechte vorbehalten.** *Die vorliegende Übersetzung wurde von Dell Inc. erstellt und wird Ihnen zum persönlichen Gebrauch zur Verfügung gestellt. Diese Übersetzung wurde nicht von Microsoft überprüft und kann Ungenauigkeiten enthalten. Die Originalversion dieses Dokuments in englischer Sprache finden Sie unter <http://technet.microsoft.com/en-us/library/bb795539.aspx>. Microsoft und Microsoft-Zulieferer übernehmen keine Garantie für die Zweckmäßigkeit und Genauigkeit der im vorliegenden Dokument enthaltenen Informationen.*