Windows Server System

Planificación de la implantación de System Center Data Protection Manager 2007

Microsoft Corporation

Publicación: septiembre de 2007

Resumen

En este documento se explica el funcionamiento de DPM y se proporcionan instrucciones para planificar la implantación de DPM.

Contenido

Planificación de la implantación de DPM 2007

En este documento se explica el funcionamiento de DPM y se proporcionan instrucciones para planificar la implantación de DPM.

En esta sección

Introducción a Data Protection Manager 2007

Microsoft System Center Data Protection Manager (DPM) 2007 es un miembro destacado de la familia de productos de gestión Microsoft System Center, diseñados para ayudar a los profesionales de TI a gestionar el entorno Windows. DPM es el nuevo estándar para la recuperación y las copias de seguridad de Windows ya que ofrece una protección de datos excelente para los servidores de archivos y las aplicaciones de Microsoft mediante el uso de medios de cinta y disco integrados.

En esta sección

Características de DPM

La protección de datos es fundamental para cualquier empresa u organización, y Microsoft System Center Data Protection Manager (DPM) 2007 es una solución eficaz que proporciona dicha protección. DPM ofrece las ventajas siguientes a las empresas:

- Recuperación y protección de datos basada en disco
- Soluciones de almacenamiento y copia de seguridad basadas en cinta
- Soluciones de recuperación de desastres

Puede hacer una copia de seguridad de la base de datos de DPM en cinta o puede utilizar un segundo servidor DPM situado en una ubicación geográfica distinta para proteger el servidor DPM principal.

Si utiliza un segundo servidor DPM, puede restaurar datos en ordenadores protegidos directamente desde el servidor DPM secundario. El servidor DPM secundario también puede proteger ordenadores hasta que el servidor DPM principal vuelva a estar conectado.

- DPM proporciona protección a los elementos siguientes:
  - Datos de archivo de volúmenes, recursos compartidos y carpetas
  - Datos de aplicación, como grupos de almacenamiento de Microsoft Exchange Server, bases de datos de Microsoft SQL Server, conjuntos de Windows SharePoint Services, así como Microsoft Virtual Server y sus máquinas virtuales
  - Archivos para estaciones de trabajo que ejecutan Windows XP Professional SP2 y todas las ediciones de Windows Vista, excepto la edición Home
  - Archivos y datos de aplicación de servidores agrupados en clúster
  - Estado del sistema para servidores de aplicaciones y de archivos protegidos

En esta sección

Soluciones de copia de seguridad que combinan disco y cinta

Protección de varios tipos de datos

Protección de servidores agrupados en clúster

Herramientas de administración

Consulte también

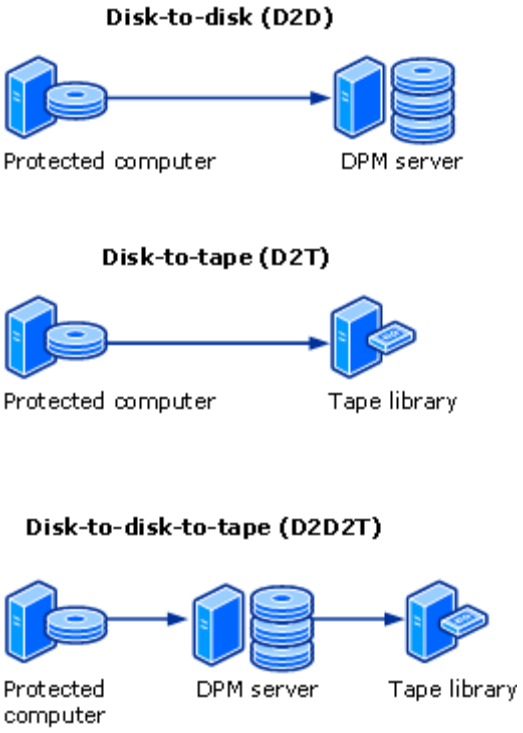
Funcionamiento de DPM

Soluciones de copia de seguridad que combinan disco y cinta

Con la protección de datos de DPM, puede utilizar el almacenamiento basado en disco, el almacenamiento basado en cinta o ambos.

