Windows Server System

Planen der Bereitstellung von System Center Data Protection Manager 2007

Microsoft Corporation

Veröffentlicht: Sep 2007

Zusammenfassung

Im vorliegenden Dokument wird die Funktionsweise von DPM beschrieben. Außerdem finden Sie hier Richtlinien für die Planung einer DPM-Bereitstellung.

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

Planen einer DPM 2007-Bereitstellung

Im vorliegenden Dokument wird die Funktionsweise von DPM beschrieben. Außerdem finden Sie hier Richtlinien für die Planung einer DPM-Bereitstellung.

In diesem Abschnitt

Einführung in Data Protection Manager 2007

Microsoft System Center Data Protection Manager (DPM) 2007 ist eine Hauptkomponente der Microsoft System Center-Reihe von Verwaltungsprodukten, mit der IT-Profis ihre Windows-Umgebung einfacher verwalten können. DPM ist der neue Standard für die Sicherung und Wiederherstellung unter Windows und gewährleistet den nahtlosen Datenschutz für Microsoft-Anwendungs- und -Dateiserver unter Verwendung integrierter Festplatten und Bandmedien.

In diesem Abschnitt

DPM-Funktionen

Datenschutz ist für Unternehmen und Organisationen entscheidend, und Microsoft System Center Data Protection Manager (DPM) 2007 ist eine effektive Lösung, um diesen Schutz zu bieten. DPM verfügt über die folgenden Vorteile:

- Festplattengestützte Sicherung und Wiederherstellung von Daten
- Bandgestützte Sicherungs- und Archivierungslösungen
- Wiederherstellungslösungen für den Notfall

Sie können die DPM-Datenbank auf Band sichern, oder Sie verwenden einen zweiten DPM-Server an einem geografisch getrennten Standort, um den primären DPM-Server zu schützen.

Wenn Sie einen zweiten DPM-Server verwenden, können Sie die Daten auf geschützten Computern direkt vom zweiten DPM-Server wiederherstellen. Der zweite DPM-Server kann auch Computer schützen, bis der primäre DPM-Server wieder einsatzbereit ist.

- DPM kann die folgenden Elemente schützen:
  - Dateidaten von Volumes, aus Freigaben und aus Ordnern
  - Anwendungsdaten, wie Microsoft Exchange Server-Speichergruppen, Microsoft SQL Server-Datenbanken, Windows SharePoint Services-Farmen sowie Microsoft Virtual Server und dessen virtueller Rechner
  - Dateien für Arbeitsstationen, auf denen Windows XP Professional SP2 und alle Windows Vista-Editionen mit Ausnahme der Home-Edition ausgeführt werden
  - Dateien und Anwendungsdaten auf Clusterservern
  - Systemstatus für geschützte Datei- und Anwendungsserver

In diesem Abschnitt

Siehe auch

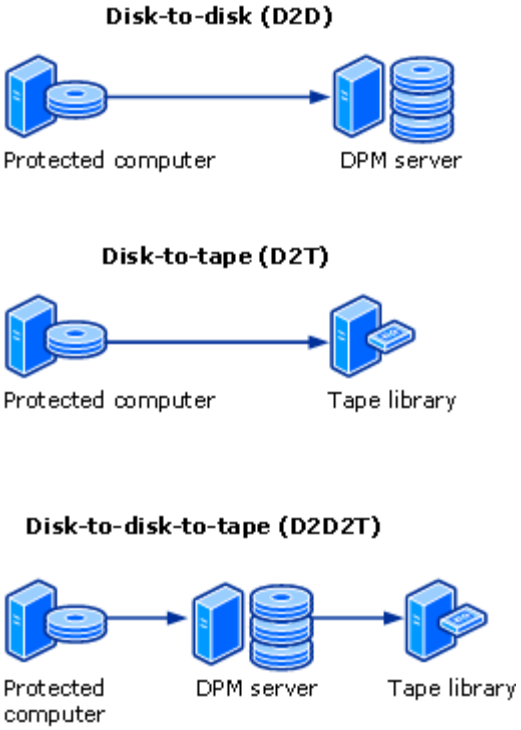
Funktionsweise von DPM

Sicherungslösungen mit Festplatte und Band

Für den DPM-Datenschutz können Sie festplattengestützten Speicher, bandgestützten Speicher oder beides verwenden.

Festplattengestützte Speicherung, auch D2D (für „disk-to-disk“) genannt, ist eine Sicherungsart, bei der Daten von einem Computer auf der Festplatte eines anderen Computers gespeichert werden. Die herkömmliche Datensicherung erfolgt zumeist nach einer anderen Methode, bei der Daten von einem Computer auf einem Speichermedium (Band) gesichert werden. Dies wird auch D2D (für „disk-to-disk“) genannt. Zum besseren Datenschutz lassen sich die beiden Methoden auch zu einer *D2D2T*-Konfiguration („disk-to-disk-to-tape“) kombinieren, um sowohl die Vorzüge einer schnellen Wiederherstellung mit der festplattengestützten, kurzfristigen Speicherung zu nutzen als auch kritische Daten langfristig bandgestützt zu archivieren. In der folgenden Abbildung sind die drei Speichermethoden dargestellt.

Methoden der Datenspeicherung



Welche Speichermethode am besten geeignet ist, richtet sich danach, wie wichtig die Schutzanforderungen Ihres Unternehmens sind.

- **Wie viel Datenverlust kann sich Ihr Unternehmen leisten?** Realistisch gesehen sind nicht alle Daten gleich wichtig. Unternehmen müssen die Auswirkungen des Verlusts gegen die Kosten des Schutzes abwägen.
- **Wie schnell müssen wiederhergestellte Daten verfügbar sein?** Die Wiederherstellung von Daten, die für laufende Vorgänge entscheidend sind, ist normalerweise wichtiger als die Wiederherstellung von Routinedaten. Auf der anderen Seite sollten Unternehmen Server identifizieren, die während der Arbeitszeit wichtige Dienste bereitstellen und deshalb nicht durch Wiederherstellungsvorgänge unterbrochen werden dürfen.
- **Wie lange muss Ihr Unternehmen Daten aufbewahren?** Je nach Art und Inhalt der Daten ist möglicherweise die langfristige Speicherung für Geschäftsprozesse erforderlich. Unter Umständen ist ein Unternehmen auch gesetzlich zur Aufbewahrung von Daten verpflichtet, zum Beispiel durch den Sarbanes-Oxley Act oder die EU-Richtlinie zu Vorratsdaten-speicherung.
- **Wie viel kann Ihr Unternehmen für den Datenschutz ausgeben?** Bei der Überlegung, welcher Betrag für den Datenschutz investiert werden soll, müssen Unternehmen die Kosten der Hardware und der Medien sowie die Personalkosten für Administration, Verwaltung und Support berücksichtigen.

Mit DPM können Sie Daten sowohl auf Festplatte als auch auf Band speichern, so dass Sie flexibel fokussierte, detaillierte Sicherungsstrategien entwickeln können, die einen effizienten und wirtschaftlichen Datenschutz gewährleisten. Wenn Sie eine einzelne Datei oder einen gesamten Server wiederherstellen müssen, so erfolgt dies schnell und unkompliziert: Sie identifizieren die Daten, und DPM sucht die Daten und ruft sie ab (möglicherweise ist Ihr Eingreifen erforderlich, weil das Band aus dem Archiv entfernt wurde).

Festplattengestützter Schutz und Wiederherstellung

Ein Vorteil der festplattengestützten Datensicherung ist die potenzielle Zeitersparnis. Beim festplattengestützten Datenschutz entfällt die Vorbereitungszeit, die beim bandgestützten Datenschutz erforderlich ist, um das richtige Band zu suchen, es zu laden und den korrekten Startpunkt des Bandes einzustellen. Die unkomplizierte Verwendung einer Festplatte führt oft dazu, dass inkrementelle Daten häufiger gesendet werden, wodurch ein möglicher Ausfall geringere Auswirkungen auf den geschützten Computer und die Netzwerkressourcen hat.

Die Datenwiederherstellung ist beim festplattengestützten Datenschutz zuverlässiger als bei bandgestützten Systemen. Festplattenlaufwerke weisen im Allgemeinen eine viel größere durchschnittliche Zeitdauer bis zum Versagen (mean time between failure, MTBF) auf als Bänder.

Die Datenwiederherstellung von der Festplatte ist schneller und unkomplizierter als die Wiederherstellung vom Band. Beim Wiederherstellen der Daten von einer Festplatte müssen lediglich frühere Versionen der Daten auf dem DPM-Server durchsucht und die ausgewählten Versionen direkt auf den geschützten Computer kopiert werden. Eine typische Datenwiederherstellung vom Band dauert mehrere Stunden und kann kostenintensiv sein. Administratoren in einem Rechenzentrum mittlerer Größe müssen damit rechnen, 10 bis 20 Wiederherstellungen pro Monat auszuführen.

Mithilfe von DPM und einem festplattengestützten Datenschutz können Daten bei Bedarf alle 15 Minuten synchronisiert und bis zu 448 Tage aufbewahrt werden.

Bandgestützte Sicherung und Archivierung

Magnetband und ähnliche Speichermedien bieten eine preisgünstige und portable Form der Datensicherung, die sich besonders für die langfristige Speicherung eignet.

In DPM können Sie Daten von einem Computer direkt auf Band sichern (D2T). Es ist jedoch auch möglich, Daten vom festplattengestützten Replikat zu sichern (D2D2T). Der Vorteil beim Erstellen einer langfristigen Sicherung auf Band vom festplattengestützten Replikat liegt darin, dass die Sicherung jederzeit erfolgen kann, ohne den geschützten Computer zu beeinträchtigen.

Des Weiteren gehört zu einem durchdachten Plan für die Wiederherstellung im Notfall auch 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 und praktische Medien für die ausgelagerte Speicherung.

Mithilfe von DPM lassen sich Daten für den kurzfristigen Schutz täglich auf Band sichern, als langfristiger Schutz können die Bändern bis zu 99 Jahre aufbewahrt werden.

Wenn Sie Softwarelösungen von DPM-Partnern einsetzen, können Sie anstelle von Bändern auch Wechselmedien wie zum Beispiel USB-Festplattenlaufwerke verwenden. Weitere Informationen finden Sie, in englischer Sprache, unter Data Protection Manager Partners (http://go.microsoft.com/fwlink/?LinkId=98869).

Siehe auch

Verwaltungshilfsprogramme

Schutz für Clusterserver

Schutz für verschiedene Datentypen

Schutz für verschiedene Datentypen

In der folgenden Tabelle sind die Datentypen aufgeführt, die mit DPM geschützt werden können, sowie die mit DPM wiederherstellbaren Datenebenen.

Hinweis

Informationen über die spezifischen Softwareanforderungen für geschützte Computer finden Sie, in englischer Sprache, unter DPM System Requirements (http://go.microsoft.com/fwlink/?LinkId=66731).

Zu schützende und wiederherstellbare Daten

Produkt	Schützbare Daten	Wiederherstellbare Daten
Exchange Server 2003 Exchange Server 2007	• Speichergruppe	• Speichergruppe • Datenbank • Mailbox
SQL Server 2000 SQL Server 2005	• Datenbank	• Datenbank
Microsoft Office SharePoint Server 2007 Windows SharePoint Services 3.0	• Farm	• Farm • Datenbank • Site • Datei oder Liste

Produkt	Schützbare Daten	Wiederherstellbare Daten
Windows Server 2003 Windows Storage Server 2003	• Volume • Freigabe • Ordner	• Volume • Freigabe • Ordner • Datei
Microsoft Virtual Server 2005 R2 SP1	• Virtuelle Hostserverkonfiguration • Virtuelle Rechner • Daten für Anwendungen, die auf virtuellen Rechnern ausgeführt werden[1]	• Virtuelle Hostserverkonfiguration • Virtuelle Rechner • Daten für Anwendungen, die auf virtuellen Rechnern ausgeführt werden[1]
Alle Computer, die mit DPM 2007 geschützt werden können, mit Ausnahme von Computern, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird	• Systemstatus	• Systemstatus
Arbeitsstationen mit Windows XP Professional SP2 oder einer beliebige Windows Vista-Edition mit Ausnahme der Home-Edition (muss Mitglied einer Domäne sein)	• Dateidaten	• Dateidaten

[1] Daten für Anwendungen, die auf virtuellen Rechnern ausgeführt werden, müssen als Anwendungsdatenquelle geschützt und wiederhergestellt werden, nicht als Komponente eines geschützten virtuellen Rechners. Um zum Beispiel Daten von einer auf einem virtuellen Rechner ausgeführten Instanz von SQL Server zu schützen und wiederherzustellen, installieren Sie den DPM-Schutz-Agent auf dem virtuellen Rechner und wählen die Datenquelle als SQL Server-Datenbank aus. Wenn Sie den Schutz-Agent auf dem virtuellen Host installieren und einen virtuellen Rechner auf dem Host schützen, werden die Anwendungsdaten ebenfalls geschützt, können jedoch nur durch eine Wiederherstellung des virtuellen Rechners wiederhergestellt werden.

Siehe auch

Managing Protected File Servers and Workstations

Managing Protected Servers Running Exchange

Managing Protected Servers Running SQL Server

Managing Protected Servers Running Windows SharePoint Services

Managing Protected Virtual Servers

Schutz für Clusterserver

DPM 2007 unterstützt freigegebene Clusterlaufwerke für Dateiserver, Exchange Server 2003, SQL Server 2000 und SQL Server 2005. DPM 2007 unterstützt sowohl freigegebene als auch nicht freigegebene Clusterlaufwerke für Exchange Server 2007.

Wenn Sie bei der Installation des DPM-Schutz-Agents einen Server auswählen, der ein Clusterknoten ist, informiert Sie DPM, so dass Sie den Schutz-Agent auch auf anderen Knoten des Clusters installieren können.

Die Endbenutzerwiederherstellung ist bei Clusterdateiservern sowohl für Cluster- als auch für Nicht-Clusterressourcen verfügbar.

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

Siehe auch

Schutz für verschiedene Datentypen

Verwaltungshilfsprogramme

Zur Vereinfachung der wichtigsten Verwaltungsaufgaben stellt DPM 2007 die folgenden Tools und Möglichkeiten für IT-Administratoren zur Verfügung:

- DPM-Verwaltungskonsole
- Berichte und Benachrichtigungen
- DPM Management Packs
- Windows PowerShell-Integration
- Remoteverwaltung
- Endbenutzerwiederherstellung

DPM-Verwaltungskonsole

Die DPM-Verwaltungskonsole beruht auf einem aufgabenbasierten Administrationsmodell, das häufige Aufgaben automatisiert, so dass der Administrator seine Aufgabe in möglichst wenigen Schritten ausführen kann.

Um die Verwaltung der Datenschutzaktivitäten zu vereinfachen, basiert DPM auf der Microsoft Management Console (MMC)-Funktionalität, um eine vertraute, intuitive Umgebung für die Konfiguration, Verwaltung und Überwachung zu bieten.

Die DPM-Verwaltungskonsole gliedert Aufgaben in fünf unkompliziert aufzurufende Aufgabenbereiche: Überwachung, Schutz, Wiederherstellung, Berichterstellung und Verwaltung. Der Assistent leitet den Administrator durch grundlegende Konfigurationsaufgaben wie das Hinzufügen von Laufwerken, das Installieren von Agents und das Erstellen von Schutzgruppen. Im Bereich **Wiederherstellung** stehen Funktionen zum Suchen und Durchsuchen zur Verfügung, um frühere Versionen von Dateien zu finden und wiederherzustellen.

Zur Überwachung der Datenschutzaktivitäten gibt es in der DPM-Verwaltungskonsole die Registerkarten **Aufträge** und **Warnungen**. Auf der Registerkarte **Aufträge** werden der Status und Details zu allen geplanten, abgeschlossenen, ausgeführten, abgebrochenen oder fehlgeschlagenen Aufträgen angezeigt. Auf der Registerkarte **Warnungen** werden informative Warnungen und Fehlerbedingungen gesammelt, um einen Überblick über die Aktivitäten für das gesamte System zu bieten. Für jeden Fehler werden empfohlenen Maßnahmen aufgeführt.

Nähere Informationen zur Verwendung der DPM-Verwaltungskonsole finden Sie, in englischer Sprache, in Appendix A: DPM Administrator Console (http://go.microsoft.com/fwlink/?LinkId=98871) in *Deploying DPM 2007*.

Berichte und Benachrichtigungen

DPM bietet eine umfassende Berichtfunktion, mit der sich Daten zu erfolgreichen und fehlgeschlagenen Schutz- und Wiederherstellungsvorgängen sowie zur Festplatten- und Bandnutzung anzeigen lassen. Sie können auch häufig auftretende Fehler identifizieren und den Bandaustausch verwalten. Zusammenfassende Berichte sammeln Informationen zu allen geschützten Computern und Schutzgruppen. Ausführliche Berichte enthalten Informationen zu einzelnen Computern oder Schutzgruppen. Administratoren können nach der ersten DPM-Bereitstellung mithilfe dieser Berichte die Feinabstimmung für den Schutz vornehmen.

Mithilfe von DPM-Benachrichtigungen werden Sie stets über kritische oder informative Meldungen sowie Warnungen informiert, sobald diese generiert werden. Sie können den Schweregrad der Meldungen festlegen, über die Sie informiert werden möchten. So ist es zum Beispiel möglich, nur kritische Warnungen zu erhalten. Sie können auch festlegen, Benachrichtigungen über den Status von Wiederherstellungsaufträgen zu erhalten, und geplante DPM-Berichte können als E-Mail-Anhänge gesendet werden, so dass Sie Datenschutztrends überwachen und Datenschutzstatistiken analysieren können, wann immer es Ihnen am besten passt. Benutzerdefinierte Benachrichtigungen können Sie mit dem DPM Management Pack für System Center Operations Manager 2007 einrichten.

Nähere Informationen zu den in DPM 2007 verfügbaren Berichten finden Sie, in englischer Sprache, unter Managing DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853). Anleitungen zum Abonnieren von Benachrichtigungen finden Sie in der DPM 2007-Hilfe.

DPM Management Packs

Management Packs für Microsoft Operations Manager 2005 (MOM) und System Center Operations Manager 2007 sind für DPM 2007 verfügbar. Im Rahmen Ihrer Datenverwaltungsstrategie können Sie das DPM Management Pack einsetzen, um den Datenschutz, den Status, den Zustand und die Leistung mehrerer DPM-Server sowie die von ihnen geschützten Server zentral überwachen. Von der Operatorkonsole in Operations Manager aus können Administratoren gleichzeitig DPM und die Netzwerkinfrastruktur überwachen und so Probleme mit dem Schutz von Daten im Zusammenhang mit anderen Faktoren der System- und Netzwerkleistung analysieren. Der Administrator kann auch andere missionskritische Anwendungen, zum Beispiel SQL Server, überwachen.

Informationen zum Herunterladen der DPM Management Packs finden Sie, in englischer Sprache, im Management Pack Catalog (http://go.microsoft.com/fwlink/?LinkId=47215).

Windows PowerShell-Integration

Windows PowerShell ist eine interaktive Befehlszeilentechnologie, die auch die aufgabenbasierte Skripterstellung unterstützt.

DPM verfügt über einen eigenen Satz von Windows PowerShell-Befehlen, die für Verwaltungsaufgaben im Bereich Datenschutz verwendet werden können. Auf diese Befehle („DPM-Cmdlets“) haben Sie über die DPM Management Shell Zugriff.

Mithilfe der DPM-Cmdlets können DPM-Administratoren alle Verwaltungsaufgaben ausführen, die in der Konsole ausgeführt werden können. Es stehen zum Beispiel Befehle für die folgenden Aufgaben zur Verfügung:

- DPM konfigurieren
- Bänder und Festplatten verwalten
- Schutzgruppen verwalten
- Daten schützen und wiederherstellen

Zusätzlich können Administratoren mit DPM-Cmdlets die folgenden Aufgaben ausführen, die von der DPM-Verwaltungskonsole aus nicht ausgeführt werden können:

- Wiederherstellungspunkte entfernen
- Startzeit für Bibliothekswartungsaufträge, zum Beispiel Inventarisieren und Aufräumen, anpassen
- Festlegen, welche LAN-Konfiguration für einen Sicherungsauftrag verwendet werden soll

Remoteverwaltung

Sie können eine Remotedesktopverbindung zu einem DPM-Server herstellen, um DPM-Vorgänge remote zu verwalten.

