Windows Server System

System Center Data Protection Manager 2007 導入の計画

Microsoft Corporation

公開：2007 年 9 月

概要

本書では、DPM の使い方を説明し、導入計画のガイダンスを示します。

本書に紹介されている情報は、説明されている問題について、公開日現在における Microsoft Corporation の最新の見解を示すものです。Microsoft は変化する市況に対応しなければならないため、本書の内容を Microsoft が確約しているものと解釈しないでください。また、Microsoft は公開日後に提示されたいかなる情報についても、その正確性を保証いたしません。

このホワイトペーパーは情報提供のみを目的とするものです。Microsoft は、明示的であれ黙示的であれ、法令によるものであれ、本書の情報についていかなる保証も致しません。

目次

DPM 2007 の導入計画

本書では、DPM の使い方を説明し、導入計画のガイダンスを示します。

本項の内容

Data Protection Manager 2007 の導入

Microsoft System Center Data Protection Manager（DPM）2007 は、IT 専門家が Windows 環境の管理に使用する管理製品である Microsoft System Center シリーズのキーメンバーです。DPM は Windows のバックアップと回復の新基準であり、内蔵ディスクとテープメディアを使用して Microsoft アプリケーションとファイルサーバーにシームレスなデータ保護を実現します。

本項の内容

DPM の機能

データ保護は企業や組織にとって不可欠なものです。Microsoft System Center Data Protection Manager (DPM) 2007 は、そのデータ保護を実現する効果的なソリューションです。DPM を導入すると、御社にとって次のメリットがあります。

- ディスクベースのデータ保護と回復
- テープベースのバックアップとアーカイブのソリューション
- 障害回復ソリューション

DPM データベースをテープにバックアップできます。または、地理的に離れている場所でセカンダリ DPM サーバーを使用して、プライマリ DPM サーバーを保護することもできます。

セカンダリ DPM サーバーを使用する場合は、セカンダリ DPM サーバーから保護されるコンピュータにデータを直接復元することが可能です。セカンダリ DPM サーバーは、プライマリ DPM サーバーがオンラインに復帰するまでコンピュータを保護することもできます。

- DPM により、次のアイテムが保護されます。
  - ボリューム、共有、およびフォルダのファイルデータ
  - Microsoft Exchange Server ストレージグループ、Microsoft SQL Server データベース、Windows SharePoint Services ファーム、および Microsoft Virtual Server とその仮想コンピュータなどのアプリケーションデータ
  - Home エディションを除く、Windows XP Professional SP2 およびすべての Windows Vista エディションを実行するワークステーションのファイル
  - クラスタサーバー上のファイルおよびアプリケーションデータ
  - 保護されるファイルおよびアプリケーションサーバーのシステム状態

本項の内容

関連項目

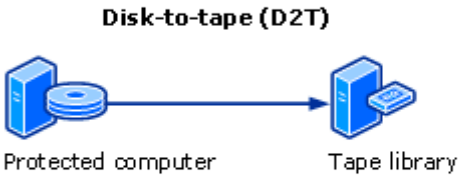
DPM の使い方

ディスクとテープを組み合わせたバックアップソリューション

DPM データ保護を使用して、ディスクベースのストレージ、テープベースのストレージ、またはその両方を行うことができます。

ディスクベースのストレージ（別名 D2D: disk-to-disk）とは、コンピュータのデータが別のコンピュータのハードディスクに格納されるというバックアップの方式です。これは、コンピュータのデータがテープなどの記憶域メディアにバックアップされる（別名 D2T: disk-to-tape）という従来の方式とは対照的です。 保護のレベルを高めるために 2 種類の方式を組み合わせた D2D2T（disk-to-disk-to-tape）構成と呼ばれる方式もあります。この方式では、短期保存にはディスクベースのストレージの利点である迅速な修復を用い、重要なデータの長期保存には、テープベースのアーカイブストレージを用います。 下図は 3 種類のストレージ方式を示したものです。

データストレージの方式



どのストレージ方式を使うかを決めるには、御社のさまざまなデータ保護要件の重要度を比較検討する必要があります。

- **失ってもかまわない会社のデータはどの程度か?** 現実的に判断すると、すべてのデータの価値が同等ということはありません。会社は、データが失われた場合の影響とデータ保護のコストをはかりにかける必要があります。
- **データの回復はどの程度緊急を要するか?** 業務の継続に不可欠なデータの回復は通常、ルーチンデータよりも緊急を要します。他方、回復操作によって中断されてはならない不可欠なサービスを営業時間中に提供しているサーバーを識別する必要があります。
- **データはいつまで保存しておく必要があるか?** データの種類や内容によっては、業務遂行のために長期保存が必要なものもあるでしょう。サーベーンズオックスレー法（Sarbanes-Oxley Act）やデータ保持指令（Data Retention Directive）など、データ保持の法的義務に従わなければならない場合もあります。
- **データ保護に投入可能な予算は?** データ保護の予算を検討する際には、ハードウェアとメディアの費用だけでなく、管理やサポートの人件費も計算に入れる必要があります。

DPM を使用すれば、ディスクとテープの両方にデータをバックアップすることで、重点的かつ詳細にわたるバックアップ戦略を自由に立てることができ、結果的にデータを効率的かつ経済的に保護できます。復元の対象がファイル 1 つでもサーバー全体でも、修復は迅速かつ単純に行えます。ユーザーはデータを確認するだけです。後は、DPM がデータを検出して回復します（ただし、テープがライブラリから取り出されている場合は、挿入する手間が必要です）。

ディスクベースの保護と回復

ディスクベースのデータ保護の利点の 1 つは、時間を節約できることです。テープベースのデータ保護の場合には、保護ジョブに必要な特定のテープを探し出してセットし、巻き戻しか早送りで正しい開始点に移動するという準備の時間が必要ですが、ディスクベースのデータ保護の場合にはそれが一切不要です。ディスクは使いやすいので、インクリメンタルデータを頻繁に保存しても苦にならず、保護の対象となるコンピュータやネットワークリソースに対する影響も小さくて済みます。

ディスクベースのデータ保護を使用した場合のデータ回復は、テープベースの場合よりも信頼性に優れています。通常、ディスクドライブはテープと比べて平均故障間隔（MTBF）がずっと長く、安定しています。

データ回復は、テープよりもディスクから行う方が速くて容易です。ディスクからのデータ回復は、DPM サーバー上で以前のバージョンのデータを参照し、選択したバージョンを保護されるコンピュータ上に直接コピーするだけの単純作業です。テープからファイルを回復する作業は、通常数時間かかり、費用も高くなる場合があります。また、中規模のデータセンターの管理者は、毎月そうした回復作業を 10 ～ 20 回、またはそれ以上行うのが通例です。

DPM とディスクベースのデータ保護を使用すれば、15 分間隔でデータの同期が行われ、データは 448 日もの長期間にわたって保存されます。

テープベースのバックアップとアーカイブ

磁気テープやそれに類する記憶メディアを使用する方式のデータ保護は、安価で持ち運びに便利なほか、長期保存には特に有用です。

DPM では、コンピュータからテープに直接（D2T）データをバックアップできます。また、ディスクベースのレプリカからデータをバックアップすることも可能です（D2D2T）。ディスクベースのレプリカから長期間保存するテープバックアップを作成する場合の利点は、バックアップ操作をいつでも実行でき、保護されるコンピュータに対する影響がまったくないことです。

また、完全障害復旧プランの場合は、重要な情報を別の場所に格納することも可能です。万一社屋が損傷または損壊した場合でも、会社のデータを復旧できるのです。テープは、データを別の場所に格納するのによく使われる便利なメディアです。

DPM を使用すれば、短期保護が目的の場合は毎日 1 回テープにデータのバックアップを取ることができます。また、長期保護の場合は 99 年間の保存が可能です。

DPM パートナーが販売しているソフトウェアソリューションを使用すれば、テープの代わりに USB ハードドライブなどのリムーバブルメディアを使用できます。詳細については、「Data Protection Manager Partners」（DPM パートナー）（http://go.microsoft.com/fwlink/?LinkId=98869）を参照してください。

関連項目

管理ツール
クラスタサーバーの保護
複数のデータ型の保護

複数のデータ型の保護

次の表は、DPM で保護できるデータ型、および DPM を使用して回復できるデータのレベルを示したものです。

メモ

保護するコンピュータに固有のソフトウェア要件については、「DPM System Requirements」（DPM のシステム要件）（http://go.microsoft.com/fwlink/?LinkId=66731）を参照してください。

保護と回復が可能なデータ

製品名	保護可能なデータ	回復が可能なデータ
Exchange Server 2003 Exchange Server 2007	• ストレージグループ	• ストレージグループ • データベース • メールボックス
SQL Server 2000 SQL Server 2005	• データベース	• データベース
Microsoft Office SharePoint Server 2007 Windows SharePoint Services 3.0	• ファーム	• ファーム • データベース • サイト • ファイルまたはリスト
Windows Server 2003 Windows Storage Server 2003	• ボリューム • 共有 • フォルダ	• ボリューム • 共有 • フォルダ • ファイル
Microsoft Virtual Server 2005 R2 SP1	• 仮想サーバーホストの構成 • 仮想コンピュータ • 仮想コンピュータで実行されているアプリケーションのデータ[1]	• 仮想サーバーホストの構成 • 仮想コンピュータ • 仮想コンピュータで実行されているアプリケーションのデータ[1]

製品名	保護可能なデータ	回復が可能なデータ
DPM 2007 によって保護が可能なすべてのコンピュータ（Windows Vista または Windows Server 2008 を実行しているコンピュータを除く）	• システム状態	• システム状態
Home エディションを除く、Windows XP Professional SP2 およびすべての Windows Vista エディションを実行しているワークステーション（ドメインのメンバーである必要があります）	• ファイルデータ	• ファイルデータ

[1] 仮想コンピュータで実行されているアプリケーションのデータは、保護される仮想コンピュータのコンポーネントとしてではなく、アプリケーションのデータソースとして保護し、回復する必要があります。たとえば、仮想コンピュータで実行されている SQL Server のインスタンス用のデータを保護し、回復するには、DPM 保護エージェントを仮想コンピュータにインストールし、データソースを SQL Server データベースとして選択します。保護エージェントを仮想ホストにインストールし、ホスト上の仮想コンピュータを保護すると、アプリケーションデータも保護されますが、仮想コンピュータそのものを回復することによってのみ回復できます。

関連項目

保護されるファイルサーバーとワークステーションの管理

Exchange を実行する保護されるサーバーの管理

SQL Server を実行する保護されるサーバーの管理

Windows SharePoint Services を実行する保護されるサーバーの管理

保護される仮想サーバーの管理

クラスタサーバーの保護

DPM 2007 は、ファイルサーバー Exchange Server 2003、SQL Server 2000、および SQL Server 2005 の共有ディスククラスタをサポートしています。DPM 2007 は、Exchange Server 2007 の非共有ディスククラスタと共有ディスククラスタの両方をサポートしています。

DPM 保護エージェントをインストールする際に、クラスタノードであるサーバーを選択すると、クラスタ内の他のノードにも保護エージェントをインストールするオプションが表示されます。

エンドユーザー回復は、クラスタファイルサーバーのクラスタリソースと非クラスタリソースの両方で使用できます。

計画的フェイルオーバーの際には、DPM は保護を続けます。非計画的フェイルオーバーの際には、DPM は整合性チェックが必要であることを示すアラートを発します。

関連項目

複数のデータ型の保護

管理ツール

主要な管理タスクのパフォーマンスを助けるために、DPM 2007 には IT 管理者用に次のツールと機能が備わっています。

- DPM 管理者コンソール
- レポートと通知
- DPM 管理パック
- Windows PowerShell の統合
- リモート管理
- エンドユーザー回復

DPM 管理者コンソール

DPM 管理者コンソールでは、タスクベースの管理モデルが使用されており、一般的なタスクが自動化されるため、管理者は少ない手順で仕事を完了することができます。

データ保護処理の管理を簡素化するために、DPM は Microsoft 管理コンソール（MMC）の機能を強化し、設定、管理、および監視のタスクを行うために見慣れた直感的な環境を提供しています。

DPM 管理者コンソールでは、各タスクが簡単にアクセスできる 5 つのタスク領域（監視、保護、回復、報告、管理）にまとめられています。管理者は、ウィザードに表示される指示に従って、タスクの追加、エージェントのインストール、および保護グループの作成などの基本設定タスクを行うことができます。ファイルの旧バージョンの検索と**回復**に役立てるために、検索と参照の機能が 回復 タスク領域に用意されています。

DPM 管理者コンソールには、データ保護処理を監視するために、**ジョブ** タブと **アラート** タブの両方があります。 **ジョブ** タブには、スケジュール済み、完了、実行中、キャンセル済み、または失敗した各ジョブについて、ステータスと動作の詳細が表示されます。 **アラート** タブには、システム全体の処理のサマリービューを示すために情報アラートとエラー状況が集められ、各エラーについて推奨する処理が示されています。

DPM 管理者コンソールの使い方の詳細については、「DPM 2007 の導入」で、「付録 A: DPM 管理者コンソール」（http://go.microsoft.com/fwlink/?LinkId=98871）を参照してください。

レポートと通知

DPM には総合的な一連のレポートを生成する機能があり、保護の成功と失敗、回復の成功と失敗、およびディスクとテープの使用率に関するデータが表示されます。また、一般的なエラーの識別や、テープの循環の管理ができます。サマリーでは、保護されるすべてのコンピュータと保護グループに関する総合情報が報告されます。詳細なレポートには、個々のコンピュータや保護グループに関する情報が表示されます。管理者は、DPM の初期導入の後に、これらのレポートを使用して保護を微調整できます。

DPM 通知は、重要なアラート、警告アラート、または情報アラートが生成されると常に通知が表示される便利な手段です。たとえば、重要なアラートのみが通知されるようにするなど、通知を受けるアラートの重大度を選択できます。また、回復ジョブのステータスについて通知を受けるように設定したり、DPM レポートを E- メールの添付ファイルとして受信するスケジュールを設定することもできます。こうした機能により、データ保護の傾向を監視し、都合の良いときにデータ保護の統計を分析できます。さらに、System Center Operations Manager 2007 に DPM 管理パックを使用して、カスタマイズされた通知を受け取ることもできます。

DPM 2007 で利用可能なレポートの詳細については、「Managing DPM Servers」（DPM サーバーの管理）（http://go.microsoft.com/fwlink/?LinkId=91853）を参照してください。通知の購読方法については、DPM 2007 のヘルプを参照してください。

DPM 管理パック

Microsoft Operations Manager 2005（MOM）および System Center Operations Manager 2007 の管理パックが、DPM 2007 でも使用できるようになります。データ管理戦略の一環として、DPM 管理パックを使用して、複数の DPM サーバーおよび保護するサーバーのデータ保護、状態、ヘルス、パフォーマンスを集中的に監視することができます。管理者は、Operations Manager の操作コンソールから、DPM とネットワークインフラを同時に監視し、システムやネットワークのパフォーマンスにおける他の要因のコンテキストに照らしてデータ保護上の問題を分析することができます。管理者は、SQL Server など、ミッションクリティカルな他のアプリケーションを監視することもできます。

DPM 管理パックのダウンロード方法については、「Management Pack Catalog」（管理パックのカタログ）（http://go.microsoft.com/fwlink/?LinkId=47215）を参照してください。

Windows PowerShell の統合

Windows PowerShell は、タスクベースのスクリプティングもサポートするインタラクティブコマンドラインテクノロジです。

DPM には独自の Windows PowerShell コマンドセットが備わっており、データ保護の管理タスクに使用できます。DPM cmdlets には、DPM 管理シェルからアクセスします。