El almacenamiento basado en disco, también denominado *D2D* (de disco a disco), es un tipo de copia de seguridad en el que los datos de un ordenador se almacenan en el disco duro de otro ordenador. Esto contrasta con el método más tradicional de realizar copias de seguridad de un ordenador a un medio de almacenamiento como puede ser una cinta, también denominado *D2T* (de disco a cinta). Para obtener una mayor protección, se pueden combinar ambos métodos en una configuración*D2D2T*(de disco a disco y de disco a cinta) que ofrece las ventajas de recuperación rápida del almacenamiento basado en disco a corto plazo y del almacenamiento de archivado basado en cinta para datos críticos a largo plazo. En la ilustración siguiente se muestran los tres métodos de almacenamiento.

Métodos de almacenamiento de datos



Para determinar qué método de almacenamiento debe utilizar, debe tener en cuenta la importancia relativa de los requisitos de protección de su empresa.

- **La cantidad de datos que la empresa puede permitirse perder?** En realidad, no todos los datos tienen el mismo valor. Las empresas deben sopesar las consecuencias de la pérdida de datos frente a los costes de protección.

- **La rapidez con la que deben estar disponibles los datos recuperados?** La recuperación de datos vitales para operaciones continuas suele ser más urgente que la de datos de rutina. Por otro lado, las empresas deben identificar los servidores que proporcionan los servicios esenciales durante la jornada laboral, que no deben verse afectados por operaciones de recuperación.
- **El periodo de tiempo que la empresa debe conservar los datos?** El almacenamiento a largo plazo puede ser necesario en operaciones comerciales, en función del tipo y del contenido de los datos. También puede que una empresa esté sujeta a requisitos legales de retención de datos, como la Ley Sarbanes-Oxley o la Directiva sobre retención de datos.
- **El importe que la empresa puede gastarse en protección de datos?** Al tener en cuenta la cantidad que se debe invertir en protección de datos, las empresas deben incluir los costes de hardware y soportes multimedia, así como los gastos de personal de administración, gestión y asistencia.

Puede utilizar DPM para hacer copias de seguridad de datos en disco y en cinta. De esta forma, obtendrá la flexibilidad necesaria para crear estrategias de copia de seguridad detalladas y enfocadas que ofrecen una protección de datos económica y eficaz. Si tiene que restaurar un único archivo o un servidor entero, la recuperación es rápida y sencilla: sólo tiene que identificar los datos y DPM los localiza y recupera (aunque quizá sea necesaria su intervención si se ha eliminado la cinta de la biblioteca).

Recuperación y protección basada en disco

Una de las ventajas de la protección de datos basada en disco es la posibilidad de ahorrar tiempo. La protección de datos basada en disco no necesita el tiempo de preparación que sí necesita la protección basada en cinta, para la que se requiere localizar la cinta específica necesaria para una tarea, cargar la cinta y colocarla en el punto de inicio correcto. La facilidad que supone utilizar un disco aumenta la frecuencia de envío de datos incrementales, lo que reduce el impacto en el ordenador que se está protegiendo y en los recursos de red.

La recuperación de datos a través de la protección de datos basada en disco es más fiable que la de los sistemas basados en cinta. Normalmente, las unidades de disco tienen un tiempo medio entre errores (MTBF) mayor que el de las cintas.

La recuperación de datos desde un disco es mucho más rápida y sencilla que desde una cinta. Para poder recuperar los datos desde un disco sólo debe examinar las versiones anteriores de los datos en el servidor DPM y copiar las versiones seleccionadas directamente en el ordenador protegido. Una recuperación de archivos normal desde una cinta puede tardar horas y ser costosa. Normalmente, los administradores de un centro de datos de tamaño medio prevén realizar entre 10 y 20 recuperaciones de este tipo al mes, o incluso más.

Mediante DPM y la protección de datos basada en disco, los datos se pueden sincronizar con una frecuencia de 15 minutos y conservar durante un máximo de 448 días.

Almacenamiento y copia de seguridad basados en cinta

Las cintas magnéticas y otros medios de almacenamiento similares ofrecen una forma económica y portátil de proteger datos que resulta especialmente útil para el almacenamiento a largo plazo.

En DPM, puede hacer copias de seguridad de datos de un ordenador directamente en una cinta (D2T). También puede realizar copias de seguridad de datos de la réplica basada en disco (D2D2T). La ventaja de crear una copia de seguridad a largo plazo en cinta desde la réplica basada en disco es que la operación de copia de seguridad se puede realizar en cualquier momento sin que el ordenador protegido se vea afectado.