DPM Management Shell kann auf Computern installiert werden, die keine DPM-Server sind, sodass Sie mehrere DPM-Server remote verwalten können. Sie können DPM Management Shell sogar auf Desktopcomputern mit dem Betriebssystem Windows XP oder Windows Vista installieren.

Endbenutzerwiederherstellung

Neben der Wiederherstellung durch Administratoren bietet DPM auch Endbenutzern die Möglichkeit, selbstständig frühere Versionen ihrer Dateien abzurufen, indem sie die vertraute Windows Explorer-Umgebung oder eine beliebige Microsoft Office 2007-Anwendung verwenden. Die Endbenutzerwiederherstellung steht nicht für Anwendungsdaten zur Verfügung.

Siehe auch

Schutz für Clusterserver

Schutz für verschiedene Datentypen

Funktionsweise von DPM

Welche Methode Data Protection Manager zum Schutz der Daten verwendet, richtet sich nach dem Format der geschützten Daten und der von Ihnen ausgewählten Schutzmethode.

In diesem Abschnitt

Festplattengestützter Schutzprozess

Bandgestützter Schutzprozess

Wiederherstellungsprozess

Schutzrichtlinien

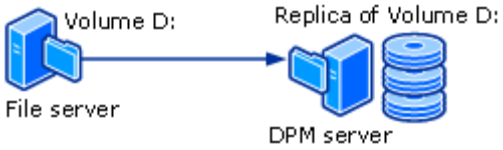
AutoErmittlungs-Prozess

DPM-Verzeichnisstruktur

Festplattengestützter Schutzprozess

Beim festplattengestützten Datenschutz erstellt der DPM-Server ein *Replikat* (eine Kopie) der Daten auf den geschützten Servern. Die Replikate werden im *Speicherpool* gespeichert, der aus mehreren Festplatten auf dem DPM-Server oder auf einem benutzerdefinierten Volume besteht. In der folgenden Abbildung ist die grundlegende Beziehung zwischen einem geschützten Volume und seinem Replikat dargestellt.

Replikaterstellung



Unabhängig davon, ob Sie Dateidaten oder Anwendungsdaten schützen, wird zunächst ein Replikat der Datenquelle erstellt.

Das Replikat wird in regelmäßigen Abständen *synchronisiert*, d. h. aktualisiert. Dies erfolgt entsprechend den von Ihnen festgelegten Einstellungen. Anhand welcher Methode DPM das Replikat synchronisiert, ist vom Typ der geschützten Daten abhängig. Weitere Informationen finden Sie unter Synchronisierungsprozess für Dateidaten und Synchronisierungsprozess für Anwendungsdaten. Wenn ein Replikat als inkonsistent identifiziert wird, führt DPM eine Konsistenzprüfung aus. Dies ist eine Block-für-Block-Überprüfung des Replikats im Vergleich mit der Datenquelle.

Ein einfaches Beispiel für eine Schutzkonfiguration besteht aus einem DPM-Server und einem geschützten Computer. Der Computer ist geschützt, wenn Sie einen DPM-*Schutz-Agent* auf dem Computer installieren und seine Daten einer *Schutzgruppe* hinzufügen.

Schutz-Agents verfolgen Änderungen an geschützten Daten und übertragen die Änderungen an den DPM-Server. Der Schutz-Agent identifiziert auch Daten auf einem Computer, die geschützt werden können, und ist in den Wiederherstellungsprozess involviert. Sie müssen auf jedem Computer, den Sie mit DPM schützen möchten, einen Schutz-Agent installieren. Schutz-Agents können von DPM installiert werden, Sie können sie jedoch auch manuell installieren, indem Sie eine Anwendung wie zum Beispiel Systems Management Server (SMS) verwenden.

Mithilfe von Schutzgruppen wird der Schutz der Datenquellen auf den Computern verwaltet. Eine Schutzgruppe ist eine Sammlung von Datenquellen, für die dieselbe Schutzkonfiguration eingerichtet wurde. Die Schutzkonfiguration besteht aus Einstellungen, die für alle Mitglieder einer Schutzgruppe gelten, zum Beispiel der Schutzgruppenname, die Schutzrichtlinien, die Festplattenzuweisungen und die Replikaterstellungsmethode.

DPM speichert für jedes *Schutzgruppenmitglied* ein separates Replikat im Speicherpool. Bei einen Schutzgruppenmitglied kann es sich um eine beliebige der folgenden Datenquellen handeln:

- Ein Volume, eine Freigabe oder ein Ordner auf einem Desktopcomputer, Dateiserver oder Servercluster
- Eine Speichergruppe auf einem Exchange-Server oder -Servercluster
- Eine Datenbank einer SQL Server-Instanz oder eines Serverclusters

Siehe auch

Synchronisierungsprozess für Anwendungsdaten

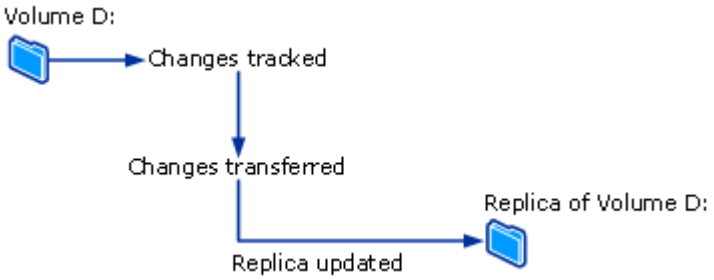
Der Unterschied zwischen Dateidaten und Anwendungsdaten

Synchronisierungsprozess für Dateidaten

Synchronisierungsprozess für Dateidaten

In DPM 2007 verwendet der Schutz-Agent für ein Dateivolume oder eine Freigabe auf einem Server einen Volumefilter und das Änderungsjournal, um festzustellen, welche Dateien geändert wurden. Danach wird ein Prüfsummenverfahren für diese Dateien ausgeführt, um nur die geänderten Blöcke zu synchronisieren. Bei der Synchronisierung werden diese Änderungen an den DPM-Server übertragen und dann auf das Replikat angewendet, um das Replikat mit der Datenquelle zu synchronisieren. In der folgenden Abbildung wird der Dateisynchronisierungs-prozess veranschaulicht.

Dateisynchronisierungsprozess



Wenn ein Replikat nicht mehr mit der Datenquelle konsistent ist, generiert DPM einen Alarm, der angibt, welcher Computer und welche Datenquellen betroffen sind. Um das Problem zu beheben, repariert der Administrator das Replikat, indem er eine *Synchronisierung mit Konsistenzprüfung* (kurz auch nur als *Konsistenzprüfung* bezeichnet) für das Replikat einleitet. Bei der Konsistenzprüfung führt DPM eine Block-für-Block-Überprüfung aus und repariert das Replikat, damit es wieder mit der Datenquelle konsistent ist.

Sie können eine tägliche Konsistenzprüfung für Schutzgruppen planen oder eine Konsistenzprüfung manuell einleiten.

In bestimmten Abständen, die Sie festlegen, erstellt DPM einen *Wiederherstellungspunkt* für die Mitglieder der Schutzgruppe. Ein Wiederherstellungspunkt ist eine Datenversion, mit der sich Daten wiederherstellen lassen. Für Dateien besteht ein Wiederherstellungspunkt aus einer Schattenkopie des Replikats, die vom Volumeschattenkopie-Dienst (VSS) des Betriebssystems auf dem DPM-Server erstellt wird.

Siehe auch

Synchronisierungsprozess für Anwendungsdaten

Der Unterschied zwischen Dateidaten und Anwendungsdaten

Festplattengestützter Schutzprozess

Synchronisierungsprozess für Anwendungsdaten

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

Wie Änderungen auf den DPM-Server übertragen werden, richtet sich nach der Anwendung und nach dem Synchronisierungstyp. Der in der DPM-Verwaltungskonsole als *Synchronisierung* bezeichnete Vorgang entspricht einer inkrementellen Sicherung und erstellt in Kombination mit dem Replikat ein genaues Abbild der Anwendungsdaten.

Während der in der DPM-Verwaltungskonsole als *vollständige Schnellsicherung* bezeichneten Synchronisierung wird durch den Volumeschattenkopie-Dienst (VSS) eine vollständige Schattenkopie erstellt, es werden jedoch nur die geänderten Blöcke auf den DPM-Server übertragen.

Bei jeder vollständigen Schnellsicherung wird ein Wiederherstellungspunkt für die Anwendungsdaten erstellt. Falls die Anwendung inkrementelle Sicherungen unterstützt, wird auch bei jeder Synchronisierung ein Wiederherstellungspunkt erstellt. Die von den einzelnen Anwendungsdatentypen unterstützten Synchronisierungsarten sind nachstehend zusammengefasst:

- Für geschützte Exchange-Dateien wird bei der Synchronisierung mithilfe von Exchange VSS Writer eine inkrementelle VSS-Schattenkopie übertragen. Wiederherstellungspunkte werden für jede Synchronisierung und vollständige Schnellsicherung erstellt.

- SQL Server-Datenbanken, die Protokollversand ausführen, schreibgeschützt sind oder das einfache Wiederherstellungsmodell verwenden, unterstützen keine inkrementellen Sicherungen. Wiederherstellungspunkte werden nur für jede vollständige Schnellsicherung erstellt. Für alle anderen SQL Server-Datenbanken wird bei der Synchronisierung eine Transaktionsprotokollsicherung übertragen, und Wiederherstellungspunkte werden für jede inkrementelle Synchronisierung und vollständige Schnellsicherung erstellt. Das Transaktionsprotokoll ist eine serielle Aufzeichnung aller Transaktionen, die für die Datenbank ausgeführt wurden, seit das Transaktionsprotokoll das letzte Mal gesichert wurde.
- Windows SharePoint Services und Microsoft Virtual Server unterstützen keine inkrementellen Sicherungen. Wiederherstellungspunkte werden nur für jede vollständige Schnellsicherung erstellt.

Inkrementelle Synchronisierungen erfordern weniger Zeit als die Ausführung einer vollständigen Schnellsicherung. Die Zeit, die zum Wiederherstellen von Daten benötigt wird, nimmt mit zunehmender Anzahl von Synchronisierungen jedoch zu. Dies liegt daran, dass DPM die letzte vollständige Sicherung wiederherstellen und dann alle inkrementellen Synchronisierungen bis zum gewählten Zeitpunkt für die Wiederherstellung anwenden muss.

Um eine schnellere Wiederherstellung zu ermöglichen, führt DPM regelmäßig eine vollständige Schnellsicherung aus, wobei das Replikat mit den geänderten Blöcken aktualisiert wird.

Während der vollständigen Schnellsicherung erstellt DPM eine Schattenkopie des Replikats, bevor das Replikat mit den geänderten Blöcken aktualisiert wird. Um häufigere Wiederherstellungspunktziele zu ermöglichen und das Zeitfenster für Datenverluste zu verkleinern, führt DPM auch inkrementelle Synchronisierungen in der Zeit zwischen zwei vollständigen Schnellsicherungen aus.

Wenn ein Replikat nicht mehr mit seiner Datenquelle konsistent ist, generiert DPM wie beim Schutz von Dateidaten eine Warnung, die angibt, welcher Server und welche Datenquelle betroffen ist. Um das Problem zu beheben, repariert der Administrator das Replikat, indem er eine Synchronisierung mit Konsistenzprüfung für das Replikat einleitet. Bei der Konsistenzprüfung führt DPM eine Block-für-Block-Überprüfung aus und repariert das Replikat, damit es wieder mit den Datenquellen konsistent ist.

Sie können eine tägliche Konsistenzprüfung für Schutzgruppen planen oder eine Konsistenzprüfung manuell einleiten.

Siehe auch

Der Unterschied zwischen Dateidaten und Anwendungsdaten

Festplattengestützter Schutzprozess

Synchronisierungsprozess für Dateidaten

Der Unterschied zwischen Dateidaten und Anwendungsdaten

Daten auf einem Dateiserver, die als Flatfile geschützt werden sollen, gelten als Dateidaten, zum Beispiel Microsoft Office-Dateien, Textdateien, Batchdateien usw.

Daten auf einem Anwendungsserver, die von DPM als Anwendung behandelt werden sollen, gelten als Anwendungsdaten, zum Beispiel Exchange-Speichergruppen, SQL Server-Datenbanken, Windows SharePoint Services-Farmen und Virtual Server.

Jede Datenquelle wird in der DPM-Verwaltungskonsole je nach dem gewählten Schutztyp, den Sie für diese Datenquelle auswählen können, angezeigt. Im Assistenten für das Erstellen neuer Schutzgruppen werden die Datentypen zum Beispiel wie folgt behandelt, wenn Sie einen Server erweitern, der Dateien enthält und sowohl Virtual Server als auch eine SQL Server-Instanz ausführt:

- Wenn Sie **Alle Freigaben** oder **Alle Volumes** erweitern, zeigt DPM die Freigaben und Volumes auf diesem Server an und schützt alle Datenquellen, die in einem dieser Knoten ausgewählt wurden, als Dateidaten.
- Wenn Sie **Alle SQL Server** erweitern, zeigt DPM die SQL Server-Instanzen auf diesem Server an und schützt alle Datenquellen, die in diesem Knoten ausgewählt wurden, als Anwendungsdaten.
- Wenn Sie **Microsoft Virtual Server** erweitern, zeigt DPM die Hostdatenbank und virtuellen Rechner auf diesem Server an und schützt alle Datenquellen, die in diesem Knoten ausgewählt wurden, als Anwendungsdaten.

Siehe auch

Synchronisierungsprozess für Anwendungsdaten

Festplattengestützter Schutzprozess

Synchronisierungsprozess für Dateidaten

Bandgestützter Schutzprozess

Wenn Sie kurzfristigen festplattengestützten Schutz und langfristigen bandgestützten Schutz verwenden, kann DPM Daten vom Replikatvolume auf Band sichern, so dass der geschützte Computer nicht beeinträchtigt wird. Wenn Sie nur bandgestützten Schutz verwenden, sichert DPM die Daten direkt vom geschützten Computer auf Band.

DPM schützt Daten auf Band, indem eine Kombination aus vollständigen und inkrementellen Sicherungen verwendet wird, und zwar entweder von der geschützten Datenquelle (für kurzfristigen Schutz auf Band oder für langfristigen Schutz auf Band, wenn DPM die Daten nicht auf der Festplatte schützt) oder vom DPM-Replikat (für langfristigen Schutz auf Band, wenn der kurzfristige Schutz auf Festplatte erfolgt).

Hinweis

Wenn eine Datei bei der letzten Synchronisierung des Replikats geöffnet war, befindet sich die Sicherung dieser Datei vom Replikat in einem *absturzkonsistenten Zustand*. Der absturzkonsistente Zustand einer Datei enthält alle Daten der Datei, die zur Zeit der letzten Synchronisierung auf der Festplatte gespeichert waren. Dies gilt nur für Dateisystemsicherungen. Anwendungssicherungen sind immer konsistent mit dem Anwendungsstatus.

Informationen zu bestimmten Sicherungstypen und -zeitplänen finden Sie unter Planen von Schutzgruppen.

Siehe auch

Funktionsweise von DPM

Festplattengestützter Schutzprozess

Wiederherstellungsprozess

Für Wiederherstellungsaufgaben spielt es keine Rolle, ob für den Schutz der Daten die festplattengestützte oder die bandgestützte Sicherung verwendet wurde. Sie wählen den Wiederherstellungspunkt der Daten, den Sie wiederherstellen möchten, und DPM stellt die Daten auf dem geschützten Computer wieder her.

DPM kann bis zu 64 Wiederherstellungspunkte für jedes Dateimitglied einer Schutzgruppe speichern. Für Anwendungsdatenquellen kann DPM bis zu 448 vollständige Schnellsicherungen und bis zu 96 inkrementelle Sicherungen für jede vollständige Schnellsicherung speichern. Wenn die Speichermöglichkeiten ausgeschöpft sind und der Aufbewahrungszeitraum für die vorhandenen Wiederherstellungspunkte nicht erreicht ist, schlagen Schutzaufträge fehl.

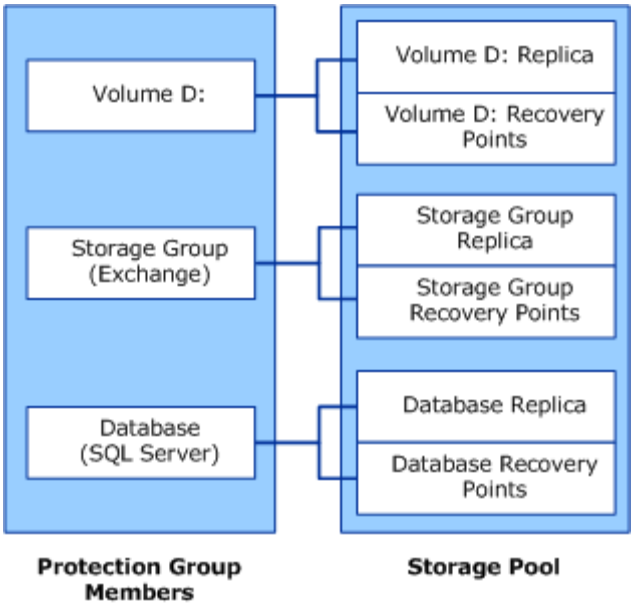
Hinweis

Um die Wiederherstellung durch Endbenutzer zu unterstützen, sind Wiederherstellungspunkte für Dateien durch den Volumeschattenkopie-Dienst (VSS) auf 64 begrenzt.

Wie in den Abschnitten Synchronisierungsprozess für Dateidaten und Synchronisierungsprozess für Anwendungsdaten beschrieben, unterscheidet sich der Prozess beim Erstellen von Wiederherstellungspunkten für Dateidaten und Anwendungsdaten. DPM erstellt Wiederherstellungspunkte für Dateidaten, indem eine Schattenkopie des Replikats nach einem von Ihnen konfigurierten Zeitplan erstellt wird. Für Anwendungsdaten wird bei jeder Synchronisierung und vollständigen Schnellsicherung ein Wiederherstellungspunkt erstellt.

In der folgenden Abbildung wird veranschaulicht, wie die einzelnen Schutzgruppenmitglieder mit dem eigenen Replikatvolume und Wiederherstellungspunktvolume zusammenhängen.

Schutzgruppenmitglieder, Replikate und Wiederherstellungspunkte



Administratoren stellen Daten von verfügbaren Wiederherstellungspunkten mit dem Wiederherstellungsassistenten der DPM-Verwaltungskonsole wieder her. Wenn Sie eine Datenquelle und einen Zeitpunkt, ab dem Sie wiederherstellen möchten, auswählen, informiert DPM Sie, ob sich die Daten auf Band befinden, ob das Band online oder offline ist und welche Bänder für die Wiederherstellung benötigt werden.

Benutzer können frühere Versionen geschützter Dateien wiederherstellen. Da Wiederherstellungspunkte die Ordner- und Dateistruktur der geschützten Datenquellen beibehalten, durchsuchen Benutzer vertraute Volumes, Ordner und Freigaben, um die gewünschten Daten wiederherzustellen. Die Endbenutzerwiederherstellung ist für Anwendungsdaten, zum Beispiel eine Exchange-Mailbox, nicht verfügbar. Die Versionen der Dateidaten, die für die Endbenutzerwiederherstellung verfügbar sind, sind die Daten, die im DPM-Speicherpool auf Festplatte gespeichert sind; Dateidaten, die auf Band archiviert wurden, können nur vom Administrator wiederhergestellt werden.

Endbenutzer stellen geschützte Dateien mithilfe eines Clientcomputers wieder her, auf dem die Schattenkopie-Clientsoftware ausgeführt wird. Benutzer können frühere Versionen über Freigaben auf Dateiservern, über Distributed File System (DFS)-Namespaces oder durch Verwendung eines Befehls im Menü **Extras** für Microsoft Office-Anwendungen wiederherstellen.