DPM 管理者は DPM cmdlets を使用して、コンソール内で実行可能なすべての管理タスクを実行できます。DPM cmdlets には、次のタスクに使用する一連のコマンドがあります。

- DPM の設定
- テープとディスクの管理
- 保護グループの管理
- データの保護と回復

また、管理者は DPM cmdlets を使用して次のタスクを実行できます。これらは DPM 管理者コンソールでは実行できないタスクです。

- 復旧ポイントの削除
- 詳細なインベントリやクリーニングなど、ライブラリのメンテナンスジョブの開始時刻のカスタマイズ
- バックアップジョブに使用する LAN 構成の指定

リモート管理

DPM サーバーに対するリモートデスクトップ接続を確立して、DPM の動作をリモートから管理することができます。

DPM 管理シェルを DPM サーバー以外の複数のコンピュータにインストールして、複数の DPM サーバーをリモートから管理することも可能です。DPM 管理シェルは、Windows XP または Windows Vista を実行しているデスクトップコンピュータにもインストールすることができます。

エンドユーザー回復

DPM では、管理者によるデータ回復のほかに、見慣れた Windows Explorer のインタフェースまたは Microsoft Office 2007 アプリケーションのいずれかを使用して、ユーザーが自身のファイルの旧バージョンを別途に取得することもできます。エンドユーザー回復はアプリケーションデータには使用できません。

関連項目

クラスタサーバーの保護

複数のデータ型の保護

DPM の使い方

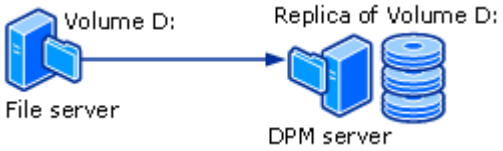
Data Protection Manager がデータの保護に使用する方法は、保護するデータの種類や選択する保護の方法によって異なります。

本項の内容

ディスクベースの保護プロセス

DPM サーバーは、ディスクベースのデータ保護を行うために、保護されるサーバー上のデータの「レプリカ」（コピー）を作成して保持します。レプリカは、DPM サーバー上またはカスタムボリューム上の一連のディスクで構成される「記憶域プール」に保存されます。下図は、保護されるボリュームとそのレプリカの基本的な関係を示したものです。

レプリカの作成



ファイルデータとアプリケーションデータのどちらを保護する場合も、まずはデータソースのレプリカを作成する作業から始めます。

レプリカは、管理者やユーザーが設定した一定の間隔で「同期」、つまりアップデートされます。DPM がレプリカの同期に使用する方法は、保護するデータの種類によって異なります。詳細については、「The File Data Synchronization Process」（ファイルデータの同期処理）および「The Application Data Synchronization Process」（アプリケーションデータの同期処理）を参照してください。レプリカの不一致が検出されると、DPM は整合性チェックを行い、レプリカがブロックごとにデータソースに照らして検証されます。

保護構成の単純な一例は、DPM サーバー 1 台と保護されるコンピュータ 1 台の構成です。DPM「保護エージェント」をコンピュータにインストールし、そのデータを「保護グループ」に追加すると、そのコンピュータは保護されます。

保護エージェントは保護されるデータへの変更を記録し、変更内容を DPM サーバーに転送します。保護エージェントはまた、コンピュータ上で、保護が可能で回復プロセスに含まれているデータを識別します。DPM を使用して保護する各コンピュータに保護エージェントをインストールする必要があります。保護エージェントは DPM によってインストールすることもできますが、Systems Management Server（SMS）などのアプリケーションを使用して手動でインストールすることも可能です。

保護グループは、コンピュータ上のデータソースの保護を管理するために使用します。保護グループとは、同じ保護構成を共有するデータソースの集まりです。保護構成とは、保護グループ名、保護ポリシー、ディスクの割り当て、およびレプリカの作成方法など、保護グループに共通な設定の集まりです。

DPM には、記憶域プール内の各保護グループメンバーについて別々のレプリカが保存されます。保護グループメンバーは、次のどのデータソースでもかまいません。

- デスクトップコンピュータ、ファイルサーバー、またはサーバークラスタ上のボリューム、共有、またはフォルダ
- Exchange サーバーまたはサーバークラスタ上のストレージグループ
- SQL Server またはサーバークラスタのインスタンスのデータベース

関連項目

アプリケーションデータの同期処理

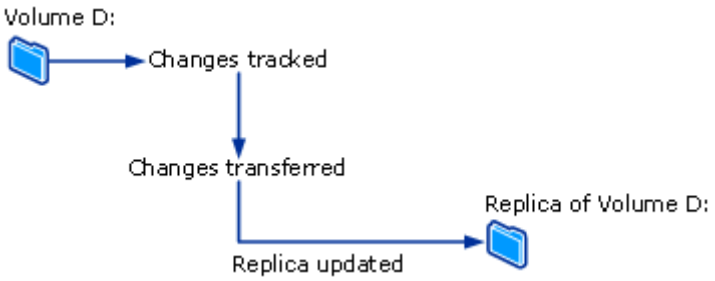
ファイルデータとアプリケーションデータの違い

ファイルデータの同期処理

ファイルデータの同期処理

DPM 2007 では、サーバー上のファイルボリュームまたは共有に対して、保護エージェントはボリュームフィルタと変更ジャーナルを使用して、どのファイルが変更されたかを判断し、それらのファイルに対してチェックサムプロシージャを実行して、変更されたブロックのみを同期します。同期中にこれらの変更は DPM サーバーに転送され、レプリカをデータソースと同期するためにレプリカに適用されます。次の図はファイルの同期処理を示したものです。

ファイルの同期処理



レプリカがそのデータソースと一致しなくなると、DPM は、どのコンピュータとどのデータソースが影響を受けるかを示すアラートを生成します。この問題を解決するには、管理者は、レプリカ上で整合性チェックによる同期（単に整合性チェックとも呼ばれます）を開始してレプリカを修復します。整合性チェック中に、DPM はブロックごとの検証を行い、レプリカを修復してデータソースと一致する状態に戻します。

保護グループに対して毎日の整合性チェックをスケジュールしたり、または整合性チェックを手動で開始することもできます。

DPM は、ユーザー / 管理者が設定した一定間隔で、保護グループメンバーの復旧ポイントを作成します。復旧ポイントとは、そこからのデータの回復が可能なデータのバージョンのことです。各ファイルにとって、復旧ポイントはレプリカのシャドウコピーで構成されています。シャドウコピーは、DPM サーバー上のオペレーティングシステムのボリュームシャドウコピーサービス（VSS）機能を使用して作成します。

関連項目

アプリケーションデータの同期処理

ファイルデータとアプリケーションデータの違い

ディスクベースの保護プロセス

アプリケーションデータの同期処理

アプリケーションデータの場合は、DPM によってレプリカが作成されると、アプリケーションファイルに属するボリュームブロックに対する変更がボリュームフィルタによって追跡されます。

変更がどのようにして DPM サーバーに転送されるかは、アプリケーションと同期の種類によって異なります。DPM 管理者コンソール内に同期と表記されている操作は増分バックアップのようなもので、レプリカと組み合わせるとアプリケーションデータの正確なリフレクションが作成されます。

DPM 管理者コンソール内に高速完全バックアップと表記された種類の同期の実行中、ボリュームシャドウコピーサービス（VSS）の完全なスナップショットが作成されますが、DPM サーバーに転送されるのは変更されたブロックのみです。

高速完全バックアップが実行されるたびに、アプリケーションデータの復旧ポイントが作成されます。アプリケーションが増分バックアップをサポートしている場合、同期実行時にも毎回復旧ポイントが作成されます。各種のアプリケーションデータによってサポートされている同期の種類は、次のようにまとめることができます。

- 保護される Exchange のデータの場合は、同期によって、Exchange VSS ライターが使用されて増分 VSS スナップショットが転送されます。同期および高速完全バックアップが実行されるたびに、復旧ポイントが作成されます。

- 読み取り専用モードでログシップされた、または単純復旧モデルを使用する SQL Server データベースは、増分バックアップをサポートしません。高速完全バックアップのみが実行されるたびに、復旧ポイントが作成されます。その他すべての SQL Server データベースの場合は、同期によってトランザクションログのバックアップが転送され、増分同期または高速完全バックアップが実行されるたびに復旧ポイントが作成されます。トランザクションログとは、それ（トランザクションログ）が前回バックアップされて以降、データベースに対して実行されたすべてのトランザクションのシリアル記録です。
- Windows SharePoint Services と Microsoft Virtual Server は、増分バックアップをサポートしません。高速完全バックアップのみが実行されるたびに、復旧ポイントが作成されます。

増分同期は、高速完全バックアップよりも短時間で済みます。これは、DPM が前回の完全バックアップを復元し、復元の対象として選択した時点までのすべての増分同期を復元して適用しなければならないためです。これは、DPM が前回の完全バックアップを復元し、復元の対象として選択した時点までのすべての増分同期を復元して適用しなければならないためです。

回復時間を短縮できるように、DPM は定期的に高速完全バックアップを実行します。これは、変更されたブロックが含まれるようにレプリカをアップデートする同期の種類です。

高速完全バックアップ中、DPM は、変更されたブロックでレプリカをアップデートする前にレプリカのスナップショットを作成します。復旧ポイントを増やすと同時にデータ損失ウィンドウを減らすために、DPM は、2 回の高速完全バックアップの間に増分同期も実行します。

ファイルデータの保護の場合と同様、レプリカがそのデータソースと一致しなくなると、DPM は、どのサーバーとどのデータソースが影響を受けるかを示すアラートを生成します。この問題を解決するには、管理者は、レプリカ上で整合性チェックによる同期を開始してレプリカを修復します。整合性チェック中に、DPM はブロックごとの検証を行い、レプリカを修復してデータソースと一致する状態に戻します。

保護グループに対して毎日の整合性チェックをスケジュールしたり、または整合性チェックを手動で開始することもできます。

関連項目

ファイルデータとアプリケーションデータの違い

ディスクベースの保護プロセス

ファイルデータの同期処理

ファイルデータとアプリケーションデータの違い

ファイルサーバー上にあり、フラットファイルとして保護する必要のあるデータは、Microsoft Office ファイル、テキストファイル、バッチファイルなどのファイルデータと見なされます。

アプリケーションサーバー上にあり、DPM がアプリケーションを認識する必要のあるデータは、Exchange ストレージグループ、SQL Server データベース、Windows SharePoint Services ファーム、および仮想サーバーなどのアプリケーションデータと見なされます。

各データソースは、そのデータソースに対して選択した保護の種類に従って DPM 管理者コンソール内に表示されます。たとえば、新しい保護グループの作成ウィザードで、ファイルが保存されていて、かつ仮想サーバーと SQL サーバーのインスタンスを実行しているサーバーを展開すると、データソースは次のように扱われます。

- **すべての共有** または **すべてのボリューム** を展開すると、DPM はそのサーバー上の共有とボリュームを表示し、それらのノードのいずれかで選択したすべてのデータソースをファイルデータとして保護します。
- **すべての SQL サーバー** を展開すると、DPM はそのサーバー上の SQL サーバーのインスタンスを表示し、そのノードで選択したすべてのデータソースをアプリケーションデータとして保護します。
- **Microsoft Virtual Server** を展開すると、DPM はそのサーバー上のホストデータベースと仮想コンピュータを表示し、そのノードで選択したすべてのデータソースをアプリケーションデータとして保護します。

関連項目

アプリケーションデータの同期処理

ディスクベースの保護プロセス

ファイルデータの同期処理

テープベースの保護プロセス

短期のディスクベースの保護と長期のテープベースの保護を使用すると、DPM はレプリカボリュームからテープにデータをバックアップできるので、保護されるコンピュータは何も影響を受けずに済みます。テープベースの保護のみを使用した場合、DPM は保護されるコンピュータからテープに直接データをバックアップします。

DPM は、完全バックアップと増分バックアップの組み合わせにより、保護されるデータソース（DPM がディスク上のデータを保存しない場合は、テープを使用する短期保護用、またはテープを使用する長期保護用）または DPM レプリカ（短期保護がディスクで行われる場合は、テープを使用する長期保護用）からのデータをテープで保護します。

メモ

レプリカが最後に同期された時に開いているファイルがあった場合、レプリカからのそのファイルのバックアップはクラッシュコンシステント状態となります。ファイルのクラッシュコンシステント状態には、前回の同期の際にディスクで持続されたファイルのすべてのデータが含まれます。これが該当するのは、ファイルシステムのバックアップのみです。アプリケーションのバックアップは、常にアプリケーションの状態と一致します。

具体的なバックアップの種類とスケジュールについては、「保護グループの計画」を参照してください。

関連項目

DPM の使い方

ディスクベースの保護プロセス

回復プロセス

データ保護の方法としてディスクベースとテープベースのどちらを使用しても、回復タスクに違いはありません。回復するデータの復旧ポイントを選択すれば、保護されるコンピュータに DPM がデータを回復します。

DPM は、保護グループの各ファイルメンバーに対して最大 64 の復旧ポイントを保存できます。アプリケーションデータソースの場合、DPM は最大 448 の高速完全バックアップを、そして、各高速完全バックアップにつき最大 96 の増分バックアップを保存できます。記憶域の限界に達し、既存の復旧ポイントの保存期間が満了していない場合、保護ジョブは失敗します。

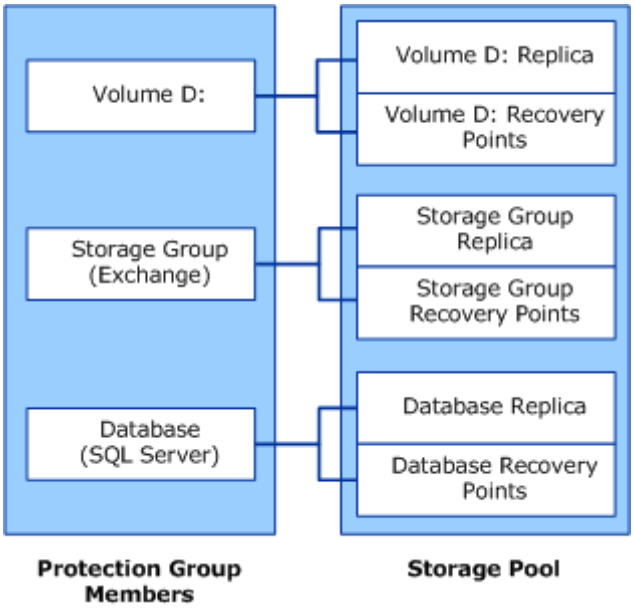
メモ

エンドユーザー回復をサポートするために、ファイルの復旧ポイントはボリュームシャドウコピーサービス（VSS）によって 64 までに制限されています。

「ファイルデータの同期処理」と「アプリケーションデータの同期処理」で説明されているように、復旧ポイントの作成手順は、ファイルデータとアプリケーションデータで異なります。DPM は、設定されたスケジュールに従ってレプリカのシャドウコピーを取ることで、ファイルデータの復旧ポイントを作成します。アプリケーションデータの場合は、同期と高速完全バックアップが実行されるたびに復旧ポイントが作成されます。

下図は、各保護グループメンバーがそれ自体のレプリカボリュームと復旧ポイントボリュームにどう関連付けられているかを示したものです。

保護グループメンバー、レプリカ、および復旧ポイント



管理者は、DPM 管理者コンソール内の回復ウィザードを使用して、使用可能な復旧ポイントからデータを回復します。データソースと回復の開始時点を選択すると、DPM はテープがオンラインかオフラインかに関係なく、データがテープ上にあるかどうか、および、回復を完了するために必要なテープを表示します。

ユーザーは、保護されたファイルの旧バージョンを回復できます。復旧ポイントには、保護されたデータソースのフォルダとファイルの構造が保持されているため、ユーザーは見慣れたボリューム、フォルダ、および共有を参照して、必要なデータを回復できます。エンドユーザー回復は、Exchange メールボックスなどのアプリケーションデータには使用できません。また、エンドユーザー回復に使用できるファイルデータのバージョンは、DPM 記憶域プール内のディスクに保存されているバージョンです。テープに保管されたファイルデータは、管理者のみが回復できます。

エンドユーザーは、シャドウコピークライアントソフトウェアを実行しているクライアントコンピュータを使用して、保護されたファイルを回復します。ユーザーは、ファイルサーバー上の共有、もしくは分散ファイルシステム（DFS）名前空間を通じて、または Microsoft Office アプリケーションの **ツール** メニューにあるコマンドを使用して、旧バージョンを回復できます。

関連項目

アプリケーションデータの同期処理

ファイルデータの同期処理

保護ポリシー

DPM は、各保護グループに対して指定された回復の目標に基づいて、各保護グループについて、保護ポリシー、またはジョブのスケジュールを設定します。回復の目標には、たとえば次のようなものがあります。

- 「運用データの損失が最大 1 時間分」
- 「保存期間を 30 日にする」
- 「データを 7 年間遡って回復できるようにする」

回復の目標は、御社のデータ保護要件を定量化するものです。DPM では、回復の目標は、保存期間、データ損失の許容範囲、復旧ポイントのスケジュール、および（データベースアプリケーションの場合は）高速完全バックアップのスケジュールによって定義されます。

保存期間とは、バックアップデータを使用可能にしておくことが必要な期間です。たとえば、今日のデータを 1 週間後まで使用可能にしておく必要がありますか? 2 週間後まで? 1 年後まで?