Además, un plan de recuperación de desastres completo incluye el almacenamiento de la información crítica en una ubicación externa para que pueda recuperar los datos de su empresa aunque sus instalaciones hayan sufrido daños o hayan quedado destruidas. La cinta es un medio popular y práctico para el almacenamiento en una ubicación externa.

Con DPM, se puede hacer una copia de seguridad de los datos en cinta con una frecuencia diaria para obtener una protección a corto plazo y ésta se puede llegar a conservar durante 99 años para obtener una protección a largo plazo.

Con las soluciones de software de los socios de DPM, podrá utilizar soportes multimedia extraíbles, como una unidad de disco duro USB, en lugar de una cinta. Para obtener más información, consulte Data Protection Manager Partners (Socios de Data Protection Manager) en http://go.microsoft.com/fwlink/?LinkId=98869.

Consulte también

Herramientas de administración

Protección de servidores agrupados en clúster

Protección de varios tipos de datos

Protección de varios tipos de datos

En la tabla siguiente se enumeran los tipos de datos que DPM puede proteger y el nivel de datos que se puede recuperar mediante DPM.

Nota

Para obtener información sobre los requisitos de software específicos de los ordenadores protegidos, consulte DPM System Requirements (Requisitos del sistema DPM) en http://go.microsoft.com/fwlink/?LinkId=66731.

Datos que se pueden proteger y recuperar

Producto	Datos que se pueden proteger	Datos que se pueden recuperar
Exchange Server 2003 Exchange Server 2007	• Grupo de almacenamiento	• Grupo de almacenamiento • Base de datos • Buzón
SQL Server 2000 SQL Server 2005	• Base de datos	• Base de datos
Microsoft Office SharePoint Server 2007 Windows SharePoint Services 3.0	• Conjunto	• Conjunto • Base de datos • Sitio • Archivo o lista
Windows Server 2003 Windows Storage Server 2003	• Volumen • Recurso compartido • Carpeta	• Volumen • Recurso compartido • Carpeta • Archivo
Microsoft Virtual Server 2005 R2 SP1	• Configuración de host del servidor virtual • Máquinas virtuales • Datos de aplicaciones que se ejecutan en máquinas virtuales[1]	• Configuración de host del servidor virtual • Máquinas virtuales • Datos de aplicaciones que se ejecutan en máquinas virtuales[1]

Producto	Datos que se pueden proteger	Datos que se pueden recuperar
Todos los ordenadores que se pueden proteger mediante DPM 2007, excepto aquellos que ejecutan Windows Vista o Windows Server 2008	• Estado del sistema	• Estado del sistema
Estaciones de trabajo que ejecutan Windows XP Professional SP2 y todas las ediciones de Windows Vista, excepto la edición Home (debe ser miembro de un dominio)	• Datos de archivo	• Datos de archivo

[1] Los datos de las aplicaciones que se ejecutan en máquinas virtuales se deben proteger y recuperar como un origen de datos de la aplicación, no como un componente de una máquina virtual protegida. Por ejemplo, para proteger y recuperar datos para una instancia de SQL Server que se ejecuta en una máquina virtual, instale el agente de protección de DPM en la máquina virtual y seleccione el origen de datos como base de datos de SQL Server. Al instalar el agente de protección en el host virtual y proteger una máquina virtual del host, los datos de la aplicación también están protegidos pero sólo se pueden recuperar si se recupera la propia máquina virtual.

Consulte también

Administración de estaciones de trabajo y servidores de archivos protegidos

Administración de servidores protegidos que ejecutan Exchange

Administración de servidores protegidos que ejecutan SQL Server

Administración de servidores protegidos que ejecutan Windows SharePoint Services

Administración de servidores virtuales protegidos

Protección de servidores agrupados en clúster

DPM 2007 admite clústeres de discos compartidos para servidores de archivos, Exchange Server 2003, SQL Server 2000 y SQL Server 2005. DPM 2007 admite clústeres de discos no compartidos y clústeres de discos compartidos para Exchange Server 2007.

Para la instalación del agente de protección de DPM, al seleccionar un servidor que es un nodo del clúster, DPM se lo notifica para que también pueda optar por instalar el agente de protección en otros nodos del clúster.

La recuperación por el usuario final está disponible tanto para recursos agrupados como no agrupados en clúster en servidores de archivos agrupados en clúster.