Siehe auch

Synchronisierungsprozess für Anwendungsdaten

Synchronisierungsprozess für Dateidaten

Schutzrichtlinien

DPM konfiguriert die *Schutzrichtlinien*, oder Auftragszeitpläne, für jede Schutzgruppe basierend auf den Wiederherstellungszielen, die Sie für diese Schutzgruppe festlegen. Beispiele für Wiederherstellungsziele:

- „Nicht mehr als 1 Stunde der Produktionsdaten verlieren“
- „Aufbewahrungszeitraum von 30 Tagen gewährleisten“
- „Daten sollen 7 Jahre für die Wiederherstellung verfügbar sein“

Ihre *Wiederherstellungsziele* quantifizieren die Datenschutzanforderungen Ihres Unternehmens. In DPM werden Wiederherstellungsziele durch den Aufbewahrungszeitraum, die Datenverlust-toleranz, den Wiederherstellungspunkt-Zeitplan und (für Datenbankanwendungen) den Zeitplan für vollständige Schnellsicherungen bestimmt.

Der *Aufbewahrungszeitraum* ist der Zeitraum, über den die gesicherten Daten verfügbar sein müssen. Müssen die Daten von heute auch in einer Woche noch verfügbar sein? In zwei Wochen? In einem Jahr?

Die *Datenverlusttoleranz* bestimmt die maximale Datenmenge (zeitlich gemessen), deren Verlust für die Geschäftsanforderungen zu verkraften ist. Sie legt fest, wie oft DPM eine Synchronisierung mit dem geschützten Server ausführt, indem Datenänderungen vom geschützten Server gesammelt werden. Sie können die Synchronisierungsfrequenz zwischen 15 Minuten und 24 Stunden einstellen. Sie können auch festlegen, kurz vor dem Erstellen eines Wiederherstellungspunkts zu synchronisieren anstatt nach einem bestimmten Zeitplan.

Der *Wiederherstellungspunkt-Zeitplan* legt fest, wie viele Wiederherstellungspunkte dieser Schutzgruppe erstellt werden. Für den Dateischutz wählen Sie die Tage und Uhrzeiten, für die Wiederherstellungspunkte erstellt werden sollen. Für den Datenschutz von Anwendungen, die inkrementelle Sicherungen unterstützen, bestimmt die Synchronisierungsfrequenz den Wiederherstellungspunkt-Zeitplan. Für den Datenschutz von Anwendungen, die keine inkrementellen Sicherungen unterstützen, bestimmt der Zeitplan für vollständige Schnellsicherungen den Wiederherstellungspunkt-Zeitplan.

Hinweis

Wenn Sie eine Schutzgruppe erstellen, identifiziert DPM den Typ der geschützten Daten und bietet nur die jeweils verfügbaren Schutzoptionen an.

Siehe auch

Funktionsweise von DPM

AutoErmittlungs-Prozess

Die AutoErmittlung ist der tägliche Prozess, mit dem DPM automatisch neue oder entfernte Computer im Netzwerk erkennt. Einmal pro Tag, zu einer von Ihnen gewählten Uhrzeit, sendet DPM ein kleines Paket (weniger als 10 KB) an den nächsten Domänencontroller. Der Domänencontroller antwortet auf die LDAP-Anforderung mit den in dieser Domäne vorhandenen Computern, und DPM identifiziert, welche Computer neu sind und welche entfernt wurden. Der Netzwerkverkehr, der durch die AutoErmittlung entsteht, ist minimal.

Bei der AutoErmittlung werden keine neuen und entfernten Computer in anderen Domänen erkannt. Um einen Schutz-Agent auf einem Computer in einer anderen Domäne zu erstellen, müssen Sie den Computer mit seinem vollständig qualifizierten Domänennamen identifizieren.

Siehe auch

Funktionsweise von DPM

DPM-Verzeichnisstruktur

Wenn Sie anfangen, mit DPM Daten zu schützen, werden Sie bemerken, dass der Installationspfad von DPM drei Ordner im Volumes-Verzeichnis enthält:

- \Microsoft DPM\DPM\Volumes\DiffArea
- \Microsoft DPM\DPM\Volumes\Replica
- \Microsoft DPM\DPM\Volumes\ShadowCopy

Der Ordner „DiffArea“ enthält bereitgestellte Schattenkopievolumes, die die Wiederherstellungspunkte für eine Datenquelle speichern.

Der Ordner „Replica“ enthält bereitgestellte Replikatvolumes.

Der Ordner „ShadowCopy“ enthält lokale Sicherungskopien der DPM-Datenbank. Zusätzlich werden im Ordner „ShadowCopy“ die Sicherungsschattenkopien gespeichert, wenn Sie DPMBackup.exe verwenden, um Sicherungsschattenkopien der Replikate zur Archivierung durch Sicherungssoftware von Drittanbietern zu erstellen.

Siehe auch

Funktionsweise von DPM

Systemanforderungen

Informationen zu den Hardware- und Softwareanforderungen von DPM und geschützten Computern finden Sie, in englischer Sprache, unter System Requirements (http://go.microsoft.com/fwlink/?LinkId=66731).

DPM-Lizenzierung

Für jeden durch DPM geschützten Computer benötigen Sie eine Lizenz. Der Lizenztyp entspricht dem Datentyp, der geschützt wird.

Es gibt zwei DPM-Lizenztypen: Standard und Enterprise. Die Standardlizenz berechtigt Sie, Volumes, Freigaben und Ordner sowie den Computersystemstatus zu schützen. Die Enterprise-Lizenz berechtigt Sie, neben den Datendateien auch Anwendungsdaten wie zum Beispiel Mailboxen und Datenbanken auf einem Exchange-Server zu schützen. Bei einem Servercluster installiert DPM einen Agent auf jedem Knoten des Clusters. Für jeden Serverknoten wird eine Lizenz verwendet.

In der folgenden Tabelle sind die Lizenzen aufgeführt, die auf die einzelnen Datentypen angewendet werden.

Für verschiedene Datentypen verwendete DPM-Lizenzen

Typ der geschützten Daten	Verwendete Lizenz
Nur Dateien.	Standard
Dateien auf einem einzelnen Knoten eines Serverclusters.	Standard
Systemstatus.	Standard
SQL Server. (Ein DPM-Schutz-Agent auf einem Computer, auf dem SQL Server ausgeführt wird, berechtigt Sie, Datenbanken für alle SQL-Instanzen auf diesem Computer zu schützen.)	Enterprise
Exchange Server.	Enterprise
Windows SharePoint Services. (In einer Windows SharePoint Services-Farm wird eine Lizenz für jeden Back-End-Server und eine für den Front-End-Webserver verwendet.)	Enterprise

Typ der geschützten Daten	Verwendete Lizenz
Virtual Server. (Auf einem Computer, auf dem Virtual Server ausgeführt wird, ermöglicht Ihnen ein einzelner auf dem Computer installierter Schutz-Agent, eine beliebe Anzahl virtueller Rechner, oder Gäste, auf dem Host-Computer zu schützen. Um bestimmte Anwendungsdaten auf einem virtuellen Rechner zu schützen, zum Beispiel, um eine Instanz von SQL Server, die auf einem virtuellen Rechner ausgeführt wird, müssen Sie einen Schutz-Agent direkt auf dem virtuellen Rechner installieren. Wenn Sie Daten auf einem virtuellen Rechner schützen, auf dem ein Schutz-Agent installiert ist, wird die entsprechende Lizenz für den geschützten Datentyp verwendet.)	Enterprise
Ein weiterer DPM-Server.	Enterprise
Daten für die „Bare-Metal-Recovery“ mit dem DPM-Hilfsprogramm für die Systemwiederherstellung.	Enterprise

Sie verwenden keine Lizenz, wenn Sie einen Schutz-Agent auf einem Computer installieren. Die Lizenz wird nur angewendet, wenn Daten auf einem Computer einer Schutzgruppe hinzugefügt werden. Wenn Sie auf einem bestimmten Computer keine Daten mehr schützen müssen, können Sie diese Lizenz auf einem anderen Computer verwenden.

Wenn sich der Typ der geschützten Daten ändert, aktualisiert DPM automatisch die Lizenznutzung. Wenn Sie zum Beispiel eine Exchange-Speichergruppe und Dateien auf einem Einzelserver schützen, haben Sie eine Enterprise-Lizenz verwendet, um diesen Server zu schützen. Später beenden Sie den Schutz der Exchange-Speichergruppe. Da DPM jetzt nur noch Dateidaten auf diesem Server schützt, ändert sich die Lizenznutzung zur Standardlizenz.

Sollten Ihnen nur Enterprise-Lizenzen zur Verfügung stehen und Sie Dateidaten auf einem neuen Computer schützen müssen, kann eine Enterprise-Lizenz verwendet werden. Sie haben zum Beispiel drei Standardlizenzen und drei Enterprise-Lizenzen. Sie schützen Dateidaten auf drei Computern. Sie fügen einer Schutzgruppe Dateidaten von einem vierten Computer hinzu. Da bereits alle Standardlizenzen in Gebrauch sind, wendet DPM eine Enterprise-Lizenz an.

Bei der DPM-Installation geben Sie die Anzahl der Lizenzen an, die Sie erworben haben. Nach der Installation können Sie die Lizenzinformationen ggf. ändern, indem Sie im Aufgabenbereich **Schutz** der DPM-Verwaltungskonsole im Bereich **Aktionen** auf **DPM-Lizenzen anzeigen** klicken und dann die Anzahl der erworbenen Lizenzen ändern.

Zusätzliche DPM-Lizenzen können Sie über das Microsoft Partner-Programm erwerben (http://go.microsoft.com/fwlink/?LinkId=71663).

Planen von Schutzgruppen

Damit Sie einen effektiven Plan für die Bereitstellung von Microsoft System Center Data Protection Manager (DPM) 2007 aufstellen können, müssen Sie die Anforderungen Ihres Unternehmens hinsichtlich des Schutzes und der Wiederherstellung von Daten sorgfältig gegen die Möglichkeiten von DPM abwägen.

In diesem Abschnitt finden Sie die Informationen, die Sie für die Planung der Mitglieder und der Konfiguration der Schutzgruppen benötigen. Im Rahmen der Schutzgruppenkonfiguration definieren Sie die Wiederherstellungsziele für die zu schützenden Daten.

Im Zusammenhang mit Microsoft Operations Framework (MOF) wird in diesem Abschnitt davon ausgegangen, dass die Änderung – die Einbindung von DPM in Ihr Unternehmen, um Datenschutz und -wiederherstellung zu bieten – genehmigt wurde und dass Sie für die Implementierung der Änderung zuständig sind.

Weitere Informationen zur Änderungsverwaltung in MOF finden Sie, in englischer Sprache, unter Service Management Functions: Change Management (http://go.microsoft.com/fwlink/?LinkId=68729).

In diesem Abschnitt wird davon ausgegangen, dass Sie DPM einer in Ihrem Unternehmen bereits vorhandenen Wiederherstellungsstrategie für den Notfall hinzufügen. Weitere Informationen zum Planen einer Wiederherstellungsstrategie für den Notfall finden Sie, in englischer Sprache, unter Introduction to Backup and Recovery Services (http://go.microsoft.com/fwlink/?LinkId=71721).

In diesem Abschnitt

Was soll geschützt werden?

Zu Beginn der DPM-Bereitstellungsplanung sollten Sie entscheiden, welche Daten Sie schützen möchten. DPM 2007 bietet Schutz für die folgenden Datentypen, die ausführlicher in späteren Abschnitten erläutert werden:

- Dateidaten auf der Ebene von Volumes, Ordnern und Freigaben auf Dateiservern mit dem Betriebssystem Microsoft Windows Server 2003 oder Windows Server 2008
- Dateidaten auf Arbeitsstationen mit dem Betriebssystem Microsoft Windows XP Professional SP2 oder einer Windows Vista-Edition mit Ausnahme der Home-Edition
- Microsoft Exchange Server 2003 SP2- und Exchange Server 2007-Daten auf der Ebene von Speichergruppen
- Microsoft SQL Server 2000 SP4-, SQL Server 2005 SP1- und SQL Server 2005 SP2-Daten auf der Ebene von Datenbanken
- Windows SharePoint Services 3.0 und Microsoft Office SharePoint Server 2007 auf der Ebene von Farmen
- Microsoft Virtual Server 2005 R2 SP1-Host- und Gastkonfigurationen
- Systemstatus

Siehe auch

Anwendungsdaten

Clusterressourcen

Dateidaten auf Servern und Arbeitsstationen

Systemstatus

Dateidaten auf Servern und Arbeitsstationen

Sie können Volumes schützen, auf die entweder über Laufwerkbuchstaben oder Bereitstellungspunkte zugegriffen wird, sowie Ordner und Freigaben.

Der einfachste Ansatz für die Auswahl der zu schützenden Daten besteht darin, alle Daten auszuwählen, die in Ihre aktuellen Sicherungen einbezogen werden. Alternativ dazu können Sie bestimmte Teilsätze der Daten für den Schutz auswählen.

Der Hauptfaktor bei der Überlegung, welche Daten ausgewählt werden, ist die Notwendigkeit, zu einem bestimmten Zeitpunkt erstellte Kopien der Daten wiederherzustellen, falls Daten verloren gehen oder beschädigt werden. Am ehesten kommen Dateien, die häufig geändert werden, für den Schutz in Betracht. Weitere wahrscheinliche Kandidaten sind Dateien, die häufig aufgerufen werden, unabhängig davon, ob sie dabei oft geändert werden.

Wichtig

Volumes auf Dateiservern sind in der Regel als NTFS formatiert, was für den Schutz mit DPM Voraussetzung ist; auf Arbeitsstationen sind Volumes jedoch auch im Format FAT oder FAT32 zu finden. Damit diese Volumes geschützt werden können, müssen Sie sie zu NTFS konvertieren. Anleitungen hierzu finden Sie, in englischer Sprache, unter How to Convert FAT Disks to NTFS (http://go.microsoft.com/fwlink/?LinkId=83022).

Siehe auch

Ausschließen von Dateien und Ordnern

Schützen von Daten in DFS-Namespaces

Nicht unterstützte Datentypen

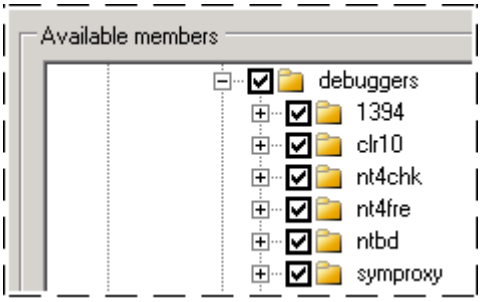
Was soll geschützt werden?

Ausschließen von Dateien und Ordnern

Sie können bei der Datenschutzkonfiguration bestimmte Ordner und auch Dateitypen anhand der Dateinamenserweiterung ausschließen.

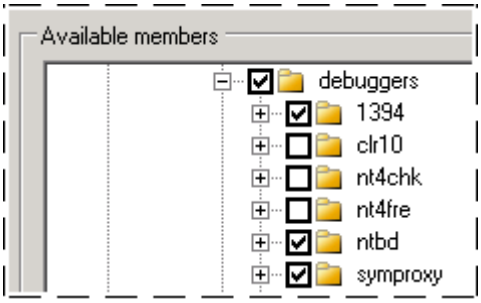
Wenn Sie ein Volume oder eine Freigabe für den Schutz auswählen, werden alle schützbaren untergeordneten Elemente dieses Volumes bzw. dieser Freigabe automatisch ebenfalls ausgewählt, wie in der folgenden Abbildung dargestellt.

Alle untergeordneten Elemente werden automatisch ausgewählt



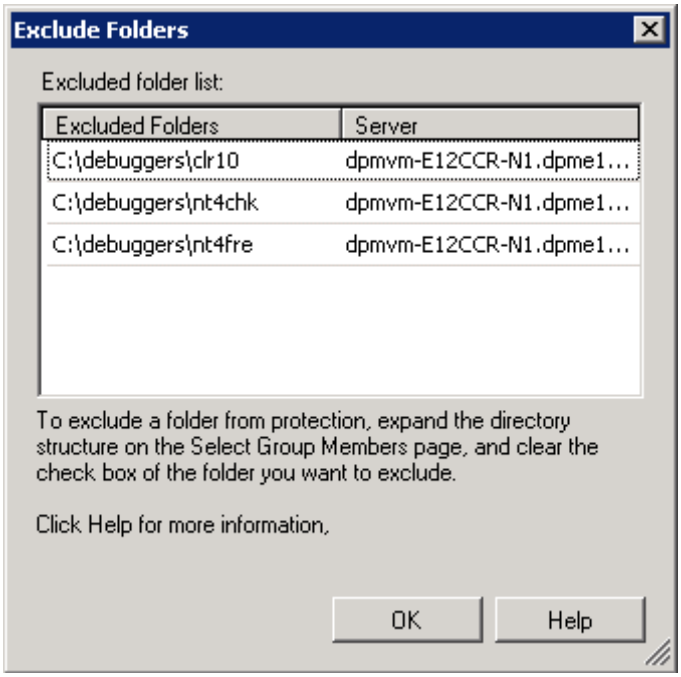
Wenn Sie bestimmte Ordner vom Schutz ausschließen möchten, wählen Sie den übergeordneten Ordner des nicht zu schützenden Ordners aus und entfernen dann die Markierung aus dem Kontrollkästchen für den Ordner, der nicht geschützt werden soll. Dies ist in der folgenden Abbildung zu sehen.

Vom Schutz ausgeschlossener Ordner



Nachdem Sie die Mitglieder für die Schutzgruppe ausgewählt haben, können Sie die ausgeschlossenen Ordner anzeigen, wie in der folgenden Abbildung dargestellt.

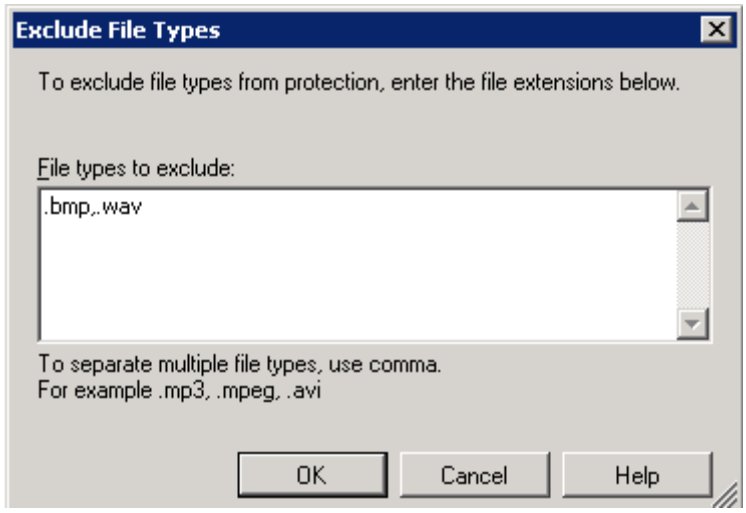
Ausgeschlossene Ordner anzeigen



Durch die Angabe der Dateinamenserweiterungen können Sie bestimmte Dateitypen innerhalb der Schutzgruppe vom Schutz ausschließen. So kann ein Dateiserver zum Beispiel Musikdateien oder private Dateien enthalten, deren Schutz im Unternehmen keinen Festplattenspeicherplatz oder Netzwerkbandbreite belegen soll. Der Ausschluss anhand der Dateinamenserweiterung gilt für alle Mitglieder der Schutzgruppe.

In der folgenden Abbildung ist der Ausschluss von Dateien anhand der Dateinamenserweiterung dargestellt.