データ損失の許容範囲とは、ビジネス要件に照らして許容できるデータ損失の最大量（時間単位）であり、これによって、保護されたサーバーからデータ変更を集めることで DPM が保護されたサーバーとの同期をどの程度の頻度で実行するかが決まります。同期の頻度は、15 分間隔から 24 時間間隔まで自由に変更できます。指定した時間スケジュールに基づいて決めるのではなく、復旧ポイントが作成されている時点の直前に同期が実行されるように設定することも可能です。

復旧ポイントのスケジュールにより、この保護グループの復旧ポイントがいくつ作成されるかが決まります。ファイルの保護には、復旧ポイントを作成する曜日と時刻を選択します。増分バックアップをサポートするアプリケーションのデータ保護の場合は、同期の頻度によって復旧ポイントのスケジュールが決まります。増分バックアップをサポートしないアプリケーションのデータ保護の場合は、高速完全バックアップのスケジュールによって復旧ポイントのスケジュールが決まります。

メモ

保護グループを作成する際には、DPM が保護されるデータの種類を識別し、そのデータに使用できる保護オプションのみを提示します。

関連項目

DPM の使い方

自動検出プロセス

自動検出は、DPM がネットワーク上の新しいコンピュータまたは取り外されたコンピュータを自動的に検出するために行う毎日の処理です。毎日 1 回、ユーザー / 管理者が設定した時刻に、DPM は最も近いドメインコントローラに小さなパケット（10 KB 未満）を送信します。ドメインコントローラは、そのドメイン内のコンピュータと共に LDAP 要求に応答し、DPM は新しいコンピュータと取り外されたコンピュータを識別します。自動検出プロセスによって生成されるネットワークトラフィックは最小限です。

自動検出では、他のドメイン内の新しいコンピュータや取り外されたコンピュータは検出されません。別のドメイン内のコンピュータに保護エージェントをインストールするには、その完全修飾ドメインネームを使用してコンピュータを識別する必要があります。

関連項目

DPM の使い方

DPM ディレクトリ構造

DPM を使用してデータの保護を開始すると、DPM のインストールパスには、Volumes ディレクトリ内に次の 3 つのフォルダが含まれていることに気がつきます。

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

DiffArea フォルダには、データソース用の復旧ポイントが保存されているマウント済みシャドウコピーボリュームが含まれています。

Replica フォルダには、マウント済みレプリカボリュームが含まれています。

ShadowCopy フォルダには、DPM データベースのローカルバックアップコピーが含まれています。また、サードパーティのバックアップソフトウェアによるアーカイブの作成にレプリカのバックアップシャドウコピーを作成するために DPMBackup.exe を使用する場合、バックアップシャドウコピーは ShadowCopy フォルダに保存されます。

関連項目

DPM の使い方

システム要件

DPM および保護するコンピュータハードウェアとソフトウェアの要件については、「System Requirements（システム要件）（http://go.microsoft.com/fwlink/?LinkId=66731）を参照してください。

DPM ライセンス

DPM によって保護される各コンピュータに 1 つのライセンスを使用できます。ライセンスの種類は、保護されるデータの種類と関連します。

DPM には、Standard および Enterprise という 2 種類のライセンスがあります。Standard ライセンスでは、コンピュータシステムの状態に加えて、ボリューム、共有、およびフォルダを保護することができます。Enterprise ライセンスでは、ファイルに加えて、Exchange Server 上のメールボックスやデータベースなどのアプリケーションデータを保護することができます。サーバークラスタ上で、DPM はクラスタの各ノードにエージェントをインストールします。1 つのサーバーノードに対して 1 つのライセンスが使用されます。

データの種類別に適用されるライセンスを次の表に示します。

データの種類別に使用される DPM ライセンス

保護されるデータの種類	使用するライセンス
ファイルのみ	Standard
サーバークラスタのシングルノード上のファイル	Standard
システム状態	Standard
SQL サーバー （SQL サーバーを実行しているコンピュータ上の DPM 保護エージェントでは、そのコンピュータ上のすべての SQL インスタンス用のデータベースが保護できます）	Enterprise
Exchange Server	Enterprise
Windows SharePoint Services （Windows SharePoint Services ファームでは、各バックエンドサーバーに 1 つのライセンス、フロントエンド Web サーバーに 1 つのライセンスが使用されます）	Enterprise

保護されるデータの種類	使用するライセンス
仮想サーバー （仮想サーバーを実行しているコンピュータで、コンピュータにインストールされている 1 つの保護エージェントにより、ホストコンピュータ上の仮想コンピュータまたはゲストをいくつでも保護できます。仮想コンピュータ上で実行されている SQL Server のインスタンス用のデータベースを保護するなど、仮想コンピュータ内の特定のアプリケーションデータを保護するには、仮想コンピュータに保護エージェントを直接インストールする必要があります。保護エージェントがインストールされている仮想コンピュータ上のデータを保護する際には、保護されるデータの種類に対応したライセンスが使用されます。）	Enterprise
別の DPM サーバー	Enterprise
DPM システム回復ツールを使用したベアメタル回復用のデータ	Enterprise

コンピュータに保護エージェントをインストールする際には、ライセンスを使用しません。ライセンスが適用されるのは、コンピュータ上のデータが保護グループに追加されるときのみです。特定のコンピュータ上のデータを今後一切保護しない場合は、別のコンピュータ上のライセンスを再利用できます。

保護されるデータの種類が変わるときには、DPM がライセンスの使用状況を自動的に更新します。たとえば、1 台のサーバー上の Exchange ストレージグループとファイルを保護している場合は、そのサーバーを保護するために Enterprise ライセンスを使用しています。その後、Exchange ストレージグループの保護をやめたとします。DPM は現在、そのサーバーのみのファイルデータを保護しているので、ライセンスの使用状況は Standard ライセンスに変わります。

使用できるライセンスが Enterprise ライセンスしかない状況で、新しいコンピュータ上のファイルデータを保護する必要がある場合は、Enterprise ライセンスを使用できます。たとえば、Standard ライセンスとEnterprise ライセンスをそれぞれ 3 つ所有しており、 3 台のコンピュータ上のファイルデータを保護しているとします。その状況で、4 台目のコンピュータからファイルデータを保護グループに追加すると、 Standard ライセンスはすでに全部使用済みなので、DPM は Enterprise ライセンスを適用します。

DPM のインストール中に、購入されたライセンスの数を入力します。インストール後にライセンス情報をアップデートします。DPM 管理者コンソールの **保護** タスク領域にある **アクション** ペインで、**View DPM licenses**（DPM ライセンスの表示）をクリックし、購入されたライセンスの数を変更します。

追加の DPM ライセンスは、「Microsoft Partner Program」（Microsoft パートナープログラム）（http://go.microsoft.com/fwlink/?LinkId=71663）から購入できます。

保護グループの計画

Microsoft System Center Data Protection Manager (DPM) 2007 の効果的な導入計画を立てるには、御社のデータ保護と回復に関する要件を入念に検討し、それらの要件を DPM の機能に照らして比較検討する必要があります。

本項では、保護グループのメンバーシップと構成の計画に必要な情報を提供します。保護グループ構成の一環として、保護されるデータの回復の目標を定義します。

Microsoft Operations Framework（MOF）のコンテキストで、本項では、変更（DPM を御社に組み込んでデータ保護と回復を提供すること）が承認済みで、ユーザー / 管理者のタスクが変更の実装計画であることを前提としています。

MOF の変更管理の詳細については、「Service Management Functions: Change Management（サービス管理機能：変更管理）（http://go.microsoft.com/fwlink/?LinkId=68729）を参照してください。

本項では、御社の既存の障害回復戦略に DPM を追加する予定であることも前提としています。障害回復戦略の計画の詳細については、「Introduction to Backup and Recovery Services」（バックアップサービスおよび回復サービスの入門）（http://go.microsoft.com/fwlink/?LinkId=71721）を参照してください。

本項の内容

何を保護するか?

DPM 導入計画の手始めに、どのデータを保護するかを決める必要があります。DPM 2007 では、次のデータの種類を保護できます。これらは、以下のトピックで詳しく説明されています。

- Microsoft Windows Server 2003 または Windows Server 2008 を実行しているファイルサーバー上の（ボリューム、フォルダ、および共有レベルの）ファイルデータ
- Microsoft Windows XP Professional SP2、および Home エディションを除く Windows Vista のすべてのエディションのいずれかを実行しているワークステーション上のファイルデータ
- Microsoft Exchange Server 2003 SP2 および Exchange Server 2007 の（ストレージグループレベルの）データ
- Microsoft SQL Server 2000 SP4、SQL Server 2005 SP1、および SQL Server 2005 SP2 の（データベースレベルの）データ
- Windows SharePoint Services 3.0 および Microsoft Office SharePoint Server 2007（ファームレベル）

- Microsoft Virtual Server 2005 R2 SP1 ホストおよびゲストの構成
- システム状態

関連項目

アプリケーションデータ
クラスタリソース
サーバーとワークステーションのファイルデータ
システム状態

サーバーとワークステーションのファイルデータ

ドライブ文字またはマウントポイントによってアクセスできるボリューム、およびフォルダ、共有を保護することができます。

保護対象のデータを選択するのに最も単純な方法は、現在のバックアップに含めるすべてのファイルデータを選択することです。または、データの特定の部分を保護の対象として選択することも可能です。

データを選択する際に検討すべき主たる要素は、データが失われたり破損したりした場合に、データの時間指定コピーを緊急に回復する必要性です。保護の対象とすべき主な候補は、頻繁に変更されるファイルです。変更の頻度には関係なく、頻繁にアクセスするファイルが次の候補です。

重要

ファイルサーバーのボリュームは通常 NTFS としてフォーマットされますが（DPM 保護にはこのフォーマットが必須です）、ワークステーションのボリュームが FAT または FAT32 としてフォーマットされることは少なくありません。これらのボリュームを保護するには、NTFS に変換する必要があります。手順については、「How to Convert FAT Disks to NTFS」（FAT ディスクを NTFS に変換する方法）（http://go.microsoft.com/fwlink/?LinkId=83022）を参照してください。

関連項目

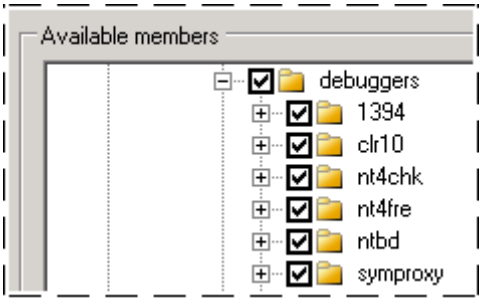
ファイルとフォルダの除外
DFS 名前空間内のデータの保護
サポートされていないデータ型
何を保護するか?

ファイルとフォルダの除外

指定したフォルダを除外するようにデータ保護を設定することができます。また、ファイル名の拡張子によって特定のファイルの種類を除外することもできます。

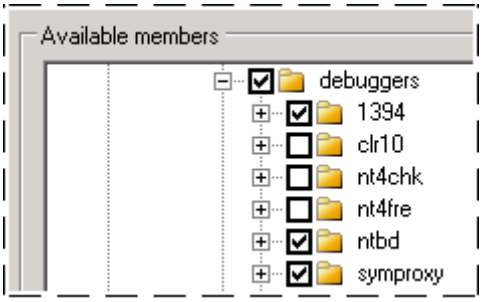
保護するボリュームまたは共有を選択すると、下図に示すように、そのボリュームまたは共有内の保護可能な子のアイテムがすべて自動的に選択されます。

自動的に選択されたすべての子アイテム



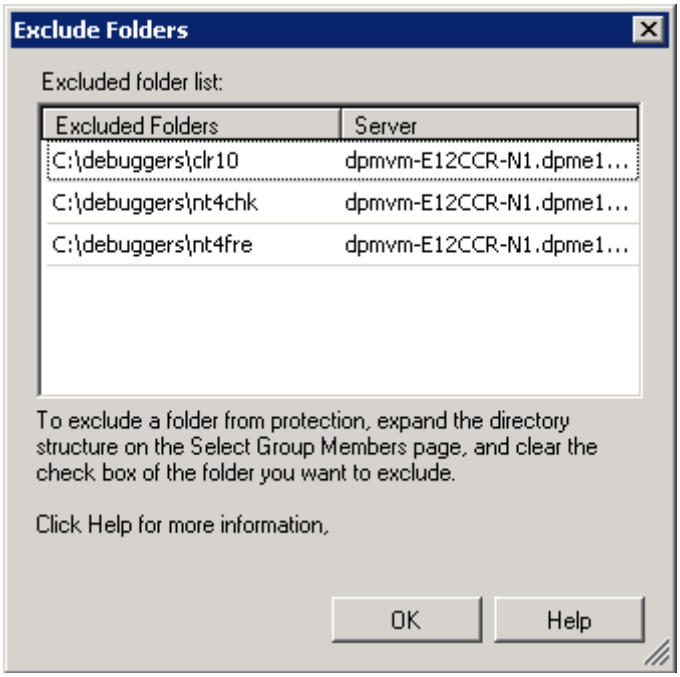
保護の対象から特定のフォルダを除外するには、保護しないフォルダの親フォルダが選択されていることを確認し、下図に示すように、保護しないフォルダのチェックボックスをオフにします。