En una sustitución tras error prevista, DPM continúa ofreciendo protección. En una sustitución tras error no prevista, DPM emite una alerta que indica que es necesario ejecutar una comprobación de coherencia.

Consulte también

Protección de varios tipos de datos

Herramientas de administración

Para facilitar la ejecución de las principales tareas de administración, DPM 2007 proporciona las herramientas y funciones siguientes a los administradores de TI:

- DPM Administrator Console
- Informes y notificaciones
- DPM Management Packs
- Integración de Windows PowerShell
- Administración remota
- Recuperación por el usuario final

DPM Administrator Console

La DPM Administrator Console (Consola de administrador de DPM) utiliza un modelo de administración basado en tareas que automatiza las tareas más habituales, lo que permite al administrador hacer el trabajo con el mínimo número de pasos.

Para simplificar la administración de las actividades de protección de datos, DPM se basa en la función de Microsoft Management Console (MMC) para proporcionar un entorno intuitivo y conocido para realizar tareas de configuración, administración y supervisión.

DPM Administrator Console organiza las tareas en cinco áreas de tareas de fácil acceso: supervisión, protección, recuperación, notificación y administración. Los asistentes guían al administrador a través de las tareas de configuración básicas como la adición de discos, la instalación de agentes y la creación de grupos de protección. Las funciones de búsqueda y exploración se encuentran en el área de tareas **Recovery** (Recuperación) para poder encontrar y recuperar las versiones anteriores de los archivos.

DPM Administrator Console también dispone de una ficha **Jobs** (Trabajos) y de otra ficha **Alerts** (Alertas) para supervisar la actividad de protección de datos. La ficha **Jobs** (Trabajos) ofrece información sobre el estado y funcionamiento de todas las tareas programadas, completadas, en ejecución, canceladas o con errores. La ficha **Alerts** (Alertas) incorpora alertas informativas y condiciones de error para ofrecer una vista de resumen de la actividad de todo el sistema, así como las acciones recomendadas para solucionar cada uno de los errores.

Para obtener información detallada sobre cómo utilizar DPM Administrator Console, consulte Appendix A: DPM Administrator Console (Apéndice A: DPM Administrator Console) en http://go.microsoft.com/fwlink/?LinkId=98871 en el documento *Deploying DPM 2007* (Implantación de DPM 2007).

Informes y notificaciones

DPM ofrece un conjunto completo de informes que proporcionan información sobre las tareas de protección y recuperación que se han realizado correctamente o con errores, así como el uso de discos y cintas. El usuario también puede identificar los errores habituales y administrar la circulación de cintas. Los informes de resumen proporcionan información relativa a todos los ordenadores protegidos y grupos de protección. Los informes detallados proporcionan información sobre determinados ordenadores o grupos de protección. Un administrador puede utilizar dichos informes para ajustar la protección tras la implantación inicial de DPM.

Las notificaciones de DPM constituyen una forma práctica de mantenerse informado cuando se generan alertas críticas, informativas o de advertencia. Puede elegir la gravedad de las alertas que desea que se le notifiquen. Por ejemplo, puede optar por recibir únicamente alertas críticas. También puede elegir recibir notificaciones del estado de las tareas de recuperación y puede recibir informes de DPM programados como archivos adjuntos de correo electrónico para que pueda supervisar las tendencias de protección de datos y analizar las estadísticas de protección de datos cuando lo desee. Asimismo, puede utilizar DPM Management Pack para System Center Operations Manager 2007 para proporcionar notificaciones personalizadas.

Para obtener información detallada sobre los informes disponibles en DPM 2007, consulte Managing DPM Servers (Administración de servidores DPM) en http://go.microsoft.com/fwlink/?LinkId=91853. Para obtener instrucciones sobre cómo suscribirse a las notificaciones, consulte la ayuda de DPM 2007.

DPM Management Packs

Los Management Packs para Microsoft Operations Manager 2005 (MOM) y System Center Operations Manager 2007 estarán disponibles para DPM 2007. Como parte de la estrategia de administración de datos, puede utilizar el DPM Management Pack para supervisar de forma centralizada la protección de datos, el estado y el rendimiento de varios servidores DPM y los servidores que protegen. Desde la Operations Console (Consola de operaciones) de Operations Manager, un administrador puede supervisar la infraestructura de red y DPM al mismo tiempo, así como analizar problemas de protección de datos en el contexto de otros factores relacionados con el rendimiento de la red y del sistema. El administrador también puede supervisar otras aplicaciones de vital importancia, como SQL Server.