Ausschluss anhand der Dateinamenserweiterung



Siehe auch

Schützen von Daten in DFS-Namespaces

Nicht unterstützte Datentypen

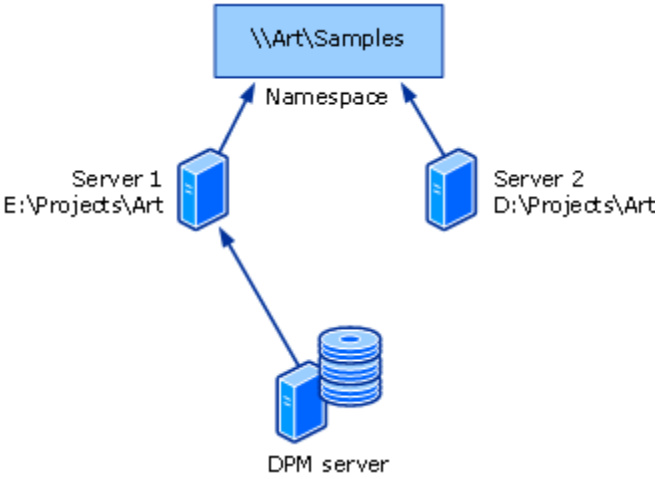
Schützen von Daten in DFS-Namespaces

Sie können Daten schützen, die Teil einer Distributed File System (DFS) Namespaces-Hierarchie sind. Es ist jedoch nicht möglich, über die DFS Namespaces-Hierarchie Freigaben für den Schutz auszuwählen. Freigaben können Sie nur über ihren Zielpfad für den Schutz auswählen.

Wenn Ihr Namespace Hauptverzeichnisse oder Links enthält, die mehrere Ziele mit denselben Daten aufweisen, wird empfohlen, nur eines der Ziele zu schützen. Mehrere Ziele mit denselben Daten zu schützen ist redundant.

In der folgenden Abbildung ist der DPM-Schutz eines DFS Namespaces-Ziels dargestellt.

DFS Namespaces-Ziel mit DPM schützen



Wenn die Endbenutzerwiederherstellung für ein geschütztes Ziel aktiviert ist, haben Benutzer über die DFS Namespaces-Hierarchie Zugriff auf frühere Dateiversionen. Versucht ein Endbenutzer, auf frühere Dateiversionen in einer Freigabe, die mehrere Ziele hat, zuzugreifen, leitet DPM ihn zum geschützten Ziel.

Siehe auch

Ausschließen von Dateien und Ordnern

Nicht unterstützte Datentypen

Nicht unterstützte Datentypen

Wenn eine geschützte Datenquelle einen nicht unterstützten Datentyp enthält, schützt DPM die unterstützten Dateitypen in der betroffenen Datenquelle. Die nicht unterstützten Dateitypen können nicht geschützt werden.

Wenn DPM einen der folgenden nicht unterstützten Dateitypen in einer geschützten Datenquelle erkennt, werden die betroffenen Daten nicht geschützt:

- Harte Links
- Analysepunkte, darunter DFS-Links und Abzweigungspunkte

  Wichtig

  Eine Schutzgruppe kann Daten mit Bereitstellungspunkten enthalten. Wenn Bereitstellungspunkte in einer Schutzgruppe enthalten sind, schützt DPM das bereitgestellte Volume, welches das Ziel des Bereitstellungspunkts ist; die Bereitstellungspunkt-Metadaten werden jedoch nicht geschützt. Beim Wiederherstellen von Daten, die Bereitstellungspunkte enthalten, müssen Sie Ihre Bereitstellungspunkthierarchie manuell neu erstellen. DPM unterstützt nicht den Schutz von bereitgestellten Volumes innerhalb von bereitgestellten Volumes.
- Papierkorb
- Auslagerungsdateien
- Informationsordner des Systemvolumes

  Hinweis

  Der Ordner „System Volume Information“ kann nicht als Dateidatenquelle geschützt werden. Um Systeminformationen für einen Computer zu schützen, müssen Sie den Systemstatus des Computers im Assistenten für das Erstellen neuer Schutzgruppenmitglieder als Schutzgruppenmitglied auswählen.
- Volumes, die nicht NTFS-formatiert sind

Wenn eine Datei feste Verknüpfungen oder symbolische Verknüpfungen von Windows Vista enthält, kann DPM keine Replikate der Dateien erstellen und die Dateien nicht wiederherstellen.

DPM kann keine Dateien schützen, die eine der folgenden Kombinationen aus Dateiattributen aufweisen:

- Verschlüsselung und Analyse
- Verschlüsselung und Single Instance Storage (SIS)
- Verschlüsselung und Groß-/Kleinschreibung beachten
- Verschlüsselung und geringe Datendichte
- Groß-/Kleinschreibung beachten und SIS
- Geringe Datendichte und Analyse
- Komprimierung und SIS

Siehe auch

Ausschließen von Dateien und Ordnern

Schützen von Daten in DFS-Namespaces

Anwendungsdaten

Mit DPM können Sie die folgenden Typen von Anwendungsdaten schützen:

- **Exchange Server-Speichergruppen.** DPM kann Speichergruppen für Microsoft Exchange Server 2003 SP2 und Exchange Server 2007 schützen.
  - Sie können Datenbanken in der ausgewählten Speichergruppe nicht vom Schutz ausschließen.
  - Alle Speichergruppen auf einem Computer mit Exchange Server 2003 müssen Mitglieder derselben Schutzgruppe sein, andernfalls werden diese Speichergruppen nicht geschützt.
  - Sie sollten die zirkuläre Protokollierung für geschützte Speichergruppen deaktivieren.
- **SQL Server-Datenbanken.** DPM kann Datenbanken für Microsoft SQL Server 2000 SP4, SQL Server 2005 SP1 und SQL Server 2005 SP2 schützen.
  - Alle Datenbanken in einer Instanz von SQL Server können zu derselben oder zu verschiedenen Schutzgruppen gehören.
  - Sie können Daten in der ausgewählten Datenbank nicht vom Schutz ausschließen.
- DPM unterstützt keine inkrementellen Sicherungen für die folgenden Datenbanken:
  - SQL Server 2000 und SQL Server 2005 master-Datenbanken
  - SQL Server 2000 msdb-Datenbank
  - SQL Server 2000 model-Datenbank
- **Windows SharePoint Services-Daten.** DPM kann Serverfarmen für Server, auf denen Windows SharePoint Services 3.0 oder Office SharePoint Server 2007 ausgeführt wird, schützen.
  - Sie können Daten in der ausgewählten Farm nicht vom Schutz ausschließen.
- **Virtual Server und virtuelle Rechner.** DPM kann einen Virtual Server-Host (einen Computer, auf dem Virtual Server 2005 R2 SP1 ausgeführt wird) und die *Gäste*, oder virtuellen Rechner, die im Kontext dieses Hosts ausgeführt werden, schützen.

Zusätzlich kann DPM die Daten der auf den virtuellen Rechnern ausgeführten Anwendungen schützen. Daten für Anwendungen, die auf virtuellen Rechnern ausgeführt werden, müssen jedoch als Anwendungsdatenquelle geschützt und wiederhergestellt werden, nicht als Komponente eines geschützten virtuellen Rechners. Um zum Beispiel Daten für eine Instanz von SQL Server, die auf einem virtuellen Rechner ausgeführt wird, zu schützen und wiederherzustellen, wählen Sie die Datenquelle als eine SQL Server-Datenbank aus. Wenn Sie einen virtuellen Rechner schützen, werden auch Anwendungsdaten geschützt. Diese können jedoch nur durch eine Wiederherstellung des virtuellen Rechners wiederhergestellt werden.

Siehe auch

Clusterressourcen

Dateidaten auf Servern und Arbeitsstationen

Systemstatus

Clusterressourcen

DPM kann freigegeben Festplattencluster für Folgendes schützen:

- Dateiserver
- SQL Server 2000 mit Service Pack 4 (SP4)
- SQL Server 2005 mit Service Pack 1 (SP1)
- Exchange Server 2003 mit Service Pack 2 (SP2)
- Exchange Server 2007

DPM kann nicht freigegebene Festplattencluster für Exchange Server 2007 schützen (cluster-kontinuierliche Replizierung). DPM kann auch Exchange Server 2007 schützen, wenn die lokale kontinuierliche Replizierung konfiguriert wurde.

Siehe auch

Anwendungsdaten

Dateidaten auf Servern und Arbeitsstationen

Systemstatus

Systemstatus

DPM kann den Status für jeden beliebigen Computer, auf dem ein DPM-Schutz-Agent installiert werden kann, schützen; ausgenommen sind allerdings Computer mit dem Betriebssystem Windows Vista oder Windows Server 2008.

Arbeitsstations- und Mitgliedsserver-Systemstatus

Wenn DPM den Systemstatus einer Arbeitsstation oder eines Mitgliedsservers sichert, werden die folgenden Komponenten geschützt:

- Die Startdateien
- COM+-Klassenregistrierungsdatenbank
- Die Registry
- Systemdateien unter Windows-Dateischutz

Domänencontroller-Systemstatus

Wenn DPM den Systemstatus eines Domänencontrollers sichert, werden die folgenden Komponenten geschützt:

- Active Directory-Domänendienste (NTDS)
- Die Startdateien
- COM+-Klassenregistrierungsdatenbank
- Die Registry
- Das Systemvolume (SYSVOL)

Zertifikatdienste-Systemstatus

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.

Clusterserver-Systemstatus

Wenn DPM den Systemstatus eines Clusterservers sichert, werden zusätzlich zu den Systemstatuskomponenten der Mitgliedsserver auch die Clusterservice-Metadaten geschützt.

Siehe auch

Anwendungsdaten

Clusterressourcen

Dateidaten auf Servern und Arbeitsstationen

Welches sind die Ziele bei der Wiederherstellung?

Beim Planen des Datenschutzes müssen Sie realistische Wiederherstellungsziele für alle zu schützenden Daten festlegen. Nicht alle Informationen oder Daten, die auf den Unternehmensrechnern vorhanden sind, müssen gleich stark geschützt werden, und nicht für alle lohnt sich dieselbe Investition für Schutzmaßnahmen. Ihr Bereitstellungsplan sollte für jede Datenquelle Wiederherstellungsziele bestimmen, die den Geschäftsanforderungen für diese Daten entsprechen.

In DPM setzen Sie Wiederherstellungsziele anhand der *Synchronisierungsfrequenz*, des *Wiederherstellungspunkt-Zeitplans* und des *Aufbewahrungszeitraums* wie folgt:

- Die Synchronisierungsfrequenz sollte an Ihre *Datenverlusttoleranz* angepasst sein. Sie können festlegen, dass eine Schutzgruppe alle 15 Minuten synchronisiert wird. Die Synchronisierung muss jedoch nicht so oft stattfinden. DPM muss die Replikate für eine Schutzgruppe mindestens ein Mal zwischen zwei Wiederherstellungspunkten synchronisieren.
- Der Wiederherstellungspunkt-Zeitplan legt fest, wie viele Wiederherstellungspunkte dieser Daten erstellt werden, und wann dies geschieht. Ein Wiederherstellungspunkt ist das Datum und die Uhrzeit einer Version einer Datenquelle, die für die Wiederherstellung von Medien, die von DPM verwaltet werden, zur Verfügung steht.
- Der Aufbewahrungszeitraum ist der Zeitraum, über den die gesicherten Daten verfügbar sein müssen. Um Ihre Anforderungen für den Aufbewahrungszeitraum zu bestimmen, berücksichtigen Sie die Wiederherstellungsanforderungen, die in der Vergangenheit in Ihrem Unternehmen aufgetreten sind. Wenn Wiederherstellungen normalerweise innerhalb von zwei Wochen nach einem Datenverlust angefordert werden, könnte ein Aufbewahrungszeitraum von 10 Tagen für Sie geeignet sein. Wenn sich Wiederherstellungsanforderungen nach einem längeren Zeitraum häufen, benötigen Sie wahrscheinlich einen längeren Aufbewahrungszeitraum.

Ihre Wiederherstellungsziele für eine bestimmte Exchange Server-Datenbank könnten zum Beispiel lauten: die neuesten Daten sind nie älter als 30 Minuten, Sie können aus Versionen wählen, die in 30-minütigen Intervallen erstellt wurden, die Daten stehen 14 Tage lang für die Wiederherstellung von der Festplatte zur Verfügung, und die Daten stehen 3 Jahre lang für die Wiederherstellung vom Band zur Verfügung.

Siehe auch

Planen von Schutzkonfigurationen

Wiederherstellungsziele für festplattengestützten Schutz

Wiederherstellungsziele für bandgestützten Schutz

Was soll geschützt werden?

Wiederherstellungsziele für festplattengestützten Schutz

Auch wenn alle Mitglieder einer Schutzgruppe mit derselben Frequenz synchronisiert werden, unterscheiden sich der Synchronisierungsprozess und der resultierende Wiederherstellungspunkt-Zeitplan je nach Typ der geschützten Daten. Weitere Informationen finden Sie unter Funktionsweise von DPM.

Synchronisierung und Wiederherstellungspunkte für Dateien

Für Dateivolumes oder Freigaben verfolgt der Schutz-Agent auf dem geschützten Computer die geänderten Blöcke im Änderungsjournal, das Teil des Betriebssystems ist. Bei der Synchronisierung werden diese Änderungen an den DPM-Server übertragen und dann auf das Replikat angewendet, um das Replikat mit der Datenquelle zu synchronisieren.

Für das Intervall für Synchronisierungen können Sie zwischen 15 Minuten und 24 Stunden einstellen. Der Standardwert beträgt 15 Minuten. Sie können auch festlegen, dass die Synchronisierung nur vor dem Erstellen eines Wiederherstellungspunkts erfolgt.

Wiederherstellungspunkte, wobei es sich um Schattenkopien der Replikate von Dateidaten handelt, werden nach einem konfigurierbaren Zeitplan von den synchronisierten Replikaten erstellt. Nicht jede Synchronisierung ergibt einen Wiederherstellungspunkt, sofern Sie nicht nur vor Wiederherstellungspunkten synchronisieren, Sie können jedoch von der aktuellsten Dateisynchronisierung manuell einen Wiederherstellungspunkt erstellen.

Zum Beispiel wird ein Volume stündlich synchronisiert, und um 8:00 Uhr, um 12:00 Uhr und um 18:00 werden Wiederherstellungspunkte für das Volume erstellt. Ein Benutzer ändert um 13:30 Uhr eine Datei im Volume. Eine Stunde später nimmt ein anderer Benutzer weitere Änderungen an dieser Datei vor, und diese wird dabei versehentlich beschädigt. Nun werden Sie gebeten, die Datei mit den Änderungen des ersten Benutzers wiederherzustellen. Da die Änderungen um 13:30 Uhr nach der Erstellung des aktuellsten Wiederherstellungspunkts vorgenommen wurden, können Sie die Datei nicht vom zuletzt erstellten Wiederherstellungspunkt wiederherstellen. Sie können jedoch einen Wiederherstellungspunkt von der entsprechenden Synchronisierung dieses Replikats erstellen und die Datei dann von diesem neuen Wiederherstellungspunkt wiederherstellen.

Standardmäßig werden täglich um 8:00 Uhr, um 12:00 Uhr und um 18:00 Uhr Wiederherstellungspunkte an jedem Tag. Sie können sowohl die Uhrzeiten als auch die Tage ändern. Es ist nicht möglich, für verschiedene Tage unterschiedliche Uhrzeiten festzulegen. Sie können zum Beispiel Wiederherstellungspunkte für 2:00 Uhr und 14:00 Uhr nur an Werktagen festlegen; Sie können aber nicht Wiederherstellungspunkte für 2:00 Uhr an Werktagen und für 12:00 Uhr an Wochenenden festlegen.

Aufbewahrungszeitraum für Dateien

Der Aufbewahrungszeitraum ist der Zeitraum, über den die Daten zur Wiederherstellung zur Verfügung stehen sollen. Wenn der Aufbewahrungszeitraum für einen Wiederherstellungspunkt abgelaufen ist, wird der Wiederherstellungspunkt gelöscht.

Sie können einen Aufbewahrungszeitraum zwischen einem Tag und 448 Tagen für den kurzfristigen festplattengestützten Schutz, bis zu 12 Wochen für den kurzfristigen bandgestützten Schutz und bis zu 99 Jahre für den langfristigen bandgestützten Schutz auswählen. DPM kann bis zu 64 Wiederherstellungspunkte für jedes Dateimitglied einer Schutzgruppe speichern.

Wenn Sie zum Beispiel vor jedem Wiederherstellungspunkt eine Synchronisierung ausführen, 6 Wiederherstellungspunkte täglich einplanen und einen Aufbewahrungszeitraum von 10 Tagen festlegen, werden die Wiederherstellungspunkte für die Dateien in dieser Schutzgruppe niemals 64 überschreiten. Wenn Sie jedoch Einstellungen kombinieren, die zu mehr als 64 Wiederherstellungspunkten führen, gibt DPM während der Konfiguration eine Warnmeldung aus, damit Sie Ihre Auswahl ändern können. Es ist nicht möglich, eine Schutzkonfiguration für Dateien zu erstellen, bei der das Limit von 64 Wiederherstellungspunkten überschritten wird.

Synchronisierung und Wiederherstellungspunkte für Anwendungsdaten

Für Anwendungsdaten werden Änderungen an Volumeblöcken, die zu Anwendungsdateien gehören, vom Volumefilter verfolgt. Die Synchronisierung von Anwendungsdaten entspricht einer inkrementellen Sicherung und erstellt in Kombination mit dem Replikat ein genaues Abbild der Anwendungsdaten.

Für das Intervall für Synchronisierungen können Sie zwischen 15 Minuten und 24 Stunden einstellen. Der Standardwert beträgt 15 Minuten. Sie können auch festlegen, dass die Synchronisierung nur vor dem Erstellen eines Wiederherstellungspunkts erfolgt. Wenn Sie nur vor dem Erstellen eines Wiederherstellungspunkts synchronisieren, führt DPM eine vollständige Schnellsicherung aus, um das Replikat entsprechend des Wiederherstellungspunkt-Zeitplans zu synchronisieren.

Bei Anwendungen, die inkrementelle Sicherungen unterstützen, führt der Standardzeitplan zu Wiederherstellungspunkten für jede Synchronisierung (alle 15 Minuten) und zu einer vollständigen Schnellsicherung um 8:00 Uhr an jedem Tag. Für Anwendungen, die keine inkrementellen Sicherungen unterstützen, führt der Standardzeitplan zu einem Wiederherstellungspunkt für die vollständige Schnellsicherung um 8:00 Uhr an jedem Tag.

Sie können sowohl die Uhrzeiten als auch die Tage ändern. Es ist nicht möglich, für verschiedene Tage unterschiedliche Uhrzeiten festzulegen. Sie können zum Beispiel Wiederherstellungspunkte für 2:00 Uhr und 14:00 Uhr nur an Werktagen festlegen; Sie können aber nicht Wiederherstellungspunkte für 2:00 Uhr an Werktagen und für 12:00 Uhr an Wochenenden festlegen.

Ausnahme für einige SQL Server-Datenbanken

Sicherungen von Transaktionsprotokollen, die DPM für die inkrementelle Synchronisierung von Anwendungsdaten verwendet, können nicht für SQL Server-Datenbanken ausgeführt werden, die schreibgeschützt sind, für den Protokollversand konfiguriert sind oder das einfache Wiederherstellungsmodell verwenden. Für diese SQL Server-Datenbanken entsprechen Wiederherstellungspunkte den einzelnen vollständigen Schnellsicherungen.

Synchronisierung und vollständige Schnellsicherung im Vergleich

Um schnellere Wiederherstellungen zu ermöglichen, führt DPM regelmäßig anstelle einer inkrementellen Synchronisierung eine vollständige Schnellsicherung aus. Eine vollständige Schnellsicherung ist ein Synchronisierungstyp, bei dem das Replikat mit den geänderten Blöcken aktualisiert wird.

Hinweis

Sie können den Zeitplan für vollständige Schnellsicherungen für jede Schutzgruppe mit Anwendungsdaten ändern, indem Sie die Aktion **Leistung optimieren** im Aufgabenbereich **Schutz** oder den Assistenten zum Ändern von Gruppen verwenden.

Aufbewahrungszeitraum für Anwendungsdaten

Sie können einen Aufbewahrungszeitraum zwischen einem Tag und 448 Tagen für den kurzfristigen festplattengestützten Schutz, bis zu 12 Wochen für den kurzfristigen bandgestützten Schutz und bis zu 99 Jahre für den langfristigen bandgestützten Schutz auswählen.