保護から除外されたフォルダ



保護グループのメンバーの選択を終えたら、除外されたフォルダを下図のように確認できます。

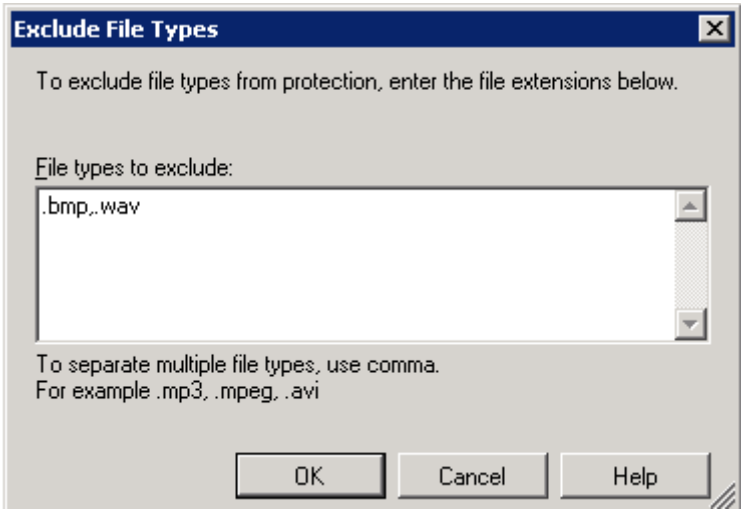
除外されたフォルダの確認



保護グループのレベルで、保護から除外するファイルのファイル名拡張子を指定するという方法もあります。たとえば、ファイルサーバーには、会社が保護のためにディス領域またはネットワーク帯域幅を使用すべきでない音楽ファイルや個人的なファイルが含まれている場合があります。ファイル名の拡張子による除外は、保護グループのすべてのメンバーに適用されます。

ファイル名の拡張子によってファイルを保護から除外する方法を下図に示します。

ファイル名の拡張子による除外



関連項目

DFS 名前空間内のデータの保護

サポートされていないデータ型

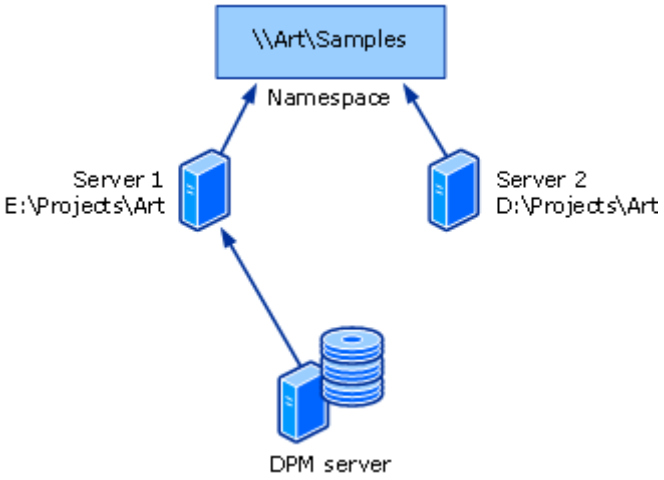
DFS 名前空間内のデータの保護

分散ファイルシステム（DFS）名前空間階層の一部となっているデータを保護することができます。ただし、DFS 名前空間階層を通じて保護する共有を選択することはできません。保護する共有を選択する唯一の方法は、ターゲットパスを使用する方法です。

名前空間に、同じデータが入っている複数のターゲットを持つルートまたはリンクが含まれている場合は、ターゲットの 1 つのみを保護することをお勧めします。同じデータが入っている複数のターゲットを保護することは不必要です。

下図は、DFS 名前空間ターゲットの DPM 保護を示したものです。

DPM を使用した DFS 名前空間ターゲットの保護



保護されるターゲットに対してエンドユーザー回復が有効になっている場合、ユーザーは DFS 名前空間階層を通じてファイルの旧バージョンにアクセスできます。エンドユーザーが、複数のターゲットを持つ共有上のファイルの旧バージョンへのアクセスを試みると、DPM はそれらのファイルを保護されるターゲットに透過的に転送します。

関連項目

ファイルとフォルダの除外

サポートされていないデータ型

サポートされていないデータ型

保護されるデータソースにサポートされていないデータ型が含まれている場合、DPM は影響を受けるデータソース内のサポートされているデータ型を引き続き保護しますが、サポートされていないデータは保護しません。

DPM が、保護されるデータソース内にサポートされていない次のデータ型のいずれかを検出した場合、影響を受けるデータは保護されません。

- ハードリンク
- DFS リンクと接続点を含む再解析ポイント

  重要

  保護グループには、マウントポイントのあるデータが含まれている場合があります。保護グループ内にマウントポイントが含まれている場合、DPM はマウントポイントのターゲットであるマウントされたボリュームを保護しますが、マウントポイントメタデータは保護しません。マウントポイントを含むデータを回復するときは、マウントポイント階層を手動で再作成する必要があります。DPM は、マウントされたボリューム内のマウントされたボリュームの保護はサポートしていません。
- ごみ箱
- ページングファイル
- システムボリューム情報フォルダ

  メモ

  システムボリューム情報フォルダは、ファイルデータソースとして保護することができません。コンピュータのシステム情報を保護するには、新しい保護グループの作成ウィザードで、コンピュータのシステム状態を保護グループメンバーとして選択する必要があります。
- NTFS でフォーマットされていないボリューム

ファイルに Windows Vista からのハードリンクやシンボリックリンクが含まれている場合、DPM はファイルのレプリケーションや回復を行うことができません。

ファイルの属性に以下のいずれかの組み合わせが存在する場合、DPM はそのファイルを保護できません。

- 暗号化と再解析
- 暗号化と単一インスタンス記憶域（SIS）
- 暗号化と大文字小文字の区別
- 暗号化とスパース
- 大文字小文字の区別と SIS
- スパースと再解析
- 圧縮と SIS

関連項目

ファイルとフォルダの除外

DFS 名前空間内のデータの保護

アプリケーションデータ

DPM を使用して次の種類のアプリケーションデータを保護できます。

- **Exchange Server のストレージグループ。**DPM は、Microsoft Exchange Server 2003 SP2 およびExchange Server 2007 用のストレージグループを保護できます。
  - 選択したストレージグループ内のどのデータベースも保護から除外することはできません。
  - Exchange Server 2003 を実行しているコンピュータ上のすべてのストレージグループは、同じ保護グループのメンバーである必要があります。そうでないと、これらのストレージグループの保護は失敗します。
  - 保護されるストレージグループについては、循環ログを無効にする必要があります。
- **SQL Server データベース。**DPM は、Microsoft SQL Server 2000 SP4、SQL Server 2005 SP1、および SQL Server 2005 SP2 用のデータベースを保護できます。
  - SQL Server のインスタンス内の各データベースは、同一のまたは異なる保護グループに所属することができます。
  - 選択したデータベース内のどのデータも保護から除外することはできません。
- DPM では、以下のデータベースについては増分バックアップに対応していません。
  - SQL Server 2000 および SQL Server 2005 のマスターデータベース
  - SQL Server 2000 の msdb データベース
  - SQL Server 2000 のモデルデータベース
- **Windows SharePoint Services のデータ。**DPM は、Windows SharePoint Services 3.0 または Office SharePoint Server 2007 を実行しているサーバーについて、サーバーファームを保護することができます。
  - 選択したファーム内のどのデータも保護から除外することはできません。
- **仮想サーバーと仮想コンピュータ。**DPM は、仮想サーバーホスト（Virtual Server 2005 R2 SP1 を実行しているコンピュータ）およびゲスト、または、そのホストのコンテキストで実行されている仮想コンピュータを保護することができます。

また、DPM はゲストで実行されているアプリケーションのデータを保護することができます。ただし、仮想コンピュータで実行されているアプリケーションのデータは、保護される仮想コンピュータのコンポーネントとしてではなく、アプリケーションのデータソースとして保護し、回復する必要があります。たとえば、仮想コンピュータで実行されている SQL Server のインスタンス用のデータを保護し、回復するには、データソースを SQL Server データベースとして選択します。仮想コンピュータを保護するとアプリケーションデータも保護されますが、仮想コンピュータ自体を回復することによってのみ回復が可能です。

関連項目

クラスタリソース
サーバーとワークステーションのファイルデータ
システム状態

クラスタリソース

DPM は、以下の共有ディスククラスタを保護することができます。

- ファイルサーバー
- SQL Server 2000 with Service Pack 4（SP4）
- SQL Server 2005 with Service Pack 1（SP1）
- Exchange Server 2003 with Service Pack 2（SP2）
- Exchange Server 2007

DPM は、Exchange Server 2007 の非共有ディスククラスタを保護できます（クラスタ連続レプリケーション）。DPM は、ローカル連続レプリケーション用に設定された Exchange Server 2007 も保護することができます。

関連項目

アプリケーションデータ
サーバーとワークステーションのファイルデータ
システム状態

システム状態

DPM は、Windows Vista または Windows Server 2008 を実行しているコンピュータを除いて、DPM 保護エージェントがインストールできるどのコンピュータについても、システム状態を保護することができます。

ワークステーションとメンバーサーバーのシステム状態

DPM がワークステーションまたはメンバーサーバーのシステム状態をバックアップすると、次のコンポーネントが保護されます。

- 起動ファイル
- COM+ クラス登録データベース
- レジストリ
- Windows ファイル保護の下にあるシステムファイル

ドメインコントローラのシステム状態

DPM がドメインコントローラのシステム状態をバックアップすると、次のコンポーネントが保護されます。

- Active Directory ドメインサービス（NTDS）
- 起動ファイル
- COM+ クラス登録データベース
- レジストリ
- システムボリューム（SYSVOL）

証明書サービスのシステム状態

証明書サービスがインストールされた状態で DPM がメンバーサーバーまたはドメインコントローラのシステム状態をバックアップする場合、メンバーサーバーまたはドメインコントローラのシステム状態のコンポーネントに加えて、証明書サービスが保護されます。

クラスタサーバーのシステム状態

DPM がクラスタサーバーのシステム状態をバックアップする場合、メンバーサーバーのシステム状態のコンポーネントに加えて、クラスタサービスメタデータが保護されます。

関連項目

アプリケーションデータ
クラスタリソース
サーバーとワークステーションのファイルデータ

回復の目標

データ保護の計画を立てる際には、保護する各データソースについて現実的な回復の目標を設定する必要があります。御社のコンピュータに保存されているすべての情報またはデータが同等の保護を必要とするわけではなく、そのすべてが保護のために同じ投資を行うに値するわけでもありません。導入計画では、そのようなデータを保護するビジネスニーズに従って、各データソースに対する回復の目標を立てる必要があります。

DPM では、同期の頻度、復旧ポイントのスケジュール、および保存期間の面から、次のように回復の目標を設定します。

- 同期の頻度は、データ損失の許容範囲（失っても支障のないデータの量）に基づいて選択します。保護グループの同期が、最短では 15 分ごとに行われるように指定することが可能です。同期の頻度を少なくすることも可能です。DPM は復旧ポイントと次の復旧ポイントの間で少なくとも 1 回、保護グループのレプリカを同期する必要があります。
- 復旧ポイントのスケジュールにより、このデータの復旧ポイントがいくつ、そしていつ作成されるかが決まります。復旧ポイントとは、DPM によって管理されるメディアから回復に使用できるデータソースのバージョンに関する日時です。
- 保存期間とは、バックアップデータを使用可能にしておくことが必要な期間です。保存期間のニーズを判断するには、社内における回復要求のパターンを考慮してください。回復要求がデータの損失から 2 週間以内に集中している場合は、保存期間は 10 日ぐらいが適しているでしょう。回復要求の集中している時期がもっと遅い場合は、保存期間を長めにする必要があります。

たとえば、特定の Exchange Server データベースに設定する回復の目標は、保存されている最新のデータがどんな場合も 30 分以上は経過しておらず、30 分間隔で作成される複数のバージョンから選択でき、ディスクからの回復が 14 日間有効で、テープからの回復が 3 年間有効、という具合に設定できます。

関連項目

保護構成の計画
ディスクベースの保護に関する回復の目標
テープベースの保護に関する回復の目標
何を保護するか?

ディスクベースの保護に関する回復の目標

保護グループのすべてのメンバーが同じ同期の頻度を共有しているものの、同期処理および結果として出来上がる復旧ポイントのスケジュールは、保護されるデータの種類によって異なります。詳細については、「DPM の使い方」を参照してください。

ファイルの同期と復旧ポイント

ファイルボリュームまたは共有に対して、保護されるコンピュータ上の保護エージェントは、変更されたブロックをオペレーティングシステムの一部である変更ジャーナルに記録します。同期中にこれらの変更は DPM サーバーに転送され、レプリカをデータソースと同期するためにレプリカに適用されます。

同期の頻度は、15 分間隔から 24 時間間隔まで自由に選択できます。デフォルトは 15 分間です。復旧ポイントが作成される前にのみ同期が実行されるように設定することも可能です。

ファイルデータのレプリカのシャドウコピーである復旧ポイントは、設定可能なスケジュールに基づいて同期されたレプリカから作成されます。各復旧ポイントの前にだけ同期を実行するのでない限り、ファイルの同期処理が実行されると、毎回復旧ポイントが作成されるわけではありません。ただし、最新のファイルの同期処理から復旧ポイントを手動で作成することは可能です。

たとえば、あるボリュームの同期が毎時行われ、そのボリュームの復旧ポイントが 8:00 AM、12:00 PM、6 PM に作成されるとします。ユーザーがそのボリューム上のファイルに 1:30 PM に変更を施しますが、1 時間後に別のユーザーが変更を施したときにファイルが不意に破損します。そこで管理者は、最初のユーザーが変更を施した状態のファイルを回復するように求められます。1:30 PM の変更は、最新の復旧ポイントが 12:00 PM に作成された後で行われたため、最新の復旧ポイントからファイルを回復することはできません。ただし、そのレプリカの適切な同期から復旧ポイントを手動で作成した後で、その新しい復旧ポイントからファイルを回復することはできます。

既定のスケジュールでは、毎日 8:00 AM、12:00 PM、6:00 PM に復旧ポイントが作成されます。時刻と曜日のどちらも変更できます。曜日ごとに異なる時刻を指定することはできません。たとえば、平日のみに 2:00 AM と 2:00 PM に復旧ポイントを設定することはできますが、平日には2:00 AM、週末には 12:00 PM というような復旧ポイントのスケジュール設定はできません。

ファイルの保存期間

保存期間とは、回復のためにデータを使用可能にしておく期間のことです。復旧ポイントの保存期間が切れると、復旧ポイントは削除されます。

短期のディスクベースの保護には 1 ～ 448 日、短期のテープベースの保護には最長 12 週、長期のテープベースの保護には最長 99 年の保存期間を選択できます。DPM は、保護グループの各ファイルメンバーに対して最大 64 の復旧ポイントを保存できます。

たとえば、復旧ポイントの前に毎回同期を行い、毎日 6 つの復旧ポイントを設定し、保存期間を 10 日に設定した場合、その保護グループ内のファイルの復旧ポイントが 64 を超えることはありません。ただし、復旧ポイントの限度である 64 を超える設定の組み合わせを試みると、選択内容を変更できるように、構成処理中に DPM が警告を発します。ファイルに対して、復旧ポイントの限度である 64 を超える保護構成を設定することはできません。

アプリケーションデータの同期と復旧ポイント

アプリケーションデータの場合は、アプリケーションファイルに属するボリュームブロックに対する変更がボリュームフィルタによって追跡されます。アプリケーションデータの同期は増分バックアップのようなもので、レプリカと組み合わせるとアプリケーションデータの正確なリフレクションが作成されます。

同期の頻度は、15 分間隔から 24 時間間隔まで自由に選択できます。デフォルトは 15 分間です。復旧ポイントが作成される前にのみ同期が実行されるように設定することも可能です。復旧ポイントが作成される前のみに同期が実行されるように設定すると、DPM は復旧ポイントのスケジュールに従って高速完全バックアップを実行し、レプリカを同期します。

増分バックアップをサポートするアプリケーションの場合は、既定のスケジュールを使用すると、毎回の同期（15 分間隔）と毎日 8:00 PM の高速完全バックアップに対して復旧ポイントが作成されます。増分バックアップをサポートしないアプリケーションの場合は、既定のスケジュールを使用すると、毎日 8:00 PM の高速完全バックアップに対して復旧ポイントが作成されます。