Para descargar los DPM Management Packs, consulte Management Pack Catalog (Catálogo de paquetes de administración) en http://go.microsoft.com/fwlink/?LinkId=47215.

Integración de Windows PowerShell

Windows PowerShell es una tecnología interactiva de línea de comandos que también admite la creación de secuencias de comandos basada en tareas.

DPM proporciona su propio conjunto de comandos de Windows PowerShell que pueden utilizarse para realizar tareas de administración de protección de datos. Se accede a los cmdlets de DPM a través del shell de DPM Management.

Un administrador de DPM puede utilizar los cmdlets de DPM para llevar a cabo todas las tareas administrativas que se pueden realizar en la consola, incluidos los conjuntos de cmdlets diseñados para ser utilizados en las tareas siguientes:

- Configurar DPM
- Administrar cintas y discos
- Administrar grupos de protección
- Proteger y recuperar datos

Además, los cmdlets de DPM permiten a los administradores realizar las tareas siguientes, que no se pueden ejecutar mediante DPM Administrator Console:

- Eliminar puntos de recuperación
- Personalizar la hora de inicio de las tareas de mantenimiento de la biblioteca, como un inventario detallado y la limpieza
- Especificar la configuración de la red de área local (LAN) que se va a utilizar para una tarea de copia de seguridad

Administración remota

Puede establecer una conexión a escritorio remoto a un servidor DPM para administrar las operaciones de DPM de forma remota.

El shell de DPM Management se puede instalar en ordenadores que no sean los del servidor DPM, lo que permite administrar varios servidores DPM de forma remota. También puede instalar el shell de DPM Management en ordenadores de escritorio que ejecutan Windows XP o Windows Vista.

Recuperación por el usuario final

Además de la recuperación de datos proporcionada por el administrador, DPM permite a los usuarios recuperar de forma independiente versiones anteriores de sus archivos a través de la interfaz conocida del Explorador de Windows o de cualquier otra aplicación de Microsoft Office 2007. La recuperación por el usuario final no está disponible para los datos de aplicación.

Consulte también

Protección de servidores agrupados en clúster

Protección de varios tipos de datos

Funcionamiento de DPM

El método que utiliza Data Protection Manager para proteger datos varía en función del tipo de datos protegidos y del método de protección seleccionado.

En esta sección

Proceso de protección basado en disco

Proceso de protección basado en cinta

Proceso de recuperación

Política de protección

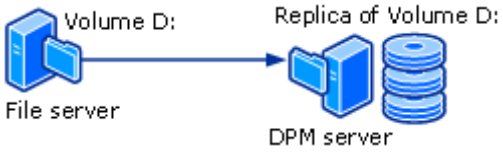
Proceso de detección automática

Estructura de directorios de DPM

Proceso de protección basado en disco

Para la protección de datos basada en disco, el servidor DPM crea y conserva una *réplica* o una copia de los datos que se encuentran en los servidores protegidos. Las réplicas se almacenan en el *bloque de almacenamiento*, que está formado por un conjunto de discos del servidor DPM o de un volumen personalizado. En la ilustración siguiente se muestra la relación básica que existe entre un volumen protegido y su réplica.

Creación de réplicas



Independientemente de si se va a proteger datos de archivo o datos de aplicación, la protección se inicia con la creación de la réplica del origen de datos.

La réplica se *sincroniza* o actualiza a intervalos regulares en función de los valores que haya configurado. El método que DPM utiliza para sincronizar la réplica depende del tipo de datos protegidos. Para obtener más información, consulte Proceso de sincronización de datos de archivo y Proceso de sincronización de datos de aplicación. Si se detecta que una réplica no es coherente, DPM ejecuta una comprobación de coherencia, que es una verificación bloque por bloque de la réplica contra el origen de datos.

Un ejemplo sencillo de una configuración de protección consiste en un servidor DPM y de un ordenador protegido. El ordenador está protegido cuando se instala un *agente de protección* de DPM en el ordenador y se añaden sus datos a un *grupo de protección*.