Wenn Sie zum Beispiel alle 15 Minuten synchronisieren und einen Aufbewahrungszeitraum von 10 Tagen festlegen, führen diese Wiederherstellungsziele zu einem Schutzplan, der nach den ersten 10 Tagen Datenschutz 960 Wiederherstellungspunkte für Anwendungsdaten in dieser Schutzgruppe beibehält.

Siehe auch

Wiederherstellungsziele für bandgestützten Schutz

Wiederherstellungsziele für bandgestützten Schutz

DPM schützt Daten auf Band, indem eine Kombination aus vollständigen und inkrementellen Sicherungen verwendet wird, und zwar entweder von der geschützten Datenquelle (für kurzfristigen Schutz auf Band oder für langfristigen Schutz auf Band, wenn DPM die Daten nicht auf der Festplatte schützt) oder vom DPM-Replikat (für langfristigen Schutz auf Band, wenn der kurzfristige Schutz auf Festplatte erfolgt).

Die Zusammenstellung von Aufbewahrungszeitraum, Frequenz der Sicherungen und Wiederherstellungsoptionen unterscheidet sich für den kurzfristigen und langfristigen Schutz.

Hinweis

Sie können den festplattengestützten oder bandgestützten kurzfristigen Schutz wählen, aber nicht beides.

Kurzfristiger Schutz auf Band

Für den kurzfristigen Schutz auf Band können Sie einen Aufbewahrungszeitraum von 1 bis 12 Wochen wählen. DPM unterstützt die Verwaltung Ihrer Bänder mit Warnmeldungen und Berichten. Der angegebene Aufbewahrungszeitraum wird verwendet, um das Ablaufdatum der einzelnen Bänder zu ermitteln.

Abhängig vom Aufbewahrungszeitraum können Sie täglich, wöchentlich oder 14-tägig Sicherungen ausführen.

Wenn Sie den kurzfristigen Schutz auf Band unter Verwendung inkrementeller und vollständiger Sicherungen wählen, ist der Aufbewahrungszeitraum länger als der von Ihnen angegebene (maximal eine Woche länger), da zwischen vollständigen und inkrementellen Sicherungen Abhängigkeiten bestehen. Bänder mit vollständigen Sicherungen werden erst dann recycelt, nachdem alle davon abhängigen inkrementellen Bänder recycelt wurden. Weil vollständige Sicherungen wöchentlich ausgeführt werden und die inkrementellen täglich, muss das Band mit der wöchentlichen vollständigen Sicherung auf das Recycling der sechs Bänder mit täglichen inkrementellen Sicherungen warten, bis das vollständige Sicherungsband recycelt wird. Wenn eine inkrementelle Sicherung fehlschlägt und kein inkrementelles Band recycelt werden kann, wird das Band mit der vollständigen Sicherung eher recycelt.

Langfristiger Schutz auf Band

Für den langfristigen Schutz von Daten, auch als Bandarchivierung bezeichnet, können Sie einen Aufbewahrungszeitraum zwischen einer Woche und 99 Jahren wählen. DPM unterstützt die Verwaltung Ihrer Bandarchive mit Warnmeldungen und Berichten. Der angegebene Aufbewahrungszeitraum wird verwendet, um das Ablaufdatum der einzelnen Bänder zu ermitteln.

Die Frequenz der Sicherungen basiert auf dem festgelegten Aufbewahrungszeitraum, wie aus der folgenden Liste ersichtlich ist:

- Wenn der Aufbewahrungszeitraum ein Jahr bis 99 Jahre lang ist, können Sie wählen, ob Sicherungen täglich, wöchentlich, 14-tägig, monatlich, vierteljährlich, halbjährlich oder jährlich ausgeführt werden sollen.
- Wenn der Aufbewahrungszeitraum 1 bis 11 Monate lang ist, können Sie wählen, ob Sicherungen täglich, wöchentlich, 14-tägig oder monatlich ausgeführt werden sollen.
- Wenn der Aufbewahrungszeitraum 1 bis 4 Wochen lang ist, können Sie wählen, ob Sicherungen täglich oder wöchentlich ausgeführt werden sollen.

Siehe auch

Wiederherstellungsziele für festplattengestützten Schutz

Planen von Schutzkonfigurationen

Nachdem Sie die Datenquellen, die Sie schützen müssen, identifiziert und Ihre Wiederherstellungsziele bestimmt haben, ist der nächste Schritt die Analyse der Informationen, die Sie gesammelt haben, damit Sie die Datenquellen in Schutzgruppen organisieren können.

Eine *Schutzgruppe* ist eine Sammlung von Datenquellen, für die dieselbe Schutzkonfiguration eingerichtet wurde. Die *Schutzkonfiguration* besteht aus dem Schutzgruppennamen und den Einstellungen für Festplattenzuweisungen, Replikaterstellungsmethoden und Komprimierung über das Netzwerk.

Zur Planung einer Schutzgruppe müssen Sie folgenden Entscheidungen treffen:

- Welche Datenquellen gehören zu der Schutzgruppe?
- Welche Schutzmethode (festplattengestützt, bandgestützt oder beides) werden Sie für die Schutzgruppe verwenden?
- Wie lauten die Wiederherstellungsziele für die Mitglieder der Schutzgruppe?
- Wie viel Speicherplatz wird benötigt, um die ausgewählten Daten zu schützen?
- Welches Band und welche Bibliothek soll verwendet werden?
- Welche Methode wird zum Erstellen der Replikate für die Mitglieder der Schutzgruppe verwendet?

Die Themen in diesem Abschnitt enthalten Richtlinien für die Entscheidungen, die beim Erstellen einer Schutzgruppe getroffen werden müssen.

In diesem Abschnitt

Siehe auch

Auswählen von Schutzgruppenmitgliedern

Mit Data Protection Manager (DPM) 2007 stehen Ihnen verschiedene Ansätze zur Verfügung, um die Datenquellen in Schutzgruppen zu organisieren, darunter folgende:

- **Nach Computer**, wobei alle Datenquellen für einen Computer zu derselben Schutzgruppe gehören.
  - Ein Vorteil bei diesem Ansatz besteht darin, dass Sie einen gemeinsamen Einstellungspunkt für Leistungslasten haben.
  - Eine Einschränkung ist dagegen, dass für alle Datenquellen eines Typs auf dem Computer dieselben Wiederherstellungsziele zugewiesen werden müssen.
- **Nach Datentyp**, wobei Dateien und die einzelnen Anwendungsdatentypen unterschiedlichen Schutzgruppen zugeteilt werden.
  - Dieser Ansatz hat den Vorteil, dass Sie Datentypen als Gruppe verwalten können.
  - Eine Einschränkung ist dagegen, dass für das Wiederherstellen eines Servers möglicherweise mehrere Bänder aus verschiedenen Schutzgruppen benötigt werden.

Definitionsgemäß haben alle Mitglieder einer Schutzgruppe dieselben Wiederherstellungsziele, was bedeutet, das für alle Datenquellen eines Typs in einer Schutzgruppe derselbe Aufbewahrungszeitraum und dieselbe Datenverlusttoleranz gilt.

Wenn Sie nur ein eigenständiges Bandlaufwerk haben, verwenden Sie eine einzelne Schutzgruppe, um die Anzahl der Bandwechsel gering zu halten. Bei mehreren Schutzgruppen wird ein separates Band für jede Schutzgruppe benötigt.

Richtlinien für Schutzgruppen

Berücksichtigen Sie beim Planen der Struktur Ihrer Schutzgruppen die folgenden Richtlinien und Einschränkungen:

- Datenquellen auf einem Computer müssen von demselben DPM-Server geschützt werden. In DPM ist eine Datenquelle ein Volume, eine Freigabe, eine Datenbank oder eine Speichergruppe, die Mitglied einer Schutzgruppe ist.
- Sie können Datenquellen von mehreren Computern in einer Schutzgruppe zusammenfassen.
- Wenn Sie einen übergeordneten Order bzw. eine übergeordnete Freigabe auswählen, werden die untergeordneten Ordner automatisch mit ausgewählt. Sie können bestimmte Unterordner oder Dateitypen anhand der Dateierweiterung vom Schutz ausschließen.
- Überprüfen Sie, dass sich nicht mehr als 100 zu schützende Datenquellen auf einem Volume befinden. Verteilen Sie Ihre Datenquellen ggf. auf mehrere Volumes.
- Alle Schutzgruppenmitglieder desselben Typs (Dateidaten oder Anwendungsdaten) haben dieselben Wiederherstellungsziele. Innerhalb einer Schutzgruppe können Dateien jedoch andere Wiederherstellungsziele als Anwendungsdaten haben.

  Ausnahme: Wenn eine SQL Server-Datenbank für die Verwendung des einfachen Wiederherstellungsmodells konfiguriert wurde oder die primäre Datenbank in einem Protokollversandpaar ist, werden die Wiederherstellungsziele für diese Datenbank getrennt von den Wiederherstellungszielen aller anderen Anwendungsdaten konfiguriert.
- Alle Speichergruppen auf einem Computer, auf dem Exchange Server 2003 ausgeführt wird, müssen Mitglieder derselben Schutzgruppe sein.
- Wenn Sie eine Datenquelle auswählen, die einen Analysepunkte enthält (Bereitstellungspunkte und Abzweigungspunkte sind Datenquellen mit Analysepunkten), fordert DPM Sie auf, festzulegen, ob Sie das Ziel des Analysepunkts in die Schutzgruppe einschließen möchten. Der Analysepunkt selbst wird nicht repliziert; Sie müssen den Analysepunkt beim Wiederherstellen der Daten manuell neu erstellen.

Besondere Überlegungen für den Datenschutz auf Arbeitsstationen

Ihre Wiederherstellungsziele für Daten auf Benutzerarbeitsstationen unterscheiden sich möglicherweise von den Wiederherstellungszielen für Daten auf Dateiservern. Sie sollten in Erwägung ziehen, Dateiserver und Arbeitsstationen in separaten Schutzgruppen zu organisieren, damit Sie die Synchronisierungszeitpläne getrennt konfigurieren können. Wenn Sie zum Beispiel Daten auf Dateiservern alle 15 Minuten synchronisieren, werden auch alle Arbeitsstationen, die zu derselben Schutzgruppe wie die Dateiserver gehören, alle 15 Minuten synchronisiert.

Besondere Überlegungen für den Datenschutz über ein WAN

Netzwerkbandbreiten-Nutzungsdrosselung und Komprimierung über das Netzwerk sind Funktionen zur Leistungsoptimierung, die wichtig sind für Bereitstellungen, in denen ein DPM-Server Daten über ein WAN (Wide Area Network) oder ein anderes langsames Netzwerk schützt.

Die Komprimierung über das Netzwerk wird auf der Schutzgruppenebene konfiguriert.

Die Drosselung der Netzwerkbandbreitennutzung wird auf der Ebene des geschützten Computers konfiguriert. Zusätzlich können Sie unterschiedliche Drosselungsraten für die Netzwerkbandbreitennutzung für Arbeitszeiten, arbeitsfreie Zeiten und Wochenenden festlegen, und Sie definieren die Zeiten für jede dieser Kategorien.

Wenn Sie Anwendungsdaten wie Exchange-Speichergruppen oder SQL Server-Datenbanken über ein WAN schützen, ziehen Sie in Betracht, die Frequenz der vollständigen Schnellsicherungen zu verringern.

Wie wichtig ist die Auswahl der Schutzgruppenmitglieder?

Schutzgruppenmitglieder können nicht zwischen Schutzgruppen verschoben werden. Wenn Sie feststellen, dass ein Schutzgruppenmitglied sich in einer anderen Schutzgruppe befinden sollte als ursprünglich vorgesehen, müssen Sie das Mitglied aus der Schutzgruppe entfernen und dann einer anderen Schutzgruppe hinzufügen.

Sollten die Mitglieder einer Schutzgruppe keinen Schutz mehr benötigen, können Sie den Schutz der Schutzgruppe beenden. Wenn Sie den Schutz beenden, können Sie die geschützten Daten beibehalten oder löschen.

- **Daten beibehalten**: Mit dieser Option werden die Replikate auf Festplatte mit den zugeordneten Wiederherstellungspunkten und auf Band für den festgelegten Aufbewahrungszeitraum beibehalten.
- **Daten löschen**: Mit dieser Option wird das Replikat auf Festplatte gelöscht, und die Daten auf Bändern erreichen ihr Ablaufdatum.

Siehe auch

Planen von Schutzkonfigurationen

Auswählen einer Datenschutzmethode

Data Protection Manager (DPM) 2007 bietet die folgenden Methoden für den Schutz von Daten: festplattengestützt (D2D), bandgestützt (D2T) oder eine Kombination aus festplattengestützt und bandgestützt (D2D2T).

Die Datenschutzmethode wird auf Schutzgruppenebene konfiguriert. Wenn Sie zwei verschiedene Methoden für den Schutz von zwei Datenquellen verwenden möchten, dürfen die Datenquellen nicht zu derselben Schutzgruppe gehören.

In der folgenden Tabelle sind die Vorteile und Nachteile der einzelnen Methoden aufgeführt.

Vergleich der Datenschutzmethoden

Methode	Vorteile	Nachteile	Verwendung
Nur festplatten-gestützter Schutz	• Schnelle Wiederher-stellung der Daten. • Schnelle Sicherung der Daten. • Die Fehlerwahr-scheinlichkeit bei Sicherungen ist geringer. • Möglichkeit der Redundanz, z. B. durch RAID, um mit Ausfällen umzugehen. • Geringerer Bedienungs-aufwand (kein Wechseln der Bänder).	• Festplatten sind keine einfache Lösung für die Archivierung, da Festplatten teuer sind und die externe Aufbewahrung unpraktisch ist.	• Bei eingeschränkter Datenverlust-toleranz. • Wenn schnellere Wiederherstellungsz eiten erforderlich sind.

Methode	Vorteile	Nachteile	Verwendung
Nur bandgestützter Schutz	• Externe Aufbewahrung aus Gründen der Sicherheit und als Quelle für die Wiederherstellung im Notfall. • Kapazität kann durch Hinzufügen von Bändern unkompliziert erweitert werden.	• Wiederherstellungsprozess ist langsamer und aufwändiger. • Höhere Fehlerwahrscheinlichkeit.	• Bei höherer Datenverlusttoleranz. • Wenn die Dauer der Wiederherstellung nicht so wichtig ist. • Für Daten, die seltener geändert werden und nicht so häufig gesichert werden müssen. • Für lange Aufbewahrungszeiträume.
Festplattengestützter und bandgestützter Schutz	• Kombinierte Vorteile wie oben, während die Nachteile der verschiedenen Methoden ausgeglichen werden. • Eine gemeinsame Basis für die Verwaltung.		

Siehe auch

Planen von Schutzkonfigurationen

Definieren von Wiederherstellungszielen

Nachdem Sie die Mitglieder einer DPM-Schutzgruppe und die Methoden für den Schutz der Daten ausgewählt haben, definieren Sie die Wiederherstellungsziele für die Datendateien und die Anwendungsdateien in dieser Schutzgruppe.

Die Wiederherstellungsziele werden durch die Konfiguration des Aufbewahrungszeitraums, der Synchronisierungsfrequenz und des Wiederherstellungspunkt-Zeitplans bestimmt. DPM bietet Standardeinstellungen für die Wiederherstellungsziele, Sie können diese Einstellungen jedoch ändern.

Zwischen zwei geplanten Wiederherstellungspunkten muss wenigstens eine Synchronisierung eingeplant werden. Angenommen, Sie legen eine Synchronisierungsfrequenz von 45 Minuten fest. In diesem Fall ist es nicht möglich, Wiederherstellungspunkte um 13:00 Uhr und um 13:30 Uhr zu erstellen, da zwischen diesen Wiederherstellungspunkte keine Synchronisierung erfolgt.

Wenn ein SQL Server für die Verwendung des einfachen Wiederherstellungsmodells konfiguriert wurde oder der primäre Server in einem Protokollversandpaar ist, werden die Wiederherstellungspunkte für geschützte Datenbanken auf diesem Server gemäß dem Zeitplan für vollständige Schnellsicherungen erstellt.

Unter den folgenden Überschriften in diesem Abschnitt finden Sie ausführliche Informationen, die Ihnen beim Planen der Wiederherstellungsziele helfen können:

- Optionen für Wiederherstellungsziele für die einzelnen Schutzmethoden
- Wiederherstellungspunkt-Zeitpläne für langfristigen Schutz
- Planungsoptionen für langfristigen Schutz
- Anpassen von Wiederherstellungszielen für langfristigen Schutz

Siehe auch

Planen von Schutzkonfigurationen

Optionen für Wiederherstellungsziele für die einzelnen Schutzmethoden

In der folgenden Tabelle sind die Optionen für Wiederherstellungsziele für die einzelnen DPM-Schutzmethoden aufgeführt.

Optionen für Wiederherstellungsziele für Schutzmethoden

Schutzmethode	Aufbewahrungs-zeitraum	Synchronisierungs-frequenz oder Sicherungszeitplan	Wiederherstellungspunkte
Kurzfristig auf Festplatte	1–448 Tage	Wählen Sie eine Frequenz zwischen 15 Minuten und 24 Stunden, oder wählen Sie die Option **Just before a recovery point**, mit der jeweils vor einem Wiederherstellungspunkt synchronisiert wird.	Bei Auswahl einer bestimmten Synchronisierungsfrequenz: • Wiederherstellungspunkte für Dateien werden entsprechend des konfigurierten Zeitplans erstellt. • Wiederherstellungspunkte für Anwendungsdaten werden nach jeder Synchronisierung erstellt. Bei Auswahl der Option zum Synchronisieren vor dem Erstellen von Wiederherstellungspunkten (**Just before a recovery point**) werden Wiederherstellungspunkte für alle Schutzgruppenmitglieder entsprechend dem konfigurierten Zeitplan erstellt.

Schutzmethode	Aufbewahrungs-zeitraum	Synchronisierungs-frequenz oder Sicherungszeitplan	Wiederherstellungspunkte
Kurzfristig auf Band	1–12 Wochen	Wählen Sie die Frequenz der Sicherungen: • Täglich • Wöchentlich • 14-tägig	Anstelle von Wieder-herstellungspunkten konfigurieren Sie einen der folgenden Sicherungstypen: • Vollständige und inkrementelle Sicherungen • Nur vollständige Sicherungen Wenn Sie die wöchentliche oder 14-tägige Sicherung wählen, sind nur vollständige Sicherungen möglich. Sie legen Tag und Uhrzeit fest. Wenn Sie täglich eine vollständige Sicherung ausführen, legen Sie die Uhrzeit fest. Wenn Sie täglich vollständige und inkrementelle Sicherungen ausführen, legen Sie den Tag und die Uhrzeit für die vollständige und für die inkrementelle Sicherung fest.
Langfristig auf Band	Mindestens 1 Woche Höchstens 99 Jahre	Wählen Sie die Frequenz der Sicherungen: • Täglich • Wöchentlich • 14-tägig • Monatlich • Vierteljährlich • Halbjährlich • Jährlich	Siehe Wiederherstellungspunkt-Zeitpläne für langfristigen Schutz und Anpassen von Wiederherstellungszielen für langfristigen Schutz.

Siehe auch

Definieren von Wiederherstellungszielen

Wiederherstellungspunkt-Zeitpläne für langfristigen Schutz

In der folgenden Tabelle sind die DPM-Wiederherstellungspunkt-Zeitpläne für die verschiedenen Kombinationen für langfristigen Schutz aufgeführt.