時刻と曜日のどちらも変更できます。曜日ごとに異なる時刻を指定することはできません。たとえば、平日のみに 2:00 AM と 2:00 PM に復旧ポイントを設定することはできますが、平日には 2:00 AM、週末には 12:00 PM というような復旧ポイントのスケジュール設定はできません。

一部の SQL Server データベースの例外

DPM がアプリケーションデータの増分同期に使用するトランザクションログのバックアップは、読み取り専用か、ログシップ用に設定されているか、または単純復旧モデルを使用するように設定された SQL Server データベースに対しては実行できません。それらの SQL Server データベースの場合、復旧ポイントは各高速完全バックアップに対応します。

同期と高速完全バックアップの比較

回復時間を短縮できるように、DPM は増分同期の代わりに高速完全バックアップを定期的に実行します。高速完全バックアップは、変更されたブロックが含まれるようにレプリカをアップデートする同期の種類です。

メモ

保護 タスク領域にある **パフォーマンスの最適化** アクションを使用するか、またはグループの変更ウィザードを使用して、アプリケーションデータが含まれているどの保護グループについても、高速完全バックアップのスケジュールを変更できます。

アプリケーションデータの保存期間

短期のディスクベースの保護には 1 ～ 448 日、短期のテープベースの保護には最長 12 週、長期のテープベースの保護には最長 99 年の保存期間を選択できます。

たとえば、15 分ごとに同期が実行される設定で保存期間を 10 日に設定した場合、データ保護を設定してから最初の 10 日が経過すると、その保護グループ内にアプリケーションデータの復旧ポイントが 960 ポイント維持される保護計画ができることになります。

関連項目

テープベースの保護に関する回復の目標

テープベースの保護に関する回復の目標

DPM は、完全バックアップと増分バックアップの組み合わせにより、保護されるデータソース（DPM がディスク上のデータを保存しない場合は、テープを使用する短期保護用、またはテープを使用する長期保護用）または DPM レプリカ（短期保護がディスクで行われる場合は、テープを使用する長期保護用）からのデータをテープで保護します。

保存期間、バックアップの頻度、および回復オプションの選択内容は、短期と長期の保護で異なります。

メモ

短期保護用にディスクとテープのどちらを選択することも可能ですが、両方を選ぶことはできません。

テープを使用する短期保護

テープで短期のデータ保護を行う場合、保存期間は 1 ～ 12 週の範囲で選択できます。DPM では、アラートとレポートを通じてテープの管理がサポートされています。また、ユーザー / 管理者の指定による保存期間を使用して各テープの有効期限が確立されます。

バックアップ頻度は、保存期間に応じて、毎日、毎週、または隔週を選択できます。

増分バックアップと完全バックアップの両方を使用してテープで短期保護を行う設定にすると、完全バックアップと増分バックアップの依存関係により、保存期間は指定した期間よりも（最長で 1 週間）長くなります。完全バックアップが保存されているテープは、従属する増分のテープがすべてリサイクルされた後に初めてリサイクルされます。完全バックアップは週に一度行われ、増分バックアップは毎日行われるため、毎週の完全バックアップテープは、完全バックアップテープがリサイクルされる前に、6 回分の毎日の増分バックアップテープがリサイクルされるまで待つ必要があります。増分バックアップが失敗し、リサイクルする増分テープがない場合は、完全バックアップテープのリサイクルが早めに行われます。

テープを使用する長期保護

長期のデータ保護（別名テープアーカイブ）を行う場合、保存期間は 1 週 ～ 99 年まで設定できます。DPM では、アラートとレポートを通じてテープアーカイブの管理がサポートされています。また、ユーザー / 管理者の指定による保存期間を使用して各テープの有効期限が確立されます。

バックアップの頻度は、次の一覧に示すように指定した保存期間に応じて異なります。

- 保存期間が 1 ～ 99 年の場合、バックアップの頻度は、毎日、毎週、隔週、毎月、年 4 回、毎年のいずれかを選択できます。
- 保存期間が 1 ～ 11 か月の場合、バックアップの頻度は、毎日、毎週、隔週、毎月のいずれかを選択できます。
- 保存期間が 1 ～ 4 週間の場合、バックアップの頻度は、毎日または毎週を選択できます。

関連項目

ディスクベースの保護に関する回復の目標

保護構成の計画

保護の必要なデータソースを識別し、回復の目標を設定したら、次のステップは、データソースを保護グループとしてまとめることができるように、収集した情報を分析することです。

保護グループとは、同じ保護構成を共有するデータソースの集まりです。保護構成は、保護グループの名前、ディスク割り当ての設定、レプリカの作成方法、送信中の圧縮から成ります。

保護グループを計画するには、次の決定を下す必要があります。

- どのデータソースを保護グループに含めるか?
- 保護グループにどの保護方法（ディスクベース、テープベース、または両方）を使用するか?
- 保護グループのメンバーに関する回復の目標は?
- 選択したデータを保護するのに必要な記憶域の大きさは?
- どのテープとライブラリを使用すべきか?
- 保護グループのメンバー用のレプリカの作成に使用する方法は?

本項のトピックは、保護グループの作成に関連する意思決定のガイドラインを示すものです。

本項の内容

関連項目

回復の目標
何を保護するか?

保護グループメンバーの選択

Data Protection Manager (DPM) 2007 では、データソースを保護グループとしてまとめるために以下のアプローチが選択できます。

- **コンピュータごと** — 1 台のコンピュータのすべてのデータソースを同一の保護グループに含める。
  - このアプローチの利点は、1 台のコンピュータの全データを同一の保護グループに含めることで、パフォーマンス負荷の調整ポイントが 1 つで済むことです。
  - このアプローチには、そのコンピュータ上のある種類のデータソースすべてに同じ回復の目標を割り当てなければならないという制約があります。
- **データ型ごと** — ファイルと各アプリケーションデータ型を別々の保護グループに分ける。
  - このアプローチには、データ型をグループとして管理できるという利点があります。
  - このアプローチの制約は、1 台のサーバーを回復するのに複数の保護グループからの複数のテープが必要な場合があることです。

その名が示すとおりに、保護グループのすべてのメンバーが回復の目標を共有します。つまり、保護グループ内の同種のすべてのデータソースが持つ保存期間とデータ損失の許容範囲が、同一でなければならないのです。

スタンドアロンテープが 1 本しかない場合は、テープを変更する手間を最小限に抑えるために、保護グループを 1 つだけにしてください。複数の保護グループを使用すると、各保護グループに対して別々のテープが必要です。

保護グループのガイドライン

保護グループの構造を設計する際には、次のガイドラインと制限に留意してください。

- 1 台のコンピュータ上のデータソースは、同一の DPM サーバーによって保護される必要があります。DPM においては、データソースは、保護グループのメンバーであるボリューム、共有、データベース、またはストレージグループです。
- 複数のコンピュータからのデータソースを 1 つの保護グループに含めることができます。
- 親フォルダまたは親共有を選択すると、そのサブフォルダが自動的に選択されます。除外するサブフォルダを指定することも、拡張子によって除外するファイルの種類を指定することも可能です。
- 1 つのボリューム内の保護可能なデータソースが 100 を超えていないことを確認してください。超えている場合は、可能なら、データソースを分散するボリュームの数を増やしてください。
- 同じ種類の保護グループメンバー（ファイルまたはアプリケーションデータ）のすべてが同じ回復の目標を持つことになります。ただし、同一の保護グループ内で、ファイルとアプリケーションデータで回復の目標が異なる場合があります。

  例外：SQL Server データベースが単純復旧モデルを使用するように設定されているか、またはログシップペア内のプライマリデータベースである場合、そのデータベースの回復の目標は、その他すべてのアプリケーションデータの回復の目標とは別に設定されます。
- Exchange Server 2003 を実行しているコンピュータ上のすべてのストレージグループは、同じ保護グループのメンバーである必要があります。
- 再解析ポイント（マウントポイントと接続点は再解析ポイントを含むデータソースです）を含むデータソースを選択すると、DPM は、再解析ポイントのターゲットを保護グループに含めるかどうかを指定するように求めます。再解析ポイント自体はレプリケートされません。データを回復する際に、再解析ポイントを手動で作成し直す必要があります。

ワークステーション上のデータを保護する際の考慮事項

ユーザーワークステーション上のデータの回復の目標は、ファイルサーバー上のデータの回復の目標とは異なる可能性があります。同期スケジュールを別々に調整できるように、ファイルサーバーとワークステーションは別々の保護グループに入れることを検討してください。たとえば、ファイルサーバー上のデータを 15 分間隔で同期する場合、ファイルサーバーと同じ保護グループに含まれるワークステーションはすべて、同じように 15 分間隔で同期されます。

WAN を介してデータを保護する際の考慮事項

ネットワークの使用帯域幅の調整と送信中の圧縮は、DPM サーバーがワイドエリアネットワーク（WAN）またはその他の低速ネットワークを介してデータを保護する導入にとって特に重要な、パフォーマンス最適化のための機能です。

送信中の圧縮は、保護グループのレベルで設定します。

ネットワークの使用帯域幅の調整は、保護されるコンピュータのレベルで設定します。また、勤務時間、勤務時間以外、および週末に対して異なるネットワークの使用帯域幅の調整速度を指定し、これらの各カテゴリーに時間を定義することができます。

Exchange ストレージグループまたは SQL Server データベースなどのアプリケーションデータを WAN を介して保護する際には、高速完全バックアップのスケジュールを減らすことを検討してください。

保護グループのメンバーシップの決定はどの程度重要か?

保護グループのメンバーは、別の保護グループに移動することができません。保護グループのあるメンバーを後に別の保護グループに移動しなければならなくなった場合は、所属している保護グループからそのメンバーを削除し、別の保護グループに加える必要があります。

ある保護グループのメンバーが保護を必要としなくなった場合は、その保護グループの保護を停止できます。保護を停止する際には、保護されていたデータを保持しておくか、または削除するかを選択します。

- **保護されていたデータを保持するオプション**：指定した保存期間にわたって、ディスク上のレプリカを関連する復旧ポイントおよびテープと共に保持します。
- **保護されていたデータを削除するオプション**：ディスク上のレプリカを削除し、テープ上のデータを失効させます。

関連項目

保護構成の計画

データ保護方法の選択

Data Protection Manager (DPM) 2007 では、次のデータ保護方法が使用できます：ディスクベース（D2D）、テープベース（D2T）、またはディスクベースとテープベースの組み合わせ（D2D2T）。

データ保護方法は、保護グループのレベルで設定します。2 つのデータソースの保護に異なる方法を使用する場合、2 つのデータソースを同じ保護グループに含めることはできません。

次の表に、各方法の長所と短所を比較して示します。

データ保護方法の比較

方法	長所	短所	どんな場合に使用するか
ディスクベースの保護のみ	• データ回復の速度。 • データバックアップの速度。 • バックアップにエラーの発生する可能性が低い。 • RAID などのテクノロジを使用してエラーを処理する冗長性。 • テープ交換などの手動による対応が少なくて済む。	• コストが高く、オフサイトでの保管が不便なため、ディスクはアーカイブのニーズに応える決定版ではない。	• データ損失の許容範囲が狭い場合。 • 回復時間を短縮する必要がある場合。
テープベースの保護のみ	• セキュリティ目的、および障害回復のための代替計画として、オフサイトでの保管が可能。 • テープの追加による容量の追加が容易。	• 回復プロセスが遅く、手間がかかる。 • エラーが発生しがち。	• データ損失の許容範囲があまり狭くない場合。 • 回復時間の目標が厳しくない場合。 • 頻繁に変更されず、あまり頻繁なバックアップを必要としないデータ用。 • 保存期間が長い場合。
ディスクベースとテープベースの両方による保護	• 両方の短所を相殺しつつ、両方の利点を得る。 • 管理ポイントが 1 箇所で済む。		

関連項目

[保護構成の計画]

回復の目標の定義

DPM 保護グループのメンバーとデータ保護に使用する方法を選択したら、その保護グループ内のデータファイルとアプリケーションデータの回復の目標を定義します。

回復の目標は、保存期間、同期の頻度、復旧ポイントのスケジュールを設定することで定義されます。DPM には回復の目標の既定値がありますが、設定は一部またはすべてを変更できます。

スケジュールされた 2 つの復旧ポイントの間で、同期が少なくとも 1 回は実行されるようにスケジュールする必要があります。たとえば、同期の頻度を 45 分間隔に設定した場合、 復旧ポイントが 1:00 PM と 1:30 PM に作成されるように設定することはできません。この 2 つの復旧ポイントの間で同期が 1 度も実行されないからです。

SQL サーバーが単純復旧モデルを使用するように設定されているか、またはログシップペア内のプライマリサーバーである場合、そのサーバー上で保護されるすべてのデータベースの復旧ポイントは、高速完全バックアップのスケジュールに従って作成されます。

本項の以下のトピックでは、回復の目標を計画する方法について詳しく説明します。

- 各保護方法における回復の目標のオプション
- 長期保護用の復旧ポイントのスケジュール
- 長期保護用のスケジュールのオプション
- 長期保護に使用する回復の目標のカスタマイズ

関連項目

保護構成の計画

各保護方法における回復の目標のオプション

DPM の各保護方法における回復の目標のオプションを次の表に示します。

保護方法における回復の目標のオプション

保護方法	保存期間	同期の頻度またはバックアップのスケジュール	復旧ポイント
ディスクを使用する短期保護	1 ～ 448 日	15 分 ～ 24 時間の間で頻度を選択するか、または **復旧ポイントの直前** を選択。.	特定の同期の頻度が選択されている場合は、次の処理が実行されます。 • ユーザー / 管理者が設定するスケジュールに従って、ファイルの復旧ポイントが作成されます。 • 同期が実行されるたびに、アプリケーションデータの復旧ポイントが作成されます。 **復旧ポイントの直前** を選択している場合は、ユーザー / 管理者が設定するスケジュールに従って、すべての保護グループメンバーの復旧ポイントが作成されます。
テープを使用する短期保護	1 ～ 12 週間	次のバックアップ間隔を選択。 • 毎日 • 毎週 • 隔週	復旧ポイントの代わりに、次のバックアップの種類からいずれか 1 つを設定します。 • 完全 / 増分バックアップ • 完全バックアップのみ 毎週または隔週を選択すると、使用できるのは完全バックアップのみです。曜日と時刻を指定します。 毎日の完全バックアップを選択する場合は、時刻を指定します。 毎日の完全 / 増分バックアップを選択する場合は、完全バックアップと増分バックアップの曜日と時刻を指定します。

保護方法	保存期間	同期の頻度またはバックアップのスケジュール	復旧ポイント
テープを使用する長期保護	最短：1 週間 最長：99 年間	次のバックアップ間隔を選択。 • 毎日 • 毎週 • 隔週 • 毎月 • 年 4 回 • 年 2 回 • 毎年	「長期保護用の復旧ポイントのスケジュール」および「長期保護に使用する回復の目標のカスタマイズ」を参照してください。

関連項目

回復の目標の定義

長期保護用の復旧ポイントのスケジュール

さまざまな長期保護の組み合わせを用いた DPM 復旧ポイントのスケジュールを次の表に示します。

長期保護用の復旧ポイントのスケジュール

バックアップ頻度と保存期間	復旧ポイントのスケジュール
毎日、1 ～ 4 週間	完全バックアップを毎日
毎日、1 ～ 11 か月	毎日 1 回の完全バックアップを 4 週間 最初の 4 週間経過後、毎月 1 回の完全バックアップ
毎日、1 ～ 99 年間	毎日 1 回の完全バックアップを 4 週間 最初の 4 週間経過後、12 か月目まで毎月 1 回の完全バックアップ 最初の 11 か月経過後、毎年 1 回の完全バックアップ
毎週、1 ～ 4 週間	完全バックアップを毎週