Los agentes de protección hacen un seguimiento de los cambios que se producen en los datos protegidos y transfieren dichos cambios al servidor DPM. El agente de protección también identifica aquellos datos del ordenador que se pueden proteger y participa en el proceso de recuperación. Debe instalar un agente de protección en cada uno de los ordenadores que desea proteger mediante DPM. Los agentes de protección se pueden instalar a través de DPM o el usuario los puede instalar manualmente mediante aplicaciones como Systems Management Server (SMS).

Los grupos de protección se utilizan para administrar la protección de los orígenes de datos de los ordenadores. Un grupo de protección es un conjunto de orígenes de datos que comparten la misma configuración de protección. La configuración de protección es la recopilación de configuraciones comunes a un grupo de protección, como por ejemplo el nombre del grupo de protección, la política de protección, las asignaciones de disco y el método de creación de réplicas.

DPM almacena una réplica distinta para cada *miembro del grupo de protección* en el bloque de almacenamiento. Un miembro del grupo de protección puede ser cualquiera de los orígenes de datos siguientes:

- Un volumen, un recurso compartido o una carpeta de un ordenador de escritorio, un servidor de archivos o un clúster de servidor
- Un grupo de almacenamiento de un servidor Exchange o de un clúster de servidor
- Una base de datos de una instancia de SQL Server o de un clúster de servidor

Consulte también

Proceso de sincronización de datos de aplicación

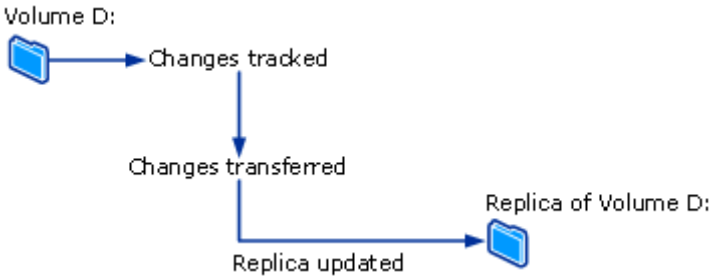
Diferencia entre datos de archivo y datos de aplicación

Proceso de sincronización de datos de archivo

Proceso de sincronización de datos de archivo

En DPM 2007, para un volumen de archivos o un recurso compartido de un servidor, el agente de protección utiliza un filtro de volúmenes y el diario de cambios para determinar qué archivos han cambiado y, a continuación, realiza un procedimiento de suma de comprobación de estos archivos para sincronizar únicamente los bloques modificados. Durante la sincronización, estos cambios se transfieren al servidor DPM y, a continuación, se aplican a la réplica para sincronizarla con el origen de datos. En la ilustración siguiente se muestra el proceso de sincronización de archivos.

Proceso de sincronización de archivos



Si una réplica no es coherente con su origen de datos, DPM genera una alerta que especifica qué ordenador y qué orígenes de datos se ven afectados. Para solucionar el problema, el administrador repara la réplica mediante el inicio de una *sincronización con comprobación de coherencia*que también se denomina simplemente*comprobación de coherencia*, en la réplica. Durante una comprobación de coherencia, DPM realiza una verificación bloque por bloque y repara la réplica para que vuelva a ser coherente con el origen de datos.

Puede programar la ejecución diaria de una comprobación de coherencia de los grupos de protección o iniciarla manualmente.

DPM crea un *punto de recuperación* para el miembro del grupo de protección a intervalos regulares que el usuario puede configurar. Un punto de recuperación es una versión de los datos a partir de la cual se pueden recuperar datos. Para los archivos, un punto de recuperación está formado por una copia simultánea de la réplica, que se crea mediante la función de servicio de copia simultánea de volumen (VSS) del sistema operativo en el servidor DPM.

Consulte también

Proceso de sincronización de datos de aplicación

Diferencia entre datos de archivo y datos de aplicación

Proceso de protección basado en disco

Proceso de sincronización de datos de aplicación

En el caso de los datos de aplicación, después de que DPM haya creado la réplica, los cambios realizados en bloques de volúmenes que pertenecen a archivos de aplicación se someten a un seguimiento por parte del filtro de volúmenes.

El método de transferencia de los cambios al servidor DPM depende de la aplicación y del tipo de sincronización. La operación que en DPM Administrator Console se denomina *sincronización* es similar a una copia de seguridad incremental y crea una reflexión exacta de los datos de aplicación al combinarlos con la réplica.