Wiederherstellungspunkt-Zeitpläne für langfristigen Schutz

Sicherungsfrequenz und Aufbewahrungszeitraum	Wiederherstellungspunkt-Zeitplan
Täglich, 1–4 Wochen	Vollständige Sicherung täglich
Täglich, 1–11 Monate	1 vollständige Sicherung täglich, vier Wochen lang 1 vollständige Sicherung pro Monat nach den ersten 4 Wochen
Täglich, 1–99 Jahre	1 vollständige Sicherung täglich, vier Wochen lang 1 vollständige Sicherung pro Monat nach den ersten 4 Wochen bis zum 12. Monat 1 vollständige Sicherung pro Jahr nach den ersten 11 Monaten
Wöchentlich, 1–4 Wochen	Vollständige Sicherung wöchentlich
Wöchentlich, 1–11 Monate	1 vollständige Sicherung wöchentlich, vier Wochen lang 1 vollständige Sicherung pro Monat nach den ersten 4 Wochen
Wöchentlich, 1–99 Jahre	1 vollständige Sicherung wöchentlich, vier Wochen lang 1 vollständige Sicherung pro Monat nach den ersten 4 Wochen bis zum 12. Monat 1 vollständige Sicherung pro Jahr nach den ersten 11 Monaten

Sicherungsfrequenz und Aufbewahrungszeitraum	Wiederherstellungspunkt-Zeitplan
14-tägig, 1–11 Monate	1 vollständige Sicherung alle zwei Wochen, vier Wochen lang 1 vollständige Sicherung pro Monat nach den ersten 4 Wochen
14-tägig, 1–99 Jahre	1 vollständige Sicherung alle zwei Wochen, vier Wochen lang 1 vollständige Sicherung pro Monat nach den ersten 4 Wochen bis zum 12. Monat 1 vollständige Sicherung pro Jahr nach den ersten 11 Monaten
Monatlich, 1–11 Monate	Vollständige Sicherung monatlich
Monatlich, 1–99 Jahre	1 vollständige Sicherung pro Monat bis zum 12. Monat 1 vollständige Sicherung pro Jahr nach den ersten 11 Monaten
Vierteljährlich, 1–99 Jahre	1 vollständige Sicherung alle 3 Monate bis zum 12. Monat 1 vollständige Sicherung pro Jahr nach den ersten 11 Monaten
Halbjährlich, 1–99 Jahre	1 vollständige Sicherung alle 6 Monate bis zum 12. Monat 1 vollständige Sicherung pro Jahr nach den ersten 11 Monaten
Jährlich, 1–99 Jahre	Vollständige Sicherung jährlich

Siehe auch

Definieren von Wiederherstellungszielen

Planungsoptionen für langfristigen Schutz

In der folgenden Tabelle sind die Planungsoptionen aufgeführt, die Sie für den langfristigen Schutz mit DPM ändern können.

Planungsoptionen für langfristigen Schutz

Sicherungsfrequenz	Mögliche Konfiguration je nach Aufbewahrungszeitraum
Täglich	• Uhrzeit der täglichen Sicherung • Bestimmter Tag oder Wochentag und Uhrzeit der monatlichen Sicherung • Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung
Wöchentlich	• Uhrzeit und Wochentag der wöchentlichen Sicherung • Bestimmter Tag oder Wochentag und Uhrzeit der monatlichen Sicherung • Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung
14-tägig	• Uhrzeit und Wochentag der 14-tägigen Sicherung • Bestimmter Tag oder Wochentag und Uhrzeit der monatlichen Sicherung • Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung
Monatlich	• Bestimmter Tag oder Wochentag und Uhrzeit der monatlichen Sicherung • Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung
Vierteljährlich	• Uhrzeit und Datum der vierteljährlichen Sicherung (Vierteljährliche Sicherungen werden im Januar, April, Juli und Oktober am angegebenen Tag ausgeführt.) • Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung
Halbjährlich	• Uhrzeit, bestimmter Tag oder Datum sowie Monate der halbjährlichen Sicherung • Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung
Jährlich	• Bestimmter Tag oder Datum und Uhrzeit der jährlichen Sicherung

Siehe auch

Definieren von Wiederherstellungszielen

Anpassen von Wiederherstellungszielen für langfristigen Schutz

Wenn Sie einen Aufbewahrungszeitraum und eine Sicherungsfrequenz angegeben, generiert DPM einen Zeitplan für die Sicherungsaufträge. (Weitere Informationen finden Sie unter Wiederherstellungspunkt-Zeitpläne für langfristigen Schutz.) Sie können den Zeitplan der Sicherungsaufträge bei Bedarf an Ihre Wiederherstellungsziele anpassen, um den Standardzeitplan zu ersetzen.

Wenn Sie den Zeitplan der Sicherungsaufträge für eine Schutzgruppe anpassen, geben Sie ein Wiederherstellungsziel für jedes Sicherungsintervall an. Folgende Optionen stehen als Intervall für die Sicherungsfrequenz zur Verfügung:

- Täglich
- Wöchentlich
- Monatlich
- Jährlich

Sie können ein Wiederherstellungsziel für bis zu drei Sicherungsfrequenzintervalle festlegen. Für jedes Sicherungsfrequenzintervall geben Sie den Aufbewahrungszeitraum für das Band, die Anzahl der Kopien, die vom Band erstellt werden sollen, sowie die Bandbezeichnung ein.

Indem Sie die Wiederherstellungsziele für eine Schutzgruppe anpassen, können Sie zum Beispiel Sicherungen für den folgenden Zeitplan konfigurieren:

- Eine Kopie wöchentlicher Sicherungen, die zwei Wochen aufbewahrt wird
- Zwei Kopien monatlicher Sicherungen, die sechs Monate aufbewahrt werden
- Eine Kopie der jährlichen Sicherung, die fünf Jahre aufbewahrt wird

Siehe auch

Planen von Schutzkonfigurationen

Zuweisen von Speicherplatz für Schutzgruppen

Wenn Sie eine Schutzgruppe erstellen und den festplattengestützten Schutz auswählen, müssen Sie im Speicherpool Speicherplatz für Replikate und Wiederherstellungspunkte für jede Datenquelle, die in dieser Schutzgruppe enthalten ist, zuweisen. Außerdem müssen Sie auf den geschützten Dateiservern oder Arbeitsstationen Speicherplatz für das Änderungsjournal zuweisen.

DPM stellt Standardeinstellungen für die Speicherplatzzuweisungen für die Mitglieder der Schutzgruppe zur Verfügung. In der folgenden Tabelle ist dargestellt, wie DPM die Standardzuweisungen berechnet.

Berechnung der DPM-Standard-Speicherplatzzuweisungen

Komponente	Standardzuweisung	Speicherort
Replikatvolume	Für Dateien: • (Größe der Datenquelle x 3) / 2 Für Exchange-Daten: • Größe der Datenquelle x (1 + Protokolländerungen) / (Warnschwellenwert - 0,05) Für SQL Server-Daten: • Größe der Datenquelle x (1 + Protokolländerungen) / (Warnschwellenwert - 0,05) Für Windows SharePoint Services-Daten: • Gesamtgröße aller Datenbanken/ (Warnschwellenwert - 0,05) Für Virtual Server-Daten: • Größe der Datenquelle x 1,5 Für den Systemstatus: • (Größe der Datenquelle x 3) / 2	DPM-Speicherpool oder benutzerdefiniertes Volume

Komponente	Standardzuweisung	Speicherort
Wiederherstellungs-punktvolume	Für Dateien: • (Größe der Datenquelle x Aufbewahrungszeitraum in Tagen x 2) / 100 + 1600 MB Für Exchange-Daten: • 4,0 x Aufbewahrungszeitraum in Tagen x Protokolländerungen x Größe der Datenquelle + 1600 MB Für SQL Server-Daten: • 2,5 x Aufbewahrungszeitraum in Tagen x Protokolländerungen x Größe der Datenquelle + 1600 MB Für Windows SharePoint Services-Daten: • 1,5 x Aufbewahrungszeitraum in Tagen x Protokolländerungen x Gesamtgröße aller Datenbanken + 1600 MB Für Virtual Server-Daten: • (Größe der Datenquelle x Aufbewahrungszeitraum in Tagen x 0,02) + 1600 MB Für den Systemstatus: • (Größe der Datenquelle x Aufbewahrungszeitraum in Tagen x 2) / 100 + 1600 MB	DPM-Speicherpool oder benutzerdefiniertes Volume
Änderungsjournal (nur für Dateischutz)	300 MB	Geschütztes Volume auf dem Dateiserver oder der Arbeitsstation

Die Werte in der vorstehenden Tabelle sind wie folgt definiert:

- **Warnschwellenwert –** Schwellenwert für die Warnung, die mit dem Replikatwachstum verknüpft ist; in der Regel 90%.
- **Protokolländerung –** Dies ist die Änderungsrate der betreffenden Datenbank oder Speichergruppe. Dieser Wert variiert stark, für die Standardempfehlung in DPM wird jedoch von 6% für Exchange- und SQL Server-Daten und von 10% für Windows SharePoint Services-Daten ausgegangen.
- **Aufbewahrungszeitraum –** Dies ist die Anzahl der gespeicherten Wiederherstellungspunkte; für die DPM-Standardempfehlungen wird von 5 ausgegangen.
- **Systemstatus-Datenquellengröße –** Die Größe der Datenquelle wird mit 1 GB veranschlagt.

Wenn Sie eine Schutzgruppe erstellen, wird im Dialogfeld **Festplattenzuweisung ändern** in der Spalte **Datengröße** für jede Datenquelle der Link **Berechnen** angezeigt. Für die anfängliche Festplattenzuweisung wendet DPM Standardformeln auf die Größe des Volumes, auf dem sich die Datenquelle befindet, an. Um die Formel auf die tatsächliche Größe der ausgewählten Datenquelle anzuwenden, klicken Sie auf den Link **Berechnen**. DPM bestimmt die Größe der Datenquelle und berechnet die Speicherzuweisung für die Wiederherstellungspunkt- und Replikatvolumes für diese Datenquelle neu. Dieser Vorgang kann mehrere Minuten dauern.

Es empfiehlt sich, die Standard-Speicherplatzzuweisungen zu verwenden, es sei denn, Sie sind sicher, dass sie Ihren Anforderungen nicht entsprechen. Das Überschreiben der Standardzuweisungen kann dazu führen, dass zu viel oder zu wenig Speicherplatz zugewiesen wird.

Wenn zu wenig Speicherplatz für die Wiederherstellungspunkte zugewiesen wird, kann DPM möglicherweise nicht genügend Wiederherstellungspunkte speichern, um den angestrebten Aufbewahrungszeitraum zu gewährleisten. Bei einer zu großen Speicherplatzzuweisung wird Speicherkapazität verschwendet.

Wenn Sie nach dem Erstellen einer Schutzgruppe feststellen, dass Sie zu wenig Speicherplatz für eine Datenquelle in der Schutzgruppe zugewiesen haben, können Sie die Zuweisungen für die Replikate und Wiederherstellungspunkte für jede Datenquelle erhöhen.

Wenn Sie feststellen, dass Sie zu viel Speicherplatz für die Schutzgruppe zugewiesen haben, besteht die einzige Möglichkeit, die Zuweisungen für eine Datenquelle zu verringern darin, die Datenquelle aus der Schutzgruppe zu entfernen, das Replikat zu löschen und dann die Datenquelle mit kleineren Zuweisungen wieder zur Schutzgruppe hinzuzufügen.

Damit Sie Ihre Speicherplatzanforderungen besser einschätzen können, downloaden Sie den DPM-Speicherplatzrechner (http://go.microsoft.com/fwlink/?LinkId=104370).

Siehe auch

Planen von Schutzkonfigurationen

Festlegen von Band- und Bibliotheksdetails

Wenn Sie Ihre Daten mithilfe von Bandmedien schützen möchten, müssen Sie angeben, wie viele Kopien DPM von jedem Band erstellen soll und die Konfigurationsoptionen für die Sicherungsbänder festlegen. Sie können eine der folgenden Optionen auswählen:

- **Daten komprimieren**

  Wenn Sie diese Option auswählen, komprimiert DPM die Daten beim Schreiben auf das Band, wodurch der Speicherplatzbedarf auf dem Band verringert wird. Somit können mehr Sicherungsaufträge auf demselben Band gespeichert werden. Durch die Komprimierung erhöht sich die Dauer des Sicherungsauftrags kaum.
  Die Komprimierungsrate variiert je nach Datentyp.

- **Daten verschlüsseln**

  Wenn Sie diese Option auswählen, verschlüsselt DPM die Daten beim Schreiben auf das Band, wodurch die Sicherheit der archivierten Daten erhöht wird. Durch die Verschlüsselung erhöht sich die Dauer des Sicherungsauftrags kaum.

  Hinweis

  Damit die Verschlüsselung verwendet werden kann, muss ein gültiges Verschlüsselungszertifikat auf dem DPM-Server verfügbar sein. Anleitungen finden Sie unter dem Thema zum Verschlüsseln von Daten in Schutzgruppen in der DPM-Hilfe.

Siehe auch

Planen von Schutzkonfigurationen

Auswählen einer Methode für die Replikaterstellung

Beim Erstellen einer Schutzgruppe müssen Sie eine Methode zum Erstellen der Replikate der Volumes in der Gruppe wählen. Bei der Replikaterstellung werden alle zu schützenden Daten auf den DPM-Server kopiert, und für jedes Replikat wird eine Synchronisierung mit Konsistenzprüfung durchgeführt.

DPM kann die Replikate automatisch über das Netzwerk erstellen, oder Sie erstellen die Replikate manuell, indem Sie die Daten von Wechselmedien wie z. B. Band wiederherstellen. Die automatische Replikaterstellung ist einfacher. Je nach Größe der geschützten Daten und der Geschwindigkeit des Netzwerks kann die manuelle Replikaterstellung jedoch schneller sein.

Als Entscheidungshilfe ist in der folgenden Tabelle die geschätzte Dauer von automatischen DPM-Replikaterstellungen über ein Netzwerk unter Berücksichtigung unterschiedlicher Mengen von geschützten Daten und verschiedener Netzwerkgeschwindigkeiten aufgeführt. Bei den Schätzungen wird davon ausgegangen, dass die vollständige Netzwerkgeschwindigkeit genutzt die Bandbreite nicht durch andere Arbeitslasten einschränkt wird. Die Zeitangaben erfolgen in Stunden.

Für die Automatische Replikaterstellung benötigte Zeit bei unterschiedlichen Netzwerkgeschwindigkeiten in Stunden

Größe der geschützten Daten	512 Kbit/s	2 Mbit/s	8 Mbit/s	32 Mbit/s	100 Mbit/s
1 GB	6	1,5	< 1	< 1	< 1
50 GB	284	71	18	5	1,5
200 GB	1137	284	71	18	6
500 GB	2844	711	178	45	15

Wichtig

Wenn Sie DPM bereitstellen, um Daten über ein WAN zu schützen, und in Ihrer Schutzgruppe mehr als 5 GB Daten enthalten sind, sollten Sie die Replikate manuell erstellen.

Automatische Replikaterstellung

Große Replikaterstellungsaufträge sollten für Zeiten geplant werden, in denen das Netzwerk nur schwach genutzt wird.

Manuelle Replikaterstellung

Wenn Sie die manuelle Replikaterstellung auswählen, legt DPM den genauen Speicherort auf dem DPM-Server fest, auf dem die Replikate erstellt werden müssen. Normalerweise werden die Replikate erstellt, indem die letzte Sicherung der Datenquelle von Wechselmedien wie z. B. Bandlaufwerken wiederhergestellt wird. Nach der Wiederherstellung der Daten schließen Sie den Prozess ab, indem Sie eine Synchronisierung mit Konsistenzprüfung für jedes Replikat durchführen.

Wenn Sie die Daten auf dem DPM-Server zur Erstellung des Replikats wiederherstellen, ist es entscheidend, dass die ursprüngliche Verzeichnisstruktur und die Eigenschaften der Datenquelle wie z. B. Zeitstempel und Sicherheitsberechtigungen beibehalten werden. Je mehr Abweichungen zwischen den Replikaten und den geschützten Quelldaten bestehen, desto länger dauert die Konsistenzprüfung. Wenn Sie die ursprüngliche Verzeichnisstruktur und die Eigenschaften der Quelldaten nicht beibehalten, kann die manuelle Replikaterstellung so lange dauern wie die automatische.

Siehe auch

Planen von Schutzkonfigurationen

Planen der DPM-Bereitstellung

Beim Erstellen des Bereitstellungsplans für Microsoft System Center Data Protection Manager (DPM) 2007 sollten Sie zuerst Ihre Schutzgruppen planen, da die Anforderungen der Schutzgruppen – Größe, Datenänderungsrate, Speicherort, Wiederherstellungsziele – das Erstellen und Platzieren von DPM-Servern und Bandbibliotheken beeinflussen.

Nachdem Sie Ihre Schutzgruppen geplant haben, können Sie den Bereitstellungsplan vervollständigen, indem Sie die Konfigurationen der DPM-Server bestimmen, die den Schutz Ihrer Daten am effizientesten gewährleisten. In diesem Abschnitt werden Überlegungen zu Sicherheit und Verwaltung behandelt, die Ihren Bereitstellungsplan beeinflussen können.

In diesem Abschnitt

Planen der DPM-Serverkonfigurationen

Überlegungen zur Endbenutzerwiederherstellung

Sicherheitsüberlegungen

Siehe auch

Planen von Schutzgruppen

Planen der DPM-Serverkonfigurationen

Ihr Bereitstellungsplan sollte die Anzahl der DPM-Server, die zum Schutz Ihrer Daten benötigt werden, enthalten und außerdem angeben, wo Sie die einzelnen DPM-Server in Ihrem Netzwerk platzieren werden.

Außerdem sollte der Bereitstellungsplan festlegen, welche Instanz von Microsoft SQL Server die einzelnen DPM-Server verwenden. DPM benötigt eine SQL Server-Instanz für die DPM- und Berichtdatenbanken. DPM installiert SQL Server während der Installation auf dem DPM-Server; Sie können aber auch eine vorhandene Instanz von SQL Server auf einem Remotecomputer verwenden.

Eine entscheidende Komponente Ihrer DPM-Serverkonfiguration ist der *Speicherpool.* Der aus mehreren Festplatten besteht, auf denen Replikate und Wiederherstellungspunkte für die geschützten Daten gespeichert werden. Die Kapazität des Speicherpools und der benutzerdefinierten Volumes, die Sie DPM zuweisen, muss ausreichend groß sein, um den festplattengestützten Schutz der ausgewählten Datenquellen zu leisten.

Falls Ihr Bereitstellungsplan den bandgestützten Schutz für Datenquellen vorsieht, müssen Sie dem DPM-Server eine Bandbibliothek oder ein eigenständiges Bandlaufwerk hinzufügen.

Wenn Sie eine große Windows SharePoint Services-Farm schützen möchten, sollten Sie DPM auf einem Volume installieren, das über genügend Speicherplatz für die DPM-Datenbank verfügt. Pro Million Elemente in der Farm benötigt die DPM-Datenbank ungefähr 1 GB. Wenn Sie zum Beispiel eine Farm mit 5 Millionen Elementen schützen, müssen Sie 5 GB Speicherplatz in der DPM-Datenbank einplanen, um den Katalog für diese Farm aufzunehmen.
Diese Speicheranforderung muss zum Speicherplatz hinzugerechnet werden, den DPM für die Bandsicherungskataloge, Auftragsprotokolle usw. benötigt.

In diesem Abschnitt

Siehe auch

Überlegungen zur Endbenutzerwiederherstellung

Sicherheitsüberlegungen

Auswählen der Anzahl der DPM-Server

Es gibt keine genaue Gleichung, um die Anzahl der DPM-Server zu bestimmen. Dies sollten Sie berücksichtigen, wenn Sie überlegen, wie viele DPM-Server Ihr Unternehmen benötigt.
In der Praxis variiert die Anzahl der Server und die Datenmenge, die ein einzelner DPM-Server schützen kann, in Abhängigkeit von den folgenden Faktoren:

- Änderungsrate der zu schützenden Datenquellen
- Im Speicherpool verfügbarer Speicherplatz
- Synchronisierungsfrequenz der Daten
- Verfügbare Bandbreite für jeden geschützten Computer
- Aggregierte Bandbreite auf dem DPM-Server

Sie können eine kürzlich durchgeführte inkrementelle Sicherung für einen durchschnittlichen Tag überprüfen, um die Datenänderungsrate einschätzen zu können. Der Prozentwert der Daten, die in einer inkrementellen Sicherung gespeichert werden, ist üblicherweise eine aussagekräftige Anzeige der Datenänderungsrate. Wenn Sie zum Beispiel insgesamt über 100 GB Daten verfügen und die inkrementelle Sicherung 10 GB enthält, beträgt Ihre Datenänderungsrate jeden Tag vermutlich ungefähr 10 Prozent.