バックアップ頻度と保存期間	復旧ポイントのスケジュール
毎週、1 ～ 11 か月	毎週 1 回の完全バックアップを 4 週間 最初の 4 週間経過後、毎月 1 回の完全バックアップ
毎週、1 ～ 99 年間	毎週 1 回の完全バックアップを 4 週間 最初の 4 週間経過後、12 か月目まで毎月 1 回の完全バックアップ 最初の 11 か月経過後、毎年 1 回の完全バックアップ
隔週、1 ～ 11 か月	隔週1 回の完全バックアップを 4 週間 最初の 4 週間経過後、毎月 1 回の完全バックアップ
隔週、1 ～ 99 年間	隔週1 回の完全バックアップを 4 週間 最初の 4 週間経過後、12 か月目まで毎月 1 回の完全バックアップ 最初の 11 か月経過後、毎年 1 回の完全バックアップ
毎月、1 ～ 11 か月	完全バックアップを毎月
毎月、1 ～ 99 年間	12 か月目まで、毎月 1 回の完全バックアップ 最初の 11 か月経過後、毎年 1 回の完全バックアップ
隔週、1 ～ 99 年間	12 か月目まで、3 か月ごとに 1 回の完全バックアップ 最初の 11 か月経過後、毎年 1 回の完全バックアップ
年 2 回、1 ～ 99 年間	12 か月目まで、6 か月ごとに 1 回の完全バックアップ 最初の 11 か月経過後、毎年 1 回の完全バックアップ
毎年、1 ～ 99 年間	完全バックアップを毎年

関連項目

[回復の目標の定義]

長期保護用のスケジュールのオプション

DPM を使用した長期保護用のスケジュールの変更可能なオプションを次の表に示します。

長期保護用のスケジュールのオプション

このバックアップ頻度用	保存期間に応じて、次の設定が可能です。
毎日	• 毎日バックアップの時刻 • 毎月バックアップの特定の日付または曜日、および時刻 • 毎年バックアップの特定の日付または曜日、および時刻
毎週	• 毎週バックアップの時刻および曜日 • 毎月バックアップの特定の日付または曜日、および時刻 • 毎年バックアップの特定の日付または曜日、および時刻
隔週	• 隔週バックアップの時刻および曜日 • 毎月バックアップの特定の日付または曜日、および時刻 • 毎年バックアップの特定の日付または曜日、および時刻
毎月	• 毎月バックアップの特定の日付または曜日、および時刻 • 毎年バックアップの特定の日付または曜日、および時刻
年 4 回	• 年 4 回のバックアップの日時（年 4 回のバックアップは、1、4、7、10 月の指定日に実行されます） • 毎年バックアップの特定の日付または曜日、および時刻
年 2 回	• 年 2 回のバックアップの時刻、特定の日付または曜日、および月 • 毎年バックアップの特定の日付または曜日、および時刻
毎年	• 毎年バックアップの特定の日付または曜日、および時刻

関連項目

回復の目標の定義

長期保護に使用する回復の目標のカスタマイズ

保存期間とバックアップ頻度を指定する際に、DPM によってバックアップジョブのスケジュールが生成されます （詳細については、「長期保護用の復旧ポイントのスケジュール」を参照してください）。回復の目標に合わせて、バックアップジョブのスケジュールをカスタマイズして既定のスケジュールに代えて使うことも可能です。

保護グループのバックアップジョブのスケジュールをカスタマイズする際には、各バックアップ間隔に対して回復の目標を指定します。選択できるバックアップ頻度は、次のとおりです。

- 毎日
- 毎週
- 毎月
- 毎年

回復の目標として、バックアップ間隔は 3 種類まで指定できます。各バックアップ間隔について、テープの保存期間、作成するテープのコピー数、およびテープラベルを指定します。

保護グループの回復の目標をカスタマイズすることで、バックアップがたとえば次のスケジュールに従って実行されるように設定できます。

- 毎週バックアップの 1 コピーを 2 週間保存
- 毎月バックアップの 2 コピーを 6 か月保存
- 毎年バックアップの 1 コピーを 5 年間保存

関連項目

保護構成の計画

保護グループへのスペースの割り当て

保護グループを作成し、ディスクベースの保護を選択する際には、記憶域プールのスペースを、グループ内のメンバーシップ用に選択したレプリカと各データソース用の復旧ポイントに割り当てる必要があります。また、保護されるファイルサーバーまたはワークステーション上のスペースを変更ジャーナルに割り当てる必要があります。

DPM は、保護グループのメンバーに既定のスペースを割り当てます。DPM による既定の割り当ての計算方法を次の表に示します。

既定のスペース割り当ての計算方法

コンポーネント	既定の割り当て	場所
レプリカボリューム	ファイル： • （データソースのサイズ x 3）/ 2 Exchange のデータ： • データソースのサイズ x（1 + ログ変更）/（警告のしきい値 - .05） SQL Server データ： • データソースのサイズ x（1 + ログ変更）/（警告のしきい値 - .05） Windows SharePoint Services のデータ： • すべてのデータベースの合計サイズ /（警告のしきい値 - .05） 仮想サーバーのデータ： • データソースのサイズ x 1.5 システム状態： • （データソースのサイズ x 3）/ 2	DPM 記憶域プールまたはカスタムボリューム
復旧ポイントボリューム	ファイル： • （データソースのサイズ x 保存期間 [日数] x 2）/ 100 + 1600 MB Exchange のデータ： • 4.0 x 保存期間 [日数] x ログ変更 x データソースのサイズ + 1600 MB SQL Server データ： • 2.5 x 保存期間 [日数] x ログ変更 x データソースのサイズ + 1600 MB Windows SharePoint Services のデータ： • 1.5 x 保存期間 [日数] x ログ変更 x すべてのデータベースの合計サイズ + 1600 MB 仮想サーバーのデータ： • （データソースのサイズ x 保存期間 [日数] x 0.02） + 1600 MB システム状態： • （データソースのサイズ x 保存期間 [日数] x 2）/ 100 + 1600 MB	DPM 記憶域プールまたはカスタムボリューム

コンポーネント	既定の割り当て	場所
変更ジャーナル（ファイルの保護専用）	300 MB	ファイルサーバーまたはワークステーション上の保護されるボリューム

上記の表に使用されている値の定義は次のとおりです。

- **警告%**—レプリカの増大と関連付けられている警告のしきい値、通常 90%。
- **ログ変更**—当該データベースまたはストレージグループ上の変更率。これは大きく変動しますが、DPM の既定の推奨においては、Exchange および SQL Server データには 6%、Windows SharePoint Services データには 10% が想定されています。
- **保存期間（RR）**—保存される復旧ポイントの数です。DPM の既定の推奨においては 5 が想定されています。
- **システム状態のデータ ソースのサイズ**—データ ソースのサイズは 1 GB が想定されています。

保護グループを作成する際に、**ディスク割り当ての変更** ダイアログボックスで、各データ ソースの **データサイズ** 列に **計算** リンクが表示されます。ディスクの割り当てを初めて行う場合、DPM は既定の式を、データ ソースが置かれているボリュームのサイズに適用します。選択したデータ ソースの実際のサイズに式を適用するには、**計算** リンクをクリックします。DPM はデータ ソースのサイズを判断し、そのデータ ソースの復旧ポイントとレプリカのボリュームに対するディスクの割り当てを再計算します。この操作は数分かかることがあります。

既定値が適切でないことが確実な場合以外は、既定の割り当てを受け入れることをお勧めします。既定の割り当てを変更すると、スペースの割り当てが少なすぎたり多すぎたりする結果になる場合があります。

復旧ポイントに対するスペースの割り当てが少なすぎると、DPM が保存期間の目標を満たすのに十分な復旧ポイントを保存できなくなるおそれがあります。スペースの割り当てが多すぎると、ディスク容量の無駄遣いになります。

保護グループの作成後に、その保護グループ内のあるデータ ソースに割り当てたスペースが少なすぎることに気づいた場合は、各データ ソースのレプリカと復旧ポイントのボリュームに対する割り当てを増やすことができます。

保護グループに割り当てたスペースが多すぎることに気づいた場合、データ ソースに対する割り当てを減らす唯一の方法は、保護グループからデータ ソースを削除し、レプリカを削除し、割り当てを少なくしてデータ ソースを保護グループに戻すことです。

必要な記憶領域を予測するには、DPM storage calculator（記憶域電卓）をダウンロードしてご利用ください（http://go.microsoft.com/fwlink/?LinkId=104370）。

関連項目

保護構成の計画

テープとライブラリの詳細の指定

テープによる保護を選択した場合は、DPM が生成する各テープのコピー数と、バックアップテープの構成オプションを指定する必要があります。次のオプションのいずれかを選択します。

- **データの圧縮**

  このオプションを選択すると、データがテープに書き込まれる際に DPM がデータを圧縮します。そのため、テープのスペースが少なくて済み、同じテープに保存できるバックアップジョブの数が増えます。圧縮によって、バックアップジョブの完了に必要な時間が大幅に延びることはありません。圧縮率は、データの種類によって異なります。

- **データの暗号化**

  このオプションを選択すると、データがテープに書き込まれる際に DPM がデータを暗号化します。そのため、アーカイブされたデータのセキュリティが強化されます。暗号化によって、バックアップジョブの完了に必要な時間が大幅に延びることはありません。

  メモ

  暗号化を有効にするには、DPM サーバー上に有効な暗号化証明書が必要です。手順については、DPM ヘルプの「保護グループ内のデータを暗号化する方法」を参照してください。

関連項目

保護構成の計画

レプリカの作成方法の選択

保護グループを作成する際には、グループに含まれるボリュームのレプリカを作成する方法を選択する必要があります。レプリカの作成には、保護の対象として選択したすべてのデータを DPM サーバーにコピーし、各レプリカに対して整合性チェックと共に同期を実行するという手順があります。

DPM はネットワークを介してレプリカを自動的に作成することができます。または、テープなどのリムーバブルメディアからデータを復元して、レプリカを手動で作成することもできます。レプリカは自動作成の方が簡単ですが、保護されるデータのサイズとネットワークの速度によっては、手動で作成した方が早い場合もあります。

レプリカの作成方法の選択を助けるために、保護されるデータのサイズとネットワークの速度の違いに応じて、ネットワーク経由のレプリカの自動作成にかかる推定時間を下記の表に示します。ここでは、ネットワークが最大速度で実行されていて、帯域幅を巡って競合するその他の処理がないことが前提とされています。時間の単位は時間（hours）です。

各ネットワーク速度でのレプリカの自動作成の所要時間

保護されるデータのサイズ	512 Kbps	2 Mbps	8 Mbps	32 Mbps	100 Mbps
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

重要

WAN 経由でデータを保護するために DPM を導入する予定で、保護グループに 5 GB 以上のデータが含まれる場合は、レプリカを手動で作成することをお勧めします。

レプリカの自動作成

大きなレプリカを作成するジョブでは、ネットワークトラフィックが少ないときにのみジョブが実行されるようにスケジュールできます。

レプリカの手動作成

レプリカの手動作成を選択すると、DPM は DPM サーバー上の正確な位置を指定します。そこにレプリカを作成してください。通常は、テープなどのリムーバブルメディアからデータソースの最新のバックアップを復元することによってレプリカを作成します。データを復元した後で各レプリカに対して整合性チェックと共に同期を実行することで、手順が完了します。

DPM サーバーにデータを復元してレプリカを作成する際に、タイムスタンプやセキュリティなど、データソースの元のディレクトリ構造とプロパティを保持することが重要です。レプリカと保護されるデータソースの間の相違が大きいほど、整合性チェックに時間がかかります。元のディレクトリ構造とプロパティを保持しておかないと、レプリカの手動作成は自動作成と同じくらい時間がかかる場合があります。

関連項目

保護構成の計画

DPM の導入計画

Microsoft System Center Data Protection Manager (DPM) 2007 の導入計画を立てる際に、保護グループの計画を最初に立ててください。サイズ、データ変更率、場所、回復の目標といった保護グループのニーズが、DPM サーバーとテープライブラリの作成と配置を決定する要因になるからです。

保護グループの計画を立てた後で、データを最も効率的に保護するのに必要な DPM サーバーの構成を決定すれば、導入計画は完了です。本項のトピックには、導入計画を左右する可能性のあるセキュリティと管理の注意事項が含まれています。

本項の内容

関連項目

保護グループの計画

DPM サーバー構成の計画

導入計画には、データの保護に必要な DPM サーバーの数と、ネットワーク上のどの場所に各 DPM サーバーを置くかを指定する必要があります。

導入計画には、各 DPM サーバーが Microsoft SQL Server のどのインスタンスを使用するかについても指定する必要があります。DPM は、DPM とレポートデータベースのために SQL サーバーのインスタンスを必要とします。DPM サーバーのインストール中に DPM は SQL サーバーをインストールします。または、リモートコンピュータ上の SQL サーバーの既存のインスタンスを使用することも可能です。

DPM サーバー構成の必須コンポーネントの 1 つが、記憶域プールです。これは、保護されるデータのレプリカと復旧ポイントを保存するディスクセットです。何らかのデータソースに対してテープベースの保護を必要とする導入計画の場合は、テープライブラリまたはスタンドアロンのテープドライブを DPM サーバーに取り付ける必要があります。

大きな Windows SharePoint Services ファームを保護する場合は、DPM データベース用に十分なディスク容量を持つボリュームに DPM をインストールする必要があります。

大きな Windows SharePoint Services ファームを保護する場合は、DPM データベース用に十分なディスク容量を持つボリュームに DPM をインストールする必要があります。DPM データベースは、ファーム内に存在する無数の個々のアイテムに対して約 1 GB を必要とします。たとえば、500 万のアイテムがあるファームを保護する場合は、そのようなファームのカタログを持つ DPM データベース内に約 5 GB の記憶域を計画するでしょう。この必要領域は、テープバックアップカタログ、ジョブのログ、その他に DPM が必要とする記憶域に加えて必要な領域です。

本項の内容

関連項目

エンドユーザー回復の注意事項

セキュリティの注意事項

DPM サーバーの台数の選択

御社で必要とする DPM サーバーの台数を検討する際には、DPM サーバーの台数を決定するための明確な式がないことに留意してください。実際には、サーバーの台数と 1 台の DPM サーバーで保護できるデータの量は、以下の要因によって左右されます。

- 保護されるデータソースの変更率
- 記憶域プール内で使用できる容量
- データが同期される頻度
- 保護される各コンピュータで使用可能な帯域幅
- DPM サーバー上の総帯域幅

データの変更率を推定するには、最近の平均的な日の増分バックアップを参照します。増分バックアップに含まれているデータのパーセンテージは、通常、データの変更率を示すものです。たとえば、データの総量が 100 GB で、増分バックアップに 10 GB が含まれている場合、1 日あたりのデータの変更率は約 10 パーセントである可能性が高いと言えます。

ただし、DPM がデータの変更を記録するのに使用する方法は、ほとんどのバックアップソフトウェアの方法と異なるため、増分バックアップのサイズは、データの変更率を必ずしも常に正確に示すとは限りません。データ変更率の予測精度を高めるには、保護するデータの特性を考慮してください。

たとえば、ほとんどのバックアップソフトウェアがファイルレベルでデータの変更を記録するのに対して、DPM はバイトレベルで変更を記録します。この点を考慮すると、保護するデータの種類によっては、データの変更率は増分バックアップによって示されているものよりも低い数字になります。