Durante el tipo de sincronización que en DPM Administrator Console se denomina *copia de seguridad completa*, se crea una instantánea de servicio de copia simultánea de volumen (VSS) completa pero sólo se transfieren los bloques modificados al servidor DPM.

Todas las copias de seguridad completas crean un punto de recuperación para datos de aplicación. Si la aplicación admite copias de seguridad incrementales, todas las sincronizaciones también crean un punto de recuperación. A continuación se resumen los tipos de sincronización admitidos por cada tipo de datos de aplicación:

- Para los datos protegidos de Exchange, la sincronización transfiere una instantánea VSS incremental mediante el escritor de VSS de Exchange. Se crean puntos de recuperación para cada sincronización y copia de seguridad completa.

- Las bases de datos de SQL Server con trasvase de registros en modo de sólo lectura o que utilizan el modelo de recuperación simple no admiten copias de seguridad incrementales. Sólo se crean puntos de recuperación para cada una de las copias de seguridad completas. Para el resto de bases de datos de SQL Server, la sincronización transfiere una copia de seguridad del registro de transacciones y los puntos de recuperación se crean para cada una de las sincronizaciones incrementales y copias de seguridad completas. El registro de transacciones es un registro serie de todas las transacciones realizadas en la base de datos desde la última vez que se hizo una copia de seguridad del registro de transacciones.
- Windows SharePoint Services y Microsoft Virtual Server no admiten copias de seguridad incrementales. Sólo se crean puntos de recuperación para cada una de las copias de seguridad completas.

Las sincronizaciones incrementales requieren menos tiempo que una copia de seguridad completa. Sin embargo, el tiempo necesario para recuperar datos aumenta a medida que aumenta el número de sincronizaciones. Esto es así porque DPM debe restaurar la última copia de seguridad completa y, a continuación, restaurar y aplicar todas las sincronizaciones incrementales hasta el momento preciso seleccionado para la recuperación.

Para que la recuperación sea más rápida, DPM realiza con regularidad una copia de seguridad completa, un tipo de sincronización que actualiza la réplica para incluir los bloques modificados.

Durante la copia de seguridad completa, DPM toma una instantánea de la réplica antes de actualizarla con los bloques modificados. Para que los objetivos de punto de recuperación sean más frecuentes, así como para reducir la ventana de pérdida de datos, DPM también realiza sincronizaciones incrementales entre dos copias de seguridad completas.

Al igual que ocurre con la protección de datos de archivo, si una réplica no es coherente con su origen de datos, DPM genera una alerta que especifica qué servidor y qué origen de datos se ven afectados. Para solucionar el problema, el administrador repara la réplica iniciando una sincronización con comprobación de coherencia en la réplica. Durante una comprobación de coherencia, DPM realiza una verificación bloque por bloque y repara la réplica para que vuelva a ser coherente con los orígenes de datos.

Puede programar la ejecución diaria de una comprobación de coherencia de los grupos de protección o iniciarla manualmente.

Consulte también

Diferencia entre datos de archivo y datos de aplicación

Proceso de protección basado en disco

Proceso de sincronización de datos de archivo

Diferencia entre datos de archivo y datos de aplicación

Los datos presentes en un servidor de archivos y que necesitan ser protegidos como si fueran un archivo plano se clasifican como datos de archivo, como por ejemplo archivos de Microsoft Office, archivos de texto, archivos de procesamiento en lote, entre otros.

Los datos presentes en un servidor de aplicaciones y que requieren que DPM tenga en cuenta la aplicación se clasifican como datos de aplicación, como por ejemplo los grupos de almacenamiento de Exchange, las bases de datos de SQL Server, los conjuntos de Windows SharePoint Services y Virtual Server.

Cada origen de datos se presenta en DPM Administrator Console según el tipo de protección que se puede seleccionar para dicho origen de datos. Por ejemplo, en el asistente para la creación de un nuevo grupo de protección, al expandir un servidor que contiene archivos y que también ejecuta Virtual Server y una instancia de SQL Server, los orígenes de datos se tratan de la forma siguiente:

- Al expandir **All Shares** (Todos los recursos compartidos) o **All Volumes** (Todos los volúmenes), DPM muestra los recursos compartidos y los volúmenes de ese servidor y protegerá todos los orígenes de datos seleccionados en cualquiera de estos nodos como datos de archivo.
- Al expandir **All SQL Servers** (Todos los servidores SQL), DPM muestra las instancias de SQL Server en ese servidor y protegerá todos los orígenes de datos seleccionados en ese nodo como datos de aplicación.
- Al expandir **Microsoft Virtual Server**, DPM muestra la base de datos host y las máquinas virtuales de ese servidor y protegerá todos los orígenes de datos seleccionados en ese nodo como datos de aplicación.