Da sich das Verfahren, mit dem DPM Änderungen an Daten aufzeichnet, jedoch von dem der meisten Sicherungsprogramme unterscheidet, ist die Größe der inkrementellen Sicherung nicht immer eine genaue Anzeige der Datenänderungsrate. Um die Einschätzung Ihrer Datenänderungsrate zu präzisieren, berücksichtigen Sie die Merkmale der zu schützenden Daten.

Während die meisten Sicherungsprogramme Datenänderungen auf Dateiebene aufzeichnen, zeichnet DPM Änderungen auf Byte-Ebene auf. Abhängig vom Typ der zu schützenden Daten kann dies zu einer geringeren Datenänderungsrate führen, als die inkrementelle Sicherung vermuten lässt.

Die folgende Tabelle enthält die maximalen Datenquellen, die ein DPM-Server, der die Mindestanforderungen erfüllt, schützen kann sowie den empfohlenen Speicherplatz je DPM-Server.

Plattform	Datenquellengrenze	Empfohlener Speicherplatz
32-Bit-Computer	150 Datenquellen. Empfohlen werden ca. 30 bis 40 Server, die in einem DPM-Server zusammenkommen.	10 TB **Hinweis** Auf x86 32-Bit-Betriebssystemen gibt es eine Volumeschattenkopie-Dienst (VSS)-Begrenzung für Nicht-Auslagerungsspeicher. Wenn Sie Daten mit einem sekundären DPM-Server schützen, beträgt der empfohlene Speicherplatz nur 6 TB.
64-Bit-Computer	300 Datenquellen Datenquellen sind im Allgemeinen auf 50 bis 75 physische Server verteilt.	40 TB

Schattenkopie-Limit

Ein DPM-Server kann bis zu 9.000 festplattengestützte Schattenkopien speichern, darunter auch diejenigen, die beibehalten werden, wenn Sie den Schutz einer Datenquelle beenden. Diese Grenze gilt für vollständige Schnellsicherungen und Datei-Wiederherstellungspunkte, nicht jedoch für inkrementelle Sicherungen.

Das Schattenkopie-Limit gilt je DPM-Server, unabhängig von der Größe des Speicherpools. Beim Konfigurieren von Schutzgruppen wird auf dem DPM-Server die Anzahl der Schattenkopien entsprechend der Schutzgruppenkonfiguration vorgesehen. Sie können das folgende Cmdlet in der DPM Management Shell verwenden, um festzustellen, für wie viele Schattenkopien der Server eingerichtet ist:

$server=Connect-DPMServer –DPMServerName *Name*
$server.CurrentShadowCopyProvision

Beim Planen der DPM-Bereitstellung müssen Sie das Schattenkopie-Limit als Teil der DPM-Serverkapazität berücksichtigen. In der folgenden Tabelle sind Beispiele für die Anzahl von Schattenkopien aufgeführt, die aus verschiedenen Schutzrichtlinien resultieren.

Schutzrichtlinien	Snapshots
Exchange-Speichergruppe: tägliche vollständige Schnellsicherung und alle 15 Minuten inkrementelle Synchronisierung mit einem Aufbewahrungszeitraum von 5 Tagen	5
Volume auf einem Dateiserver: 3 tägliche Wiederherstellungspunkte mit einem Aufbewahrungszeitraum von 21 Tagen	63
SQL-Datenbank: 2 vollständige Schnellsicherungen täglich mit einem Aufbewahrungszeitraum von 14 Tagen	28
Gesamt:	**96**

Siehe auch

Planen der DPM-Serverkonfigurationen

Platzieren der DPM-Server

Zur Unterstützung der Schutz- und Wiederherstellungsvorgänge benötigt DPM eine Windows Server 2003 Active Directory-Domänendienste-Verzeichnisdienststruktur.

DPM kann Server und Arbeitsstationen schützen, die sich in derselben Domäne wie der DPM-Server befinden oder in einer Domäne, für die eine bidirektionale Vertrauensstellung zu der Domäne mit dem DPM-Server hergestellt wurde.

Wenn Sie entscheiden, wo der DPM-Server platziert werden soll, berücksichtigen Sie die Netzwerkbandbreite zwischen dem DPM-Server und den geschützten Computern.

DPM unterstützt Teaming-Netzwerkkarten (network interface cards, NIC). Teaming-NICs sind mehrere physische NICs, die so konfiguriert sind, dass sie vom Betriebssystem als eine NIC behandelt werden. Teaming-NICs bieten eine höhere Bandbreite, indem die einzelnen Bandbreiten, die für jede NIC verfügbar sind, kombiniert werden und das Failover auf die verbleibende NIC bzw. die verbleibenden NICs erfolgt, wenn eine NIC ausfällt. DPM kann die erhöhte Bandbreite nutzen, die durch die Verwendung von Teaming-NICs auf dem DPM-Server erzielt wird.

Eine andere Überlegung für die Platzierung der DPM-Server ist die Notwendigkeit, Bänder und Bandbibliotheken manuell zu verwalten, zum Beispiel neue Bänder zur Bibliothek hinzuzufügen oder Bänder für die Offsite-Archivierung zu entfernen.

Siehe auch

Planen der DPM-Serverkonfigurationen

Auswählen der SQL Server-Instanz

Eine typische DPM-Installation beinhaltet eine SQL Server-Instanz, die von DPM Setup installiert wird. Die von DPM Setup installierte SQL Server-Instanz ist in der DPM-Software enthalten und erfordert keine separate SQL Server-Lizenz.

Sie können bei der Installation von DPM 2007 jedoch auch eine Remoteinstanz von SQL Server angeben, die anstelle der in DPM enthaltenen Standardinstanz von SQL Server verwendet wird.

Damit eine Remoteinstanz von SQL Server verwendet werden kann, sollten sich der Server, auf dem SQL Server ausgeführt wird, und der DPM-Server in derselben Domäne befinden. Eine bestimmte SQL Server-Instanz kann jeweils nur von einem DPM-Server verwendet werden. Die Remoteinstanz von SQL Server darf sich nicht auf einem Computer befinden, der als Domänencontroller betrieben wird.

Hinweis

Wenn die Remoteinstanz von SQL Server als ein Domänenkonto betrieben wird, sollten Sie das Named Pipes-Protokoll für die Kommunikation mit dem DPM-Server aktivieren. Anleitungen zur Konfiguration des Named Pipes-Protokolls finden Sie, in englischer Sprache, unter Configuring Client Network Protocols (http://go.microsoft.com/fwlink/?LinkId=87976).

Die Remoteinstanz von SQL Server muss Internet Information Services (IIS) und SQL Server 2005 Standard oder Enterprise Edition mit SP2 einschließlich der folgenden Komponenten ausführen:

- SQL Server-Datenbankmodul
- Reporting Services

Es wird empfohlen, für die Remoteinstanz von SQL Server die folgenden Einstellungen zu verwenden:

- Verwenden Sie die Standardeinstellung für die Fehlerüberwachung.
- Verwenden Sie den Windows-Standardauthentifizierungsmodus.
- Weisen Sie dem sa-Konto (Systemadministratorkonto) ein sicheres Kennwort zu.
- Aktivieren Sie die Überprüfung der Kennwortrichtlinien.
- Installieren Sie nur die Komponenten SQL Server-Datenbankmodul und Reporting Services.
- Eine Remoteinstanz von SQL Server sollte nicht als lokales System ausgeführt werden.
- Führen Sie SQL Server unter Verwendung eines Domänenbenutzerkontos mit niedriger Berechtigungsstufe aus.

Siehe auch

Planen der DPM-Serverkonfigurationen

Planen des Speicherpools

Der Speicherpool ist ein Satz von Datenträgern, auf denen der DPM-Server die Replikate und Wiederherstellungspunkte für geschützte Daten speichert. Das Planen des Speicherpools umfasst das Berechnen der Kapazitätsanforderungen und das Planen der Datenträger-konfigurationen.

Sie können auch benutzerdefinierte Volumes, die Sie in der Datenträgerverwaltung definieren, für Volumes im Speicherpool einsetzen.

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.

Wenn Sie ein SAN für den Speicherpool verwenden, ist es empfehlenswert, eine separate Zone für die in DPM verwendeten Festplatten und Bänder zu erstellen. Mischen Sie die Geräte nicht in einer gemeinsamen Zone.

USB/1394-Datenträger können dem Speicherpool nicht hinzugefügt werden.

Es wird empfohlen, Datenträger mit einer Speicherkapazität von unter 1,5 Terabyte einzusetzen. Da ein dynamisches Volume bis zu 32 Datenträger enthalten kann, kann DPM Replikatvolumes von bis zu 48 Terabyte erstellen, wenn Datenträger von 1,5 Terabyte verwendet werden.

Wichtig

Einige Orginalcomputerhersteller (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

Siehe auch

Planen der DPM-Serverkonfigurationen

Berechnen der Kapazitätsanforderungen

Die Kapazitätsanforderungen für den DPM-Speicherpool sind variabel. Sie sind hauptsächlich von der Größe der geschützten Daten, der Größe des täglichen Wiederherstellungspunkts, der erwarteten Wachstumsrate der Volumedaten und dem angestrebten Aufbewahrungszeitraum abhängig.

Die Größe des täglichen Wiederherstellungspunkts bezieht sich auf den Gesamtumfang der Änderungen an den geschützten Daten während eines Tages. Sie ist etwa so groß wie eine inkrementelle Sicherung. Der Aufbewahrungszeitraum bezieht sich auf die Anzahl der Tage, über die Wiederherstellungspunkte von geschützten Daten auf Datenträgern gespeichert werden sollen. Für Dateien können in DPM maximal 64 Wiederherstellungspunkte pro Volume in eine Schutzgruppe aufgenommen werden. Pro Tag können maximal acht geplante Wiederherstellungspunkte für jede Schutzgruppe erstellt werden.

Hinweis

Die Grenze von 64 Wiederherstellungspunkten für Dateien ist durch die Einschränkungen der Volumeschattenkopie-Dienste (VSS) begründet, welche für die DPM-Funktion der Endbenutzerwiederherstellung erforderlich ist. Diese Höchstgrenze für Wiederherstellungspunkte gilt nicht für Anwendungsdaten.

Im Allgemeinen wird empfohlen, für den Speicherpool den zweifachen Umfang der geschützten Daten als Speicherplatz einzuplanen. Diese Empfehlung beruht auf einer angenommenen Größe des täglichen Wiederherstellungspunkts von etwa 10 Prozent der Größe der geschützten Daten und auf einem Aufbewahrungszeitraum von 10 Tagen (zwei Wochen ohne Wochenenden).

Wenn die Größe des täglichen Wiederherstellungspunkts mehr oder weniger als 10 Prozent der Größe der geschützten Daten beträgt, oder wenn der angestrebte Aufbewahrungszeitraum länger oder kürzer als zehn Tage ist, können Sie die Kapazitätsanforderungen Ihres Speicherpools entsprechend anpassen.

Unabhängig davon, wie viel Kapazität Sie bei der ersten Bereitstellung für den Speicherpool einplanen, sollten Sie erweiterbare Hardware verwenden. So können Sie bei Bedarf zusätzlichen Speicherplatz hinzufügen.

In den folgenden Abschnitten finden Sie Richtlinien für das Festlegen der Größe des täglichen Wiederherstellungspunkts und des angestrebten Aufbewahrungszeitraums.

Geschätzte Größe für den täglichen Wiederherstellungspunkt

Die Empfehlung, für den Speicherpool den zweifachen Umfang der geschützten Daten einzuplanen, gilt unter der Voraussetzung, dass die Größe des täglichen Wiederherstellungspunkts etwa 10 Prozent der Größe der geschützten Daten beträgt. Die Größe des täglichen Wiederherstellungspunkts ist abhängig von der Datenänderungsrate und bezieht sich auf die Gesamtgröße aller Wiederherstellungspunkte, die im Laufe eines Tages erstellt werden. Als Grundlage für die geschätzte Größe des täglichen Wiederherstellungspunkts für Ihre geschützten Daten können Sie eine aktuelle inkrementelle Sicherung an einem durchschnittlichen Tag nehmen. Die Größe einer inkrementellen Sicherung lässt in der Regel Rückschlüsse auf die Größe des täglichen Wiederherstellungspunkts zu. Wenn zum Beispiel die inkrementelle Sicherung bei einer Datenmenge von 100 GB einen Anteil von 10 GB umfasst, beträgt die Größe des täglichen Wiederherstellungspunkts wahrscheinlich etwa 10 GB.

Ermitteln der Ziele für den Aufbewahrungszeitraum

Die Empfehlung, für den Speicherpool den zweifachen Umfang der geschützten Daten als Speicherplatz einzuplanen, geht von einem angestrebten Aufbewahrungszeitraum von zehn Tagen (zwei Wochen ohne Wochenenden) aus. Die Datenwiederherstellungsanfragen in den meisten Unternehmen konzentrieren sich auf einen Zeitraum von zwei bis vier Wochen nach einem Datenverlust. Durch einen Aufbewahrungszeitraum von zehn Tagen wird die Datenwiederherstellung bis zu zwei Wochen nach einem Datenverlust gewährleistet.

Je länger der angestrebte Aufbewahrungszeitraum ist, desto weniger Wiederherstellungspunkte können pro Tag erstellt werden. Wenn der angestrebte Aufbewahrungszeitraum beispielsweise 64 Tage beträgt, kann nur ein Wiederherstellungspunkt pro Tag erstellt werden. Wenn der angestrebte Aufbewahrungszeitraum acht Tage beträgt, können acht Wiederherstellungspunkte pro Tag erstellt werden. Bei einem angestrebten Aufbewahrungszeitraum von zehn Tagen können etwa sechs Wiederherstellungspunkte pro Tag erstellt werden.

Siehe auch

Definieren angepasster Volumes

Planen der Festplattenkonfiguration

Planen der DPM-Serverkonfigurationen

Planen der Festplattenkonfiguration

Wenn Sie für den Speicherpool DAS (Direct Attached Storage) verwenden, können Sie entweder eine hardwarebasierte RAID-Konfiguration (Redundant Array of Independent Disks) oder eine JBOD-Konfiguration (Just a Bunch Of Disks) einsetzen. Erstellen Sie keine softwarebasierte RAID-Konfiguration für Festplatten, die Sie dem Speicherpool hinzufügen.

Bei der Entscheidung für eine Festplattenkonfiguration berücksichtigen Sie die relative Bedeutung der Kapazität, der Kosten, der Zuverlässigkeit und der Leistung für Ihre Umgebung. Da beispielsweise bei der JBOD-Konfiguration kein Speicherplatz auf der Festplatte zum Speichern der Paritätsdaten benötigt wird, bietet diese Konfiguration die optimale Nutzung der Speicherkapazität. Aus dem gleichen Grund sind JBOD-Konfigurationen jedoch auch weniger zuverlässig. Ein einziger Festplattenfehler führt unvermeidbar zu Datenverlust.

Für eine typische DPM-Bereitstellung ist eine RAID 5-Konfiguration normalerweise ein guter Kompromiss hinsichtlich Kapazität, Kosten, Zuverlässigkeit und Leistung. Da jedoch die Arbeitslast des DPM-Servers vor allem aus Schreibvorgängen besteht, beeinträchtigt RAID 5 die Leistung eines DPM-Servers wesentlich stärker als bei einem Dateiserver.
Diese Leistungsverringerung kann sich wiederum auf die Skalierbarkeit von DPM auswirken. Bei einer schlechteren Leistung nimmt auch die Datenschutzfähigkeit von DPM ab.

Als Entscheidungshilfe für die Festplattenkonfiguration in Ihrem Speicherpool werden in der folgenden Tabelle die Vor- und Nachteile von JBOD und den verschiedenen RAID-Ebenen auf einer Skala von 4 (sehr gut) bis 1 (akzeptabel) verglichen.

Vergleich der Konfigurationsoptionen für Festplatten im Speicherpool

Festplattenkonfiguration	Kapazität	Kosten	Zuverlässigkeit	Leistung und Skalierbarkeit
JBOD	4	4	1	4
RAID 0	4	4	1	4
RAID 1	1	1	4	3
RAID 5	3	3	3	2
RAID 10	1	1	4	4

Weitere Informationen über RAID finden Sie, in englischer Sprache, unter Achieving Fault Tolerance by Using RAID (http://go.microsoft.com/fwlink/?LinkId=46086).

Siehe auch

Berechnen der Kapazitätsanforderungen

Definieren angepasster Volumes

Planen der DPM-Serverkonfigurationen

Definieren angepasster Volumes

In DPM 2007 können Sie einem Schutzgruppenmitglied ein *benutzerdefiniertes Volume* anstelle des DPM-Speicherpools zuweisen. Ein benutzerdefiniertes Volume ist ein Volume, das sich nicht im DPM-Speicherpool befindet und das für die Speicherung der Replikate und Wiederherstellungspunkte eines Schutzgruppenmitglieds spezifiziert wurde.

Der von DPM verwaltete Speicherpool erfüllt zwar die meisten Geschäftsanforderungen, eventuell wünschen Sie aber eine stärkere Kontrolle über die Speicherung bestimmter Datenquellen. Zum Beispiel verfügen Sie über kritische Daten, die Sie unter Verwendung einer Hochleistungs-LUN (logical unit number, logische Gerätenummer) in einem Speicherbereichsnetzwerk speichern möchten.

Jedes Volume, das dem DPM-Server hinzugefügt wurde, kann als benutzerdefiniertes Volume im Assistenten zum Erstellen neuer Schutzgruppen ausgewählt werden, mit Ausnahme des Volumes, das die System- und Programmdateien enthält. Um benutzerdefinierte Volumes für ein Schutzgruppenmitglied verwenden zu können, sind zwei benutzerdefinierte Volumes erforderlich: ein Volume zum Speichern des Replikats und ein Volume zum Speichern der Wiederherstellungspunkte.

Der Speicherplatz der benutzerdefinierten Volumes kann nicht von DPM verwaltet werden. Wenn DPM eine Warnung ausgibt, dass ein benutzerdefiniertes Volume für Replikate oder Wiederherstellungspunkte nicht mehr viel freien Speicherplatz aufweist, müssen Sie in der Datenträgerverwaltung die Größe des benutzerdefinierten Volumes manuell ändern.

Nachdem Sie eine Schutzgruppe erstellt haben, können Sie die Auswahl von Speicherpool oder benutzerdefiniertem Volume für diese Schutzgruppe nicht mehr ändern. Wenn Sie den Speicherort für das Replikat oder die Wiederherstellungspunkte einer Datenquelle ändern möchten, ist dies nur möglich, indem Sie die Datenquelle aus dem Schutz entfernen und dann einer anderen Schutzgruppe als neues Schutzgruppenmitglied hinzufügen.

Siehe auch

Berechnen der Kapazitätsanforderungen

Planen der Festplattenkonfiguration

Planen der DPM-Serverkonfigurationen

Planen der Bandbibliothekskonfiguration

Sie können DPM Bandbibliotheken und eigenständige Bandlaufwerke hinzufügen, um den kurzfristigen und langfristigen Datenschutz auf Band zu ermöglichen. Die Bandbibliotheken und die eigenständigen Bandlaufwerke müssen physisch an den DPM-Server angeschlossen sein.

Hinweis

Der Begriff *Bandbibliotheken* bezieht sich sowohl auf Bandhardware mit mehreren Laufwerken als auch auf eigenständige Bandlaufwerke.

Berücksichtigen Sie beim Planen der Kapazität Ihrer Bandbibliothek die Anzahl der Bandsicherungsaufträge und die Größe der geschützten Daten. Auch die Hardwaremerkmale sollten nicht außer Acht gelassen werden: eine Bandbibliothek ohne Autoloader erfordert das manuelle Austauschen der Bänder, wenn Aufträge ausgeführt werden.