最小ハードウェア要件を満たす DPM サーバーによって保護できるデータソースの限度と DPM サーバー 1 台あたりに必要とされる推奨ディスク容量を次の表に示します。

プラットフォーム	データソースの限度	推奨ディスク容量
32 ビットコンピュータ	150 データソース。 約 30 ～ 40 台のサーバーが 1 台の DPM サーバーに直接接続された構成をお勧めします。	10 TB **メモ** x86 32 ビットのオペレーティングシステムには、ボリュームシャドウコピーサービス（VSS）非ページプールの制限があります。セカンダリ DPM サーバーを使用してデータを保護する場合、推奨ディスク容量は 6 TB です。
64 ビットコンピュータ	300 データソース データソースは通常、 50 ～ 75 台の物理サーバーに分散されます。	40 TB

スナップショットの制限

DPM サーバーは、データソースの保護を停止した時に保持されるものも含め、ディスクベースのスナップショットを最大 9,000 まで保存できます。スナップショットの制限は、高速完全バックアップとファイルの復旧ポイントに適用されますが、増分同期には適用されません。

スナップショットの制限は、記憶域プールのサイズに関係なく、DPM サーバーごとに適用されます。保護グループを設定する際に、DPM サーバーは、保護グループの設定を収めるスナップショットの数に対して提供されます。DPM 管理シェルで次の cmdlet を使用すると、サーバーが提供されるスナップショットの数を確認できます。

$server=Connect-DPMServer –DPMServerName 名前
$server.CurrentShadowCopyProvision

DPM の導入を計画する際には、DPM サーバーの容量の一部としてスナップショットの制限を考慮する必要があります。次の表は、さまざまな保護ポリシーから導き出されるスナップショットの数の例を示したものです。

保護ポリシー	スナップショット
Exchange ストレージグループ：毎日の高速完全バックアップ、15 分間隔の増分同期、保存期間 5 日	5
ファイルサーバー上のボリューム：毎日の復旧ポイント 3 つ、保存期間 21 日	63
SQL データベース：毎日の高速完全バックアップ 2 つ、保存期間 14 日	28
合計：	**96**

関連項目

DPM サーバー構成の計画

DPM サーバーの位置の確認

DPM は、保護と回復の操作をサポートするために、Windows Server 2003 Active Directory ドメインサービスのディレクトリサービス構造を必要とします。

DPM は、DPM サーバーと同じドメインにあるか、または DPM サーバーがあるドメインとの間に双方向の信頼関係を持つドメインにあるサーバーとワークステーションを保護できます。

DPM サーバーを置く場所を決定する際には、DPM サーバーと保護されるコンピュータの間のネットワーク帯域幅を考慮してください。

DPM は、チーム化された NIC をサポートしています。チーム化された NIC とは、オペレーティングシステムによって単一の NIC として扱われるように設定された複数の物理 NIC のことです。チーム化された NIC は、各 NIC を使用して使用可能な帯域幅を結合することで帯域幅を増やし、NIC が失敗したときには、残りの NIC にフェールオーバーします。DPM は、DPM サーバー上のチーム化された NIC を使用して増えた帯域幅を使用することができます。

DPM サーバーの位置を決定するためのもう 1 つの検討事項は、ライブラリに新しいテープを追加したり、オフサイトでの保管のためにテープを取り出すなど、テープとテープライブラリを手動で管理する必要性です。

関連項目

DPM サーバー構成の計画

SQL サーバーのインスタンスの選択

DPM のインストールには通常、DPM セットアップによってインストールされる SQL サーバーのインスタンスが含まれます。DPM セットアップによってインストールされる SQL サーバーのインスタンスは、DPM ソフトウェアに含まれており、SQL サーバーの別のライセンスを必要としません。

ただし、DPM 2007 をインストールする際には、DPM に含まれている SQL サーバーの既定のインスタンスの代わりに、DPM が使用する SQL サーバーのリモートインスタンスを指定できます。

SQL サーバーのリモートインスタンスを使用するには、SQL サーバーを実行しているサーバーと DPM サーバーが同じドメインに置かれている必要があります。SQL サーバーの特定のインスタンスは、1 台の DPM サーバーのみによって使用できます。SQL サーバーのリモートインスタンスを、ドメインコントローラとして実行されているコンピュータ上に置くことはできません。

メモ

SQL サーバーのリモートインスタンスがドメインアカウントとして実行されている場合は、DPM サーバーとの通信のために名前付きパイププロトコルを有効にしてください。名前付きパイププロトコルの設定手順については、「Configuring Client Network Protocols」（クライアントネットワークプロトコルの設定）（http://go.microsoft.com/fwlink/?LinkId=87976）を参照してください。

SQL サーバーのリモートインスタンスには、次のコンポーネントも含めて、インターネットインフォメーションサービス（IIS）と SQL Server 2005 Standard/Enterprise Edition With SP2 が実行されている必要があります。

- SQL サーバーデータベースエンジン
- レポートサービス

SQL サーバーのリモートインスタンスには、次の設定を使用することをお勧めします。

- 失敗の監査の既定の設定を使用する。
- 既定の Windows 認証モードを使用する。
- sa アカウントに強力なパスワードを設定する。
- パスワードポリシーのチェックを有効にする。
- SQL サーバーデータベースエンジンとレポートサービスのコンポーネントのみをインストールする。
- SQL サーバーのリモートインスタンスは、ローカルシステムとして実行しない。
- 特権の低いドメインユーザーアカウントを使用して SQL サーバーを実行する。

関連項目

DPM サーバー構成の計画

記憶域プールの計画

記憶域プールとは、DPM サーバーが保護されるデータのレプリカや復旧ポイントを保存するディスクセットのことです。記憶域プールの計画には、必要容量の計算とディスク構成の計画が含まれます。

記憶域プール内のボリュームの代わりに、ディスクの管理で定義するカスタムボリュームを使用することもできます。

DPM では、記憶域プールに次のどれでも使用できます。

- 直接接続記憶域（DAS）
- ファイバチャネル記憶域ネットワーク（SAN）
- iSCSI 記憶装置または SAN

記憶域プールは、IDE、SATA、SCSI をはじめ、ほとんどのディスクの種類をサポートしており、マスタブートレコード（MBR）と GUID パーティションテーブル（GPT）の両方のパーティションスタイルをサポートしています。

記憶域プールに SAN を使用する場合は、DPM 上で使用するディスクとテープ用に別個のゾーンを作成することをお勧めします。1 つのゾーンにデバイスを混在させないでください。

USB/1394 ディスクを DPM 記憶域プールに追加することはできません。

容量が 1.5 TB 以下のディスクを使用することをお勧めします。ダイナミックボリュームは 32 台までのディスクをスパンできるので、1.5 TB のディスクを使用すると、DPM は最大 48 TB のレプリカボリュームを作成できます。

重要

一部の OEM では、独自に提供するメディアを使用してインストールする診断パーティションをディスクに含めています。診断パーティションは、OEM パーティション、または EISA パーティションとも呼ばれます。EISA パーティションは、ディスクを DPM 記憶域プールに追加する前にディスクから削除しておく必要があります。

本項の内容

関連項目

DPM サーバー構成の計画

必要容量の計算

DPM 記憶域プールの必要容量は、主に保護されるデータのサイズ、毎日の復旧ポイントのサイズ、ボリュームデータの予想増加率、および保存期間の目標に応じて変動します。

毎日の復旧ポイントのサイズとは、1 日の間に保護データに対して行われる変更の合計サイズを意味します。これは、増分バックアップのサイズとほぼ同等です。保存期間とは、ディスク上の保護データの復旧ポイントを保存しておく日数を意味します。ファイルに関しては、DPM は保護グループに含まれている各ボリュームについて最大 64 の復旧ポイントを保存できます。また、毎日各保護グループについて、復旧ポイントのスケジュールを最大 8 つまで作成できます。

メモ

ファイルに関して復旧ポイントが 64 までに制限されているのは、ボリュームシャドウ コピーサービス（VSS）の制限によるもので、この制限は、DPM のエンドユーザー回復の機能にとって必要なものです。復旧ポイントの制限は、アプリケーションデータには適用されません。

一般に、記憶域プールのサイズを、ファイル保護のために保護されるデータの 2 倍のサイズにすることをお勧めします。これは、毎日の復旧ポイントのサイズを保護されるデータのサイズの約 10 パーセントとし、保存期間を 10 日間（週末を除いて 2 週間）とする仮定に基づく推奨です。

毎日の復旧ポイントのサイズが保護されるデータのサイズの 10 パーセントよりも大きいか小さい場合、または、保存期間の目標が 10 日よりも長いか短い場合は、記憶域プールの必要容量をそれに応じて調整してください。

初期導入の時点で記憶域プールに割り当てる容量の多少に関係なく、後で必要が生じた場合に容量を追加できるように、拡張可能なハードウェアを使用することをお勧めします。

以下の項では、毎日の復旧ポイントのサイズと保存期間の目標を決定するためのガイドラインを示します。

毎日の復旧ポイントのサイズを予測する方法

記憶域プールを保護されるデータの 2 倍のサイズにするという推奨は、毎日の復旧ポイントのサイズが保護されるデータの 10 パーセントのサイズであることを前提としています。毎日の復旧ポイントのサイズは、データの変更率と関連しており、1 日の間に作成されるすべての復旧ポイントの合計サイズを指します。保護されるデータの毎日の復旧ポイントのサイズを推定するには、最近の平均的な日の増分バックアップを参照します。増分バックアップのサイズは通常、毎日の復旧ポイントのサイズを示すものです。たとえば、100 GB のデータの増分バックアップに 10 GB のデータが含まれている場合、毎日の復旧ポイントのサイズはおそらく、約 10 GB です。

保存期間の目標の決定

記憶域プールを保護されるデータの 2 倍のサイズにするという推奨は、保存期間の目標が 10 日間（週末を除いて 2 週間）であることを前提としています。一般的な企業では、データ回復の要求は、データが失われたイベントから 2 ～ 4 週間以内に集中しています。10 日間という保存期間は、データが失われるイベントから最長 2 週間のデータ回復を可能にします。

保存期間の目標が長いほど、1 日に作成できる復元ポイントは少なくなります。たとえば、保存期間の目標が 64 日間だとすると、1 日に作成できる復旧ポイントは 1 つだけになります。保存期間の目標が 8 日間なら、1 日に作成できる復旧ポイントは 8 つになります。保存期間の目標が 10 日間なら、1 日に作成できる復旧ポイントは約 6 つになります。

関連項目

カスタムボリュームの定義

ディスク構成の計画

DPM サーバー構成の計画

ディスク構成の計画

DPM 記憶域プールに直接接続の記憶域を使用する場合は、ハードウェアベースのどんな RAID 構成でも使用できます。または、JBOD（just a bunch of disks: ただのディスク束）構成を使用することも可能です。記憶域プールに追加するディスク上にソフトウェアベースの RAID 構成を作成しないでください。

ディスクの構成を決めるには、お使いの環境における容量、コスト、信頼性、およびパフォーマンスの相対的な重要性を検討してください。たとえば、JBOD はパリティデータを保存するためにディスク容量を使用しないので、JBOD 構成では記憶容量を最大限に活用できます。同じ理由で、JBOD 構成の信頼性は良くありません。1 台のディスクに障害が発生しただけで、データの損失が避けられないのです。

DPM の典型的な導入例では、RAID 5 の構成にすると、容量、コスト、信頼性、およびパフォーマンスのバランスが良くなります。ただし、DPM サーバーの負荷は主に書き込み操作によるため、RAID 5 は、ファイルサーバーの場合よりも目に見えて DPM サーバーのパフォーマンスを低下させる可能性が高くなります。こうしたパフォーマンスの低下は、ひいては DPM のスケーラビリティに影響を与える可能性があります。パフォーマンスが低下すると、データを効果的に保護する DPM の能力も低下するのです。

下記の表は、記憶域プール内のディスクを構成する際の各オプションの評価を助けるために、JBOD とさまざまな RAID のレベルの間の長所と短所を 4（秀）～ 1（可）の 4 段階で比較したものです。

記憶域プールのディスクに使う構成オプションの比較

ディスク構成	容量	コスト	信頼性	パフォーマンスとスケーラビリティ
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

RAID の詳細については、「Achieving Fault Tolerance by Using RAID」（RAID によるフォールトトレランスの実現）（http://go.microsoft.com/fwlink/?LinkId=46086）を参照してください。

関連項目

必要容量の計算

カスタムボリュームの定義

DPM サーバー構成の計画

カスタムボリュームの定義

DPM 2007 では、DPM 記憶域プールの代わりにカスタムボリュームを保護グループのメンバーに割り当てることができます。カスタムボリュームとは、DPM 記憶域プール内にはなく、保護グループのメンバーのためにレプリカと復旧ポイントを保存するように指定されたボリュームのことです。

DPM によって管理される記憶域プールはほとんどのビジネスのニーズにとって十分ですが、特定のデータ ソースの記憶域に対する制御の強化が必要になる可能性もあります。たとえば、記憶域ネットワーク上の高パフォーマンス論理ユニット番号（LUN）を使用して保存したい重要なデータがあるとします。

DPM サーバーに接続されているどのボリュームでも（ただし、システムファイルとプログラムファイルが入っているボリュームを除く）、新しい保護グループの作成ウィザードで、カスタムボリュームとして選択できます。保護グループのメンバーとしてカスタムボリュームを使用するには、2 つのカスタムボリュームが使用可能でなければなりません。1 つはレプリカの保存用、もう 1 つは復旧ポイントの保存用です。

DPM は、カスタムボリューム内の領域を管理できません。カスタムレプリカボリュームまたは復旧ポイントボリュームの空き領域が少なくなっているというアラートが表示されたら、ディスクの管理を使用してカスタムボリュームのサイズを手動で変更する必要があります。

グループの作成後に、保護グループのメンバーに対する記憶域プールまたはカスタムボリュームの選択を変更することはできません。データソースのレプリカまたは復旧ポイントの保存場所を変更する必要がある場合は、データソースをいったん保護から削除し、新しい保護グループのメンバーとして保護グループに追加する以外に方法はありません。

関連項目

必要容量の計算

ディスク構成の計画

DPM サーバー構成の計画

テープライブラリの構成の計画

テープライブラリとスタンドアロンのテープドライブを DPM に追加して、テープベースの短期および長期のデータ保護を有効にすることができます。テープライブラリとスタンドアロンのテープドライブは、DPM サーバーに物理的に接続されている必要があります。

メモ

テープライブラリという語は、マルチドライブのテープハードウェアとスタンドアロンのテープドライブの両方を指します。

テープライブラリの容量を計画する際には、テープバックアップジョブの数と保護されるデータのサイズを考慮します。ハードウェアの機能も考慮する必要があります。たとえば、自動ローダーがないテープライブラリは、ジョブの実行中にテープのローテーションを手動で行う必要があります。

各保護グループに必要となるテープの個数を計画するには、バックアップ頻度に保存期間を乗じます。

長期保護に使用するテープのテープラベルは、保護グループの作成時に割り当てられます。DPM は、次の形式で既定のテープラベルを割り当てます：**DPM - <保護グループ名> - long-term tape <番号>**。既定のスキームを使用しない場合は、保護グループの作成を開始する前にテープの名前付けスキームを計画する必要があります。

詳細については、「Managing Tape Libraries」（テープライブラリの管理）（http://go.microsoft.com/fwlink/?LinkId=91964）を参照してください。

関連項目

DPM サーバー構成の計画

エンドユーザー回復の注意事項

導入計画には、エンドユーザー回復を有効とするデータと、エンドユーザー回復を提供するために Active Directory ドメインサービスで設定する必要のある DPM サーバーが指定されている必要があります。