Consulte también

Proceso de sincronización de datos de aplicación

Proceso de protección basado en disco

Proceso de sincronización de datos de archivo

Proceso de protección basado en cinta

Al utilizar la protección basada en disco a corto plazo y la protección basada en cinta a largo plazo, DPM puede realizar copias de seguridad de datos del volumen de réplica en cinta para que el ordenador protegido no se vea afectado. Cuando sólo se utiliza la protección basada en cinta, DPM hace una copia de seguridad en cinta de los datos directamente desde el ordenador protegido.

DPM protege datos en cinta a través de una combinación de copias de seguridad completas e incrementales a partir del origen de datos protegidos (para una protección en cinta a corto plazo o una protección en cinta a largo plazo cuando DPM no protege los datos en disco) o bien a partir de la réplica de DPM (para una protección en cinta a largo plazo cuando la protección a corto plazo se realiza en disco).

Nota

Si se ha abierto un archivo cuando la réplica se ha sincronizado por última vez, la copia de seguridad de dicho archivo de la réplica se encontrará en un *estado coherente tras la interrupción*. Un estado coherente tras la interrupción del archivo contendrá todos los datos del archivo que se almacenaron en el disco en el momento de la última sincronización. Esto sólo se aplica a las copias de seguridad del sistema de archivos. Las copias de seguridad de la aplicación siempre serán coherentes con el estado de la aplicación.

Para obtener información sobre determinados tipos de copia de seguridad y programaciones, consulte Planificación de grupos de protección.

Consulte también

Funcionamiento de DPM

Proceso de protección basado en disco

Proceso de recuperación

El método de protección de datos, ya sea basado en disco o en cinta, no afecta a la tarea de recuperación. Se selecciona el punto de recuperación de datos que se desea recuperar y DPM recupera los datos en el ordenador protegido.

DPM puede almacenar un máximo de 64 puntos de recuperación para cada archivo miembro de un grupo de protección. Para orígenes de datos de aplicación, DPM puede almacenar un máximo de 448 copias de seguridad completas y hasta 96 copias de seguridad incrementales para cada copia de seguridad completa. Si se han alcanzado los límites del área de almacenamiento pero el intervalo de retención de los puntos de recuperación existentes todavía no ha concluido, las tareas de protección fallarán.

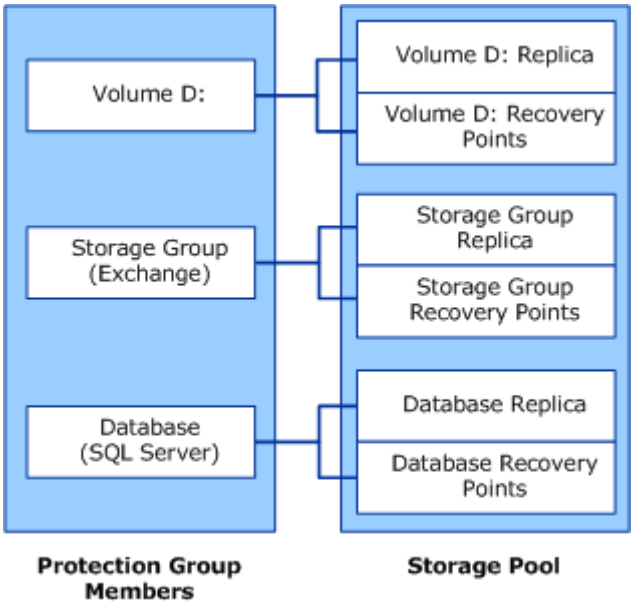
Nota

Para admitir la recuperación por el usuario final, el servicio de instantáneas de volumen (VSS) limita a 64 los puntos de recuperación de los archivos.

Tal como se explica en Proceso de sincronización de datos de archivo y Proceso de sincronización de datos de aplicación, el proceso de creación de puntos de recuperación varía según si se trata de datos de archivo o de datos de aplicación. DPM crea puntos de recuperación para datos de archivo tomando una copia simultánea de la réplica según la programación configurada. Para