Um zu ermitteln, wie viele Bänder Sie für die einzelnen Schutzgruppen benötigen, multiplizieren Sie die Sicherungsfrequenz mit dem Aufbewahrungszeitraum.

Die Bandbezeichnungen der 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>**. Bevor Sie mit dem Erstellen von Schutzgruppen beginnen, sollten Sie sich ein Schema für die Bandbenennung überlegen, falls Sie nicht das Standardschema verwenden möchten.

Weitere Informationen finden Sie, in englischer Sprache, unter Managing Tape Libraries (http://go.microsoft.com/fwlink/?LinkId=91964).

Siehe auch

Planen der DPM-Serverkonfigurationen

Überlegungen zur Endbenutzerwiederherstellung

In Ihrem Bereitstellungsplan sollte festgelegt werden, für welche Daten die Endbenutzer-wiederherstellung möglich ist. Außerdem sollten die DPM-Server angegeben werden, die in den Active Directory-Domänendiensten konfiguriert werden müssen, um die Endbenutzerwieder-herstellung zu ermöglichen.

Die Endbenutzerwiederherstellung ermöglicht Endbenutzern, Daten selbstständig durch die Wiederherstellung früherer Dateiversionen wiederherzustellen. Endbenutzer können frühere Versionen über Freigaben auf Dateiservern, über DFS-Namespaces oder durch die Verwendung eines Menüpunkts im Menü **Extras** von Microsoft® Office 2003-Anwendungen wiederherstellen.

Wenn auf einem Computer, den Sie mit DPM schützen, zurzeit Schattenkopien von freigegebenen Ordnern aktiviert sind, können Sie diese Funktion deaktivieren und den so gewonnenen Speicherplatz nutzen. Endbenutzer und Administratoren können Dateien von den Wiederherstellungspunkten auf dem DPM-Server wiederherstellen.

Zum Aktivieren der Endbenutzerwiederherstellung müssen Sie das Schema der Active Directory-Verzeichnisdienste konfigurieren, die Endbenutzerwiederherstellung auf dem DPM-Server aktivieren und die Wiederherstellungspunkt-Clientsoftware auf den Clientcomputern installieren.

Konfigurieren der Active Directory Domänendienste

Das Konfigurieren der Active Directory-Domänendienste für die Unterstützung der Endbenutzerwiederherstellung umfasst vier Vorgänge:

1. Erweitern des Schemas
2. Erstellen eines Containers
3. Gewähren von Berechtigungen für den DPM-Server zum Ändern der Containerinhalte
4. Hinzufügen von Zuordnungen zwischen Quellenfreigaben und Freigaben aus den Replikaten

Das Schema wird nur ein Mal erweitert; Sie müssen die Active Directory-Schemaerweiterung allerdings für jeden DPM-Server konfigurieren. Wenn Sie die Endbenutzerwiederherstellung für weitere DPM-Server in der Domäne aktivieren, werden Schritt 3 und 4 für jeden zusätzlichen Server ausgeführt. DPM aktualisiert die Freigabenzuweisung (Schritt 4) bei Bedarf nach jeder Synchronisierung.

DPM-Administratoren, die sowohl Schema- als auch Domänenadministratoren in der Active Directory-Domänendienst-Domäne sind, können diese Schritte mit einem einzigen Klick in der

DPM-Verwaltungskonsole ausführen. DPM-Administratoren, die nicht Schema- und Domänenadministratoren sind, können diese Schritte ausführen, indem sie einen Schema- und Domänenadministrator anweisen, das Programm DPMADSchemaExtension auszuführen.

Das Programm DPMADSchemaExtension ist auf dem DPM-Server im Ordner „Microsoft Data Protection Manager\2006\End User Recovery“ gespeichert. Benutzer, die Schema- und Domänenadministratoren sind, können das Tool auf allen Computern mit Windows Server 2003 ausführen, die derselben Domäne angehören, in der der DPM-Server bereitgestellt wird. Der Administrator muss beim Ausführen des Programms den Namen des DPM-Servers angeben.

Wenn Sie die Endbenutzerwiederherstellung mithilfe von DPMADSchemaExtension aktivieren, müssen Sie dieses Programm für jeden DPM-Server ein Mal ausführen.

Installieren der Schattenkopie-Clientsoftware

Die DPM-Wiederherstellungspunkt-Clientsoftware muss auf den Computern der Endbenutzer installiert werden, bevor diese selbstständig frühere Versionen ihrer Dateien wiederherstellen können. Wenn ein Client für Schattenkopien von freigegebenen Ordnern auf dem Computer vorhanden ist, muss die Clientsoftware für die Unterstützung von DPM aktualisiert werden.

Die Wiederherstellungspunkt-Clientsoftware kann auf Computern mit dem Betriebssystem Microsoft Windows XP mit Service Pack 2 (SP2) oder höher bzw. Windows Server 2003 (mit oder ohne SP1) installiert werden.

Siehe auch

Planen der DPM-Serverkonfigurationen

Sicherheitsüberlegungen

Sicherheitsüberlegungen

DPM wird im Netzwerk als ein Server mit hoher Berechtigung ausgeführt. Um die Sicherheit des DPM-Servers zu gewährleisten, beruht die DPM-Sicherheitsarchitektur auf den Sicherheitsfunktionen von Windows Server 2003 und Active Directory-Domänendiensten, SQL Server 2005 und SQL Server Reporting Services.

So verwalten Sie die DPM-Sicherheitsarchitektur:

- Akzeptieren Sie alle Standardsicherheitseinstellungen.
- Installieren Sie keine unnötige Software auf dem DPM-Server.
- Ändern Sie nach der Bereitstellung von DPM nicht die Sicherheitseinstellungen. Dies gilt besonders für die Einstellungen in SQL Server 2005, Internet Information Services (IIS) und DCOM sowie für die Einstellungen für lokale Benutzer und Gruppen, die DPM während der Produktinstallation erstellt.
- Eine Remoteinstanz von SQL Server sollte nicht als lokales System ausgeführt werden.

Durch die Installation unnötiger Software und das Ändern der Standardsicherheitseinstellungen kann die Sicherheit von DPM ernsthaft gefährdet werden.

In diesem Abschnitt

Siehe auch

Überlegungen zur Endbenutzerwiederherstellung

Planen der DPM-Serverkonfigurationen

Konfigurieren des Antivirusprogramms

DPM ist mit den meisten gebräuchlichen Antivirusprogrammen kompatibel. Allerdings können Antivirusprogramme die Leistung von DPM beeinträchtigen, und wenn sie nicht richtig konfiguriert sind, können sie sogar Beschädigungen von Daten in Replikaten und Wiederherstellungspunkten verursachen. In diesem Abschnitt finden Sie Anleitungen zur Vermeidung derartiger Probleme.

Konfigurieren der Echtzeitüberwachung gegen Viren

Um die Leistungsbeeinträchtigung des DPM-Servers zu minimieren, deaktivieren Sie für alle geschützten Datenquellen die Antiviren-Echtzeitüberwachung der Replikate. Deaktivieren Sie dazu die Echtzeitüberwachung des DPM-Prozesses „msDPMprotectionagent.exe“ im Ordner „Microsoft Data Protection Manager\DPM\bin“. Die Echtzeitüberwachung von Replikaten beeinträchtigt die Leistung, weil die Antivirussoftware dabei alle betroffenen Dateien scannt, wenn DPM Änderungen an den Replikaten vornimmt.

Wenn Sie eine Verschlechterung der Leistung bei Verwendung der DPM-Verwaltungskonsole bemerken, deaktivieren Sie zusätzlich die Echtzeitüberwachung des Prozesses „csc.exe“, der sich im Ordner „Windows\Microsoft.net\Framework\v2.0.50727“ befindet. Bei dem Prozess „csc.exe“ handelt es sich um den C#-Compiler. Die Leistung wird durch Echtzeitüberwachung des Prozesses „csc.exe“ beeinträchtigt, da das Antivirusprogramm dabei Dateien scannt, die durch diesen Prozess beim Erstellen von XML-Meldungen ausgegeben werden.

Anleitungen zum Konfigurieren der Echtzeitüberwachung für einzelne Prozesse finden Sie in der Produktdokumentation Ihres Antivirusprogramms.

Festlegen von Optionen für infizierte Dateien

Um Schäden an Daten in Replikaten und Wiederherstellungspunkten zu verhindern, konfigurieren Sie das Antivirusprogramm auf dem DPM-Server so, dass infizierte Dateien gelöscht und nicht automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenschäden 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 Datenschäden im Replikat und in den Wiederherstellungspunkten verursacht werden. Sie umgehen dieses Problem, indem Sie das Antivirusprogramm so konfigurieren, dass infizierte Dateien gelöscht werden. Beachten Sie jedoch, dass jedes Mal, wenn das Antivirusprogramm eine Datei aus einem Replikat löscht, manuell eine Synchronisierung mit Konsistenzprüfung ausgeführt werden muss. Anleitungen zum Konfigurieren des Antivirusprogramms zum Löschen infizierter Dateien finden Sie im Produkthandbuch.

Siehe auch

Sicherheitsüberlegungen

Konfigurieren von Firewalls

Wenn sich die zu schützenden Computer hinter einer Firewall befinden, müssen Sie diese so konfigurieren, dass die Kommunikation zwischen dem DPM-Server, den zu schützenden Computern und den Domänencontrollern zugelassen ist.

Protokolle und Ports

Je nach Netzwerkkonfiguration müssen Sie möglicherweise die Konfiguration der Firewall ändern, um die Kommunikation zwischen DPM, den geschützten Servern und den Domänencontrollern zu ermöglichen. Zur Unterstützung bei der Firewallkonfiguration finden Sie in der folgenden Tabelle ausführliche Informationen über die von DPM verwendeten Protokolle und Ports.

Von DPM verwendete Protokolle und Ports

Protokoll	Port	Details
DCOM	135/TCP Dynamic	Das DPM-Steuerungsprotokoll verwendet DCOM. DPM richtet DCOM-Aufrufe an den Schutz-Agent, um ihm Befehle zu übermitteln. Der Schutz-Agent antwortet mit DCOM-Aufrufen an den DPM-Server. TCP-Port 135 ist der von DCOM zur Auflösung verwendete DCE-Endpunkt. Standardmäßig weist DCOM dynamisch Ports aus dem TCP-Portbereich 1024 bis 65535 zu. Sie können diesen Bereich jedoch mithilfe der Komponentendienste konfigurieren. Weitere Informationen finden Sie, in englischer Sprache, unter Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkId=46088).
TCP	5718/TCP 5719/TCP	Der DPM-Datenkanal basiert auf TCP. Sowohl DPM als auch der geschützte Computer bauen Verbindungen auf, um DPM-Vorgänge wie Synchronisierung und Wiederherstellung zu aktivieren. DPM kommuniziert mit dem Agent-Koordinator über den Port 5718 und mit dem Schutz-Agent über Port 5719.
DNS	53/UDP	Wird zwischen DPM und dem Domänencontroller sowie zwischen dem geschützten Computer und dem Domänencontroller zur Hostnamensauflösung verwendet.
Kerberos	88/UDP 88/TCP	Wird zwischen DPM und dem Domänencontroller sowie zwischen dem geschützten Computer und dem Domänencontroller zur Authentifizierung des Verbindungsendpunkts verwendet.
LDAP	389/TCP 389/UDP	Wird zwischen DPM und dem Domänencontroller für Abfragen verwendet.
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	Wird zwischen DPM und dem geschützten Computer, zwischen DPM und dem Domänencontroller sowie zwischen dem geschützten Computer und dem Domänencontroller für verschiedene Vorgänge verwendet. Wird für den direkt über TCP/IP gehosteten SMB für DPM-Funktionen verwendet.

Windows-Firewall

Die Windows Firewall ist in Windows Server 2003 SP1 enthalten. Wenn Sie die Windows-Firewall auf dem DPM-Server aktivieren, bevor Sie DPM installieren, kann DPM Setup die Firewall für DPM korrekt konfigurieren. Wenn Sie die Windows-Firewall auf dem DPM-Server aktivieren, nachdem Sie DPM installiert haben, müssen Sie die Firewall manuell konfigurieren, um die Kommunikation zwischen dem DPM-Server und den geschützten Computern zu ermöglichen. Konfigurieren Sie die Windows-Firewall auf einem DPM-Server, indem Sie Port 135 für TCP-Verkehr öffnen und den DPM-Dienst (Microsoft Data Protection Manager/DPM/bin/MsDPM.exe) und den Schutz-Agent (Microsoft Data Protection Manager/DPM/bin/Dpmra.exe) als Ausnahmen für die Windows-Firewall festlegen.

Anleitungen zum Konfigurieren der Windows-Firewall finden Sie unter dem Suchwort „Windows Firewall“ in „Windows-Hilfe und Support für Windows Server 2003“.

Siehe auch

Sicherheitsüberlegungen

Sicherheitsüberlegungen für die Endbenutzerwiederherstellung

Sie können die Endbenutzerwiederherstellung nur für Dateidaten, nicht für Anwendungsdaten aktivieren. Verwenden Sie nur domänenbasierte Sicherheitsgruppen für Berechtigungen für Dateien und Ordner, für die die Endbenutzerwiederherstellung ermöglicht werden soll. Wenn Sie sich auf lokale Sicherheitsgruppen verlassen, kann DPM keine Konsistenz zwischen dem Endbenutzerzugriff auf Daten auf geschützten Computern und dem Endbenutzerzugriff auf Wiederherstellungspunkte von diesen Daten auf dem DPM-Server gewährleisten.

Wenn sich z. B. der Benutzersatz in der lokalen Benutzergruppe des geschützten Computers von dem Benutzersatz in der lokalen Benutzergruppe des DPM-Servers unterscheidet, haben unterschiedliche Benutzersätze Zugriff auf die Daten auf dem Dateiserver und auf die Wiederherstellungspunkte dieser Daten.

Siehe auch

Sicherheitsüberlegungen

Gewähren geeigneter Benutzerrechte

Prüfen Sie vor einer DPM-Bereitstellung, ob die jeweiligen Benutzer über die erforderlichen Berechtigungen zur Ausführung der unterschiedlichen Aufgaben verfügen. In der folgenden Tabelle sind die Benutzerberechtigungen aufgeführt, die für die wichtigsten DPM-Aufgaben erforderlich sind.

Erforderliche Benutzerberechtigungen für das Ausführen von DPM-Aufgaben

Aufgabe	Erforderliche Berechtigungen
Hinzufügen eines DPM-Servers zu einer Active Directory-Domäne	Domänenadministratorkonto oder Benutzerrechte zum Hinzufügen einer Arbeitsstation zu einer Domäne
Installieren von DPM	Administratorkonto auf dem DPM-Server
Installieren des DPM-Schutz-Agent auf einem Computer	Domänenkonto, das Mitglied der lokalen Administratorgruppe auf dem Computer ist
Öffnen der DPM-Verwaltungskonsole	Administratorkonto auf dem DPM-Server
Erweitern des Active Directory-Domänendienste-Schemas zur Aktivierung der Endbenutzerwiederherstellung	Schemaadministrator-Berechtigungen in der Domäne
Erstellen eines Active Directory-Domänendienste-Containers zur Aktivierung der Endbenutzerwiederherstellung	Domänenadministrator-Berechtigungen in der Domäne
Gewähren von DPM-Serverberechtigungen zum Ändern der Container-Inhalte	Domänenadministrator-Berechtigungen in der Domäne
Aktivieren der Endbenutzerwiederherstellung auf einem DPM-Server	Administratorkonto auf dem DPM-Server
Installieren der Wiederherstellungspunkt-Clientsoftware auf einem Clientcomputer	Administratorkonto auf dem Clientcomputer
Zugreifen auf frühere Versionen geschützter Daten von einem Clientcomputer	Benutzerkonto mit Zugriff auf die geschützte Freigabe
Wiederherstellen der Windows SharePoint Services-Daten	Windows SharePoint Services-Farmadministratorkonto, das auch Administratorkonto auf dem Front-End-Webserver ist, auf dem der Schutz-Agent installiert ist

Siehe auch

Sicherheitsüberlegungen

Checkliste und Roadmap für den Bereitstellungsplan

Diese Checkliste enthält die Planungsaufgaben, die für die Vorbereitung der Bereitstellung von Data Protection Manager (DPM) 2007 erforderlich sind.

Aufgabe	Referenz
Identifizieren Sie alle zu schützenden Datenquellen einschließlich der folgenden Informationen: • Datenquellentyp (Datei, Microsoft Exchange, Microsoft SQL Server, Microsoft Windows SharePoint Services, Microsoft Virtual Server, Systemstatus) • Größe der Datenquelle • Ordner oder Dateinamenserweiterungen, die vom Schutz ausgenommen werden sollen • Vollständig qualifizierter Domänenname (FQDN) des Computers • Clustername (falls zutreffend)	Was soll geschützt werden?
Identifizieren Sie eine der folgenden Methoden für jede Schutzgruppe: • Kurzfristiger festplattengestützter Schutz • Kurzfristiger bandgestützter Schutz • Langfristiger bandgestützter Schutz • Kurzfristiger festplattengestützter Schutz und langfristiger bandgestützter Schutz • Kurzfristiger bandgestützter Schutz und langfristiger bandgestützter Schutz	Auswählen einer Datenschutzmethode

Aufgabe	Referenz
Bestimmen Sie die Wiederherstellungsziele für die einzelnen Datenschutzmethoden, die Sie verwenden. Für den kurzfristigen festplattengestützten Schutz identifizieren Sie die folgenden Informationen: • Aufbewahrungszeitraum • Synchronisierungsfrequenz • Anzahl der Wiederherstellungspunkte Für den kurzfristigen bandgestützten Schutz identifizieren Sie die folgenden Informationen: • Aufbewahrungszeitraum • Sicherungszeitplan • Sicherungstyp • Anzahl der Sicherungskopien • Bandbezeichnungsschema Für den langfristigen bandgestützten Schutz identifizieren Sie die folgenden Informationen: • Aufbewahrungszeitraum • Sicherungszeitplan und Sicherungsoptionen • Anzahl der Sicherungskopien • Bandbezeichnungsschema	Welches sind die Ziele bei der Wiederherstellung? Definieren von Wiederherstellungszielen
Organisieren Sie die Datenquellen in Schutzgruppen.	Auswählen von Schutzgruppenmitgliedern
Ermitteln Sie Ihre Speicheranforderungen anhand der Informationen über die geschützten Daten und Wiederherstellungsziele.	Zuweisen von Speicherplatz für Schutzgruppen
Wenn Sie den bandgestützten Schutz verwenden, entscheiden Sie, ob Sie Daten auf Bändern komprimieren oder verschlüsseln möchten.	Festlegen von Band- und Bibliotheksdetails
Legen Sie fest, welche Methode der Replikaterstellung für die einzelnen Schutzgruppen verwendet werden soll.	Auswählen einer Methode für die Replikaterstellung

Aufgabe	Referenz
Identifizieren Sie die erforderlichen DPM-Serverkonfigurationen, darunter die folgenden Informationen: • Anzahl der DPM-Server • Platzierung der DPM-Server • Verwendete Instanz von SQL Server auf den einzelnen DPM-Servern	Planen der DPM-Serverkonfigurationen
Ermitteln Sie die erforderlichen Datenträgerkonfigurationen für die einzelnen DPM-Server, um die Speicheranforderungen der Schutzgruppen zu erfüllen. Schließen Sie ggf. benutzerdefinierte Volumes mit ein, die für bestimmte Datenquellen verwendet werden.	Planen des Speicherpools
Identifizieren Sie die DPM-Server, die Bandbibliotheken benötigen, sowie die Kapazität der einzelnen Bibliotheken.	Planen der Bandbibliothekskonfiguration
Identifizieren Sie die DPM-Server, für die die Endbenutzerwiederherstellung aktiviert werden soll, und auf welchen Clients die Wiederherstellungspunkt-Clientsoftware installiert werden muss.	Überlegungen zur Endbenutzerwiederherstellung

Siehe auch

Einführung in Data Protection Manager 2007

Planen der DPM-Bereitstellung

Planen von Schutzgruppen