エンドユーザー回復を使用すれば、エンドユーザーは、ファイルの旧バージョンを回復することでデータを個別に回復できます。エンドユーザーは、ファイルサーバー上の共有、もしくは DFS 名前空間を通じて、または Microsoft Office 2003 アプリケーションの **ツール** メニューにあるコマンドを使用して、旧バージョンを回復できます。

DPM で保護するコンピュータ上で、共有フォルダのシャドウコピーが現在有効に設定されている場合は、その機能を無効にすれば、使用されていたディスク容量を回復できます。エンドユーザーと管理者は、DPM サーバー上の復旧ポイントからファイルを回復できるようになります。

エンドユーザー回復を有効にするには、Active Directory ドメインサービスのスキーマを設定し、DPM サーバー上のエンドユーザー回復機能を有効にし、クライアントコンピュータに復旧ポイントクライアントソフトウェアをインストールする必要があります。

Active Directory ドメインサービスの設定

エンドユーザー回復をサポートするように Active Directory ドメインサービスを設定する手順は、次の 4 つです。

1. スキーマの拡張
2. コンテナの作成
3. コンテナの内容を変更する DPM サーバー権限を付与
4. ソース共有とレプリカ上の共有の間にマッピングを追加

スキーマは 1 回のみ拡張されます。ただし、各 DPM サーバーについて Active Directory のスキーマ拡張を設定する必要があります。ドメイン内の追加の DPM サーバーについてエンドユーザー回復を有効にすると、追加の各サーバーについて手順 3 と 4 が実行されます。必要に応じて、毎回の同期後に DPM は共有マッピングを更新します（手順 4）。

Active Directory ドメインサービスドメイン内のスキーマとドメインの両方の管理者である DPM 管理者は、DPM 管理者コンソール内で、1 回のクリック操作だけでこれらの手順を完了することができます。スキーマとドメインの管理者ではない DPM 管理者は、スキーマとドメインの管理者に DPMADSchemaExtension ツールを実行するように指示することで、これらの手順を完了することができます。

DPMADSchemaExtension ツールは、DPM サーバーの Microsoft Data Protection Manager\2006\End User Recovery というフォルダに保存されています。スキーマとドメインの両方の管理者であるユーザーは、DPM サーバーが展開されているドメインのメンバーで、Windows Server 2003 を実行しているどのコンピュータ上でも、このツールを実行できます。管理者は、このツールを実行する際に、DPM サーバーの名前を指定する必要があります。

DPMADSchemaExtension ツールを使用してエンドユーザー回復を有効にする場合は、ツールを各 DPM サーバーについて 1 回実行する必要があります。

シャドウコピークライアントソフトウェアのインストール

エンドユーザーは、各自のファイルの旧バージョンを個別に回復する前に、DPM 復旧ポイントクライアントソフトウェアを自らのコンピュータにインストールする必要があります。共有フォルダのシャドウコピーのクライアントがコンピュータ上に存在する場合は、DPM をサポートするようにクライアントソフトウェアを更新する必要があります。

復旧ポイントクライアントソフトウェアは、Service Pack 2 (SP2) 以降が適用された Windows XP、および Windows Server 2003（SP1 が適用されているか否かは問わない）が実行されているコンピュータにインストールできます。

関連項目

DPM サーバー構成の計画

セキュリティの注意事項

セキュリティの注意事項

DPM は、ネットワーク上で高い権限を持つサーバーとして動作します。DPM サーバーのセキュリティを確実にするために、DPM セキュリティアーキテクチャは、 Windows Server 2003 と Active Directory ドメインサービス、SQL Server 2005、および SQL Server レポートサービスのセキュリティ機能を利用します。

DPM セキュリティアーキテクチャを維持するには、次のことを守ってください。

- 既定のセキュリティ設定をすべて受け入れる。
- DPM サーバーに不要なソフトウェアをインストールしない。
- DPM の導入後は、セキュリティ設定を変更しない。特に、SQL Server 2005 の設定、インターネットインフォメーションサービス（IIS）の設定、DCOM の設定、または、製品のインストール中に DPM によって作成されるローカルユーザーとグループ用の設定を変更しないでください。
- SQL サーバーのリモートインスタンスは、ローカルシステムとして実行しない。

不要なソフトウェアをインストールしたり、既定のセキュリティ設定を変更したりすると、DPM のセキュリティに深刻な問題が生じるおそれがあります。

本項の内容

アンチウイルスソフトウェアの設定

ファイアウォールの設定

エンドユーザー回復のセキュリティに関する注意事項

適切なユーザー権限の付与

関連項目

エンドユーザー回復の注意事項

DPM サーバー構成の計画

アンチウイルスソフトウェアの設定

DPM は、よく使われるアンチウイルスソフトウェア製品のほとんどに対応しています。ただし、アンチウイルス製品は DPM のパフォーマンスに影響を与える場合があり、正しく設定されていないと、レプリカや復旧ポイントのデータ破損を招くことがあります。本項では、そうした問題を軽減する方法について説明します。

ウイルスのリアルタイム監視の設定

DPM サーバーのパフォーマンスの低下を最小限に抑えるには、保護されるすべてのデータ ソースに対してレプリカのアンチウイルスリアルタイム監視を無効にしてください。それには、Microsoft Data Protection Manager\DPM\bin というフォルダにある DPM プロセスのリアルタイム監視（msDPMprotectionagent.exe）を無効にします。レプリカのリアルタイム監視が有効に設定されているとパフォーマンスが低下するのは、DPM がレプリカに変更を適用するたびに毎回、関連するファイルのすべてがアンチウイルスソフトウェアによってスキャンされるためです。

また、DPM 管理者コンソールの使用中にパフォーマンスが低下する場合は、csc.exe プロセスのリアルタイム監視を無効にしてください。これは Windows\Microsoft.net\Framework\v2.0.50727 というフォルダにあります。csc.exe プロセスは C# コンパイラです。csc.exe プロセスのリアルタイム監視によってパフォーマンスが低下するのは、csc.exe プロセスで XML メッセージの生成時に出るファイルをアンチウイルスソフトウェアがスキャンするためです。

個別のプロセスに対してリアルタイム監視を設定する手順については、アンチウイルス製品のマニュアルを参照してください。

ウイルスに感染したファイルに対するオプションの設定

レプリカと復旧ポイントのデータ破損を防ぐために、DPM サーバー上のアンチウイルスソフトウェアを、自動クリーンアップや検疫ではなく、感染したファイルを削除する設定にしてください。自動クリーンアップや検疫が実行されるとデータが破損するおそれがあります。これらの処理によってアンチウイルスソフトウェアがファイルを修正した結果、DPM が検出できない変更が施されるためです。別のプログラムによって修正されたレプリカに対して DPM が同期を試みると、レプリカと復旧ポイントのデータが破損するおそれがあります。感染したファイルを削除するようにアンチウイルスソフトウェアを設定すれば、この問題を避けることができます。ただし、アンチウイルスソフトウェアによってレプリカからファイルが削除されるたびに毎回、整合性チェックと共に同期を手動で実行する必要があります。ウイルスに感染したファイルを削除するようにアンチウイルスソフトウェアを設定する手順については、製品のマニュアルを参照してください。

関連項目

セキュリティの注意事項

ファイアウォールの設定

保護するコンピュータがファイアウォールの内側にある場合は、DPM サーバー、それによって保護されるコンピュータ、およびドメインコントローラの間の通信が許可されるようにファイアウォールを設定する必要があります。

プロトコルとポート

ネットワーク構成によっては、DPM、保護されるサーバー、およびドメインコントローラの間で通信ができるようにようにファイアウォールを設定する必要があります。DPM によって使用されるプロトコルとポートの詳細を下記の表に示します。ファイアウォールを設定する際に参考にしてください。

DPM によって使用されるプロトコルとポート

プロトコル	ポート	詳細
DCOM	135/TCP ダイナミック	DPM 制御プロトコルでは、DCOM が使用されます。DPM は、DCOM 呼び出しを行うことで保護エージェントにコマンドを発行します。保護エージェントは、DPM サーバーに対してDCOM 呼び出しを行うことで応答します。 TCP ポート 135 は、DCOM で使用される DCE エンドポイント解決ポイントです。 既定では、DCOM は TCP ポート範囲 1024 ～ 65535 から動的にポートを割り当てます。ただし、この範囲はコンポーネントサービスを使用して構成できます。詳細については、「Using Distributed COM with Firewalls（ファイアウォールでの分散 COM の使用）（http://go.microsoft.com/fwlink/?LinkId=46088）を参照してください。
TCP	5718/TCP 5719/TCP	DPM のデータチャネルは TCP に基づいています。DPM と保護されるコンピュータの両方で、同期や回復など、DPM 操作を有効にするための接続が開始されます。 DPM は、ポート 5718 でエージェントコーディネータと通信し、ポート 5719 で保護エージェントと通信します。
DNS	53/UDP	DPM とドメインコントローラの間、および保護されるコンピュータとドメインコントローラの間で、ホスト名解決に使用されます。
Kerberos	88/UDP 88/TCP	DPM とドメインコントローラの間、および保護されるコンピュータとドメインコントローラの間で、接続エンドポイントの認証に使用されます。
LDAP	389/TCP 389/UDP	DPM とドメインコントローラの間で、照会に使用されます。
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	DPM と保護されるコンピュータの間、DPM とドメインコントローラの間、および保護されるコンピュータとドメインコントローラの間で、その他の操作に使用されます。TCP/IP で直接ホストされている SMB で、DPM 機能に使用されます。

Windows ファイアウォール

Windows ファイアウォールは Windows Server 2003 SP1 に含まれています。DPM をインストールする前に Windows Firewall on the DPM サーバーを有効にすると、DPM セットアップがファイアウォールを DPM 用に正しく設定します。DPM のインストール後に Windows Firewall on the DPM サーバーを有効にした場合は、DPM サーバーと保護されるコンピュータの間の通信を許可するために、ファイアウォールを手動で設定する必要があります。ポート 135 を TCP トラフィックに対して開き、DPM サービス（Microsoft Data Protection Manager/DPM/bin/MsDPM.exe）と保護エージェント（Microsoft Data Protection Manager/DPM/bin/Dpmra.exe）を Windows ファイアウォールポリシーに対する例外として指定することで、DPM サーバー上の Windows ファイアウォールを設定します。

Windows ファイアウォールの設定手順については、Windows Server 2003 の Windows のヘルプとサポートで「Windows ファイアウォール」を検索してください。

関連項目

セキュリティの注意事項

エンドユーザー回復のセキュリティに関する注意事項

ファイルデータについてはエンドユーザー回復を有効にできますが、アプリケーションデータについてはできません。エンドユーザー回復を有効にする予定のファイルとフォルダに対する権限には、ドメインベースのセキュリティグループのみを使用してください。ローカルセキュリティグループを使用すると、DPM は、保護されるコンピュータ上のデータに対するエンドユーザーのアクセスと、DPM サーバー上のそのデータの復旧ポイントに対するエンドユーザーのアクセスの間の整合性を保証することができません。

たとえば、保護されるコンピュータのローカルユーザーグループに含まれているユーザーの組が、DPM サーバーのローカルユーザーグループに含まれているユーザーの組と異なる場合は、複数の異なるユーザーの組が、保護されるコンピュータ上のデータとそのデータの復旧ポイントにアクセスできるようになります。

関連項目

セキュリティの注意事項

適切なユーザー権限の付与

DPM の導入を開始する前に、さまざまな操作を行うために必要な権限が適切なユーザーに付与されていることを確認してください。DPM と関連のある主要な操作を行うために必要なユーザー権限を次の表に示します。

DPM の操作に必要なユーザー権限

操作	必要な権限
DPM サーバーを Active Directory ドメインに追加する	ドメインにワークステーションを追加するためのドメイン管理者アカウントまたはユーザー権限
DPM のインストール	DPM サーバーの管理者アカウント
コンピュータへの DPM 保護エージェントのインストール	コンピュータ上のローカル Administrators グループのメンバーであるドメインアカウント
DPM 管理者コンソールを開く	DPM サーバーの管理者アカウント
エンドユーザー回復を有効にするための Active Directory ドメインサービススキーマの拡張	ドメイン内のスキーマ管理者権限
エンドユーザー回復を有効にするための Active Directory ドメインサービスコンテナの作成	ドメイン内のドメイン管理者権限
コンテナの内容を変更する DPM サーバー権限の付与	ドメイン内のドメイン管理者権限
DPM サーバー上のエンドユーザー回復機能の有効化	DPM サーバーの管理者アカウント
クライアントコンピュータに復旧ポイントクライアントソフトウェアをインストール	クライアントコンピュータの管理者アカウント
保護されるデータの旧バージョンにクライアントコンピュータからアクセス	保護される共有にアクセスできるユーザーアカウント
Windows SharePoint Services のデータの回復	保護エージェントがインストールされているフロントエンド Web サーバーの管理者アカウントでもある、Windows SharePoint Services ファームの管理者アカウント

関連項目

セキュリティの注意事項

導入計画のチェックリストとロードマップ

このチェックリストには、Data Protection Manager (DPM) 2007 の導入の準備に必要な計画のタスクが記載されています。

操作	参照先
次の情報を含め、保護する各データソースを識別する。 • データソースの種類（ファイル、Microsoft Exchange、Microsoft SQL Server、Microsoft Windows SharePoint Services、Microsoft Virtual Server、システム状態） • データソースのサイズ • 保護から除外するフォルダまたはファイル名拡張子 • コンピュータの完全修飾ドメインネーム（FQDN） • クラスタ名（該当する場合）	何を保護するか?
各保護グループについて、次の方法から 1 つを識別する。 • ディスクベースの短期保護 • テープベースの短期保護 • テープベースの長期保護 • ディスクベースの短期保護とテープベースの長期保護 • テープベースの短期保護とテープベースの長期保護	データ保護方法の選択
各データソースについて、使用する各データ保護方法に関する回復の目標を定める。 ディスクベースの短期保護については、次の情報を確認する。 • 保存期間 • 同期の頻度 • 復旧ポイントの数 テープベースの短期保護については、次の情報を確認する。 • 保存期間 • バックアップのスケジュール • バックアップの種類 • バックアップコピーの数 • テープラベルのスキーム テープベースの長期保護については、次の情報を確認する。 • 保存期間 • バックアップのスケジュールとスケジュールのオプション • バックアップコピーの数 • テープラベルのスキーム	回復の目標 回復の目標の定義

操作	参照先
データ ソースを保護グループに分類する。	保護グループメンバーの選択
保護されるデータ ソースと回復の目標に関する情報に基づいて、記憶域の必要を判断する。	保護グループへのスペースの割り当て
テープベースの保護を使う場合は、テープに保存するデータを圧縮または暗号化するかどうかを決める。	テープとライブラリの詳細の指定
各保護グループについて、レプリカ作成のどの方法を使用するかを決める。	レプリカの作成方法の選択
次の情報を含め、必要な DPM サーバー構成を判断する。 • DPM サーバーの台数 • 各 DPM サーバーの設置場所 • 各 DPM サーバーが SQL サーバーのどのインスタンスを使用するか	DPM サーバー構成の計画
保護グループの記憶域の必要を満たすために各 DPM サーバーに必要なディスク構成を判断する。特定のデータ ソースが使用するカスタム ボリュームをすべて含める。	記憶域プールの計画
テープ ライブラリを必要とする DPM サーバーと各ライブラリの容量を確認する。	テープ ライブラリの構成の計画
エンドユーザー回復が有効とされる DPM サーバーを確認する。また、どのクライアントが復旧ポイント クライアント ソフトウェアのインストールを必要とするかを確認する。	エンドユーザー回復の注意事項

関連項目

Data Protection Manager 2007 の導入

DPM の導入計画

保護グループの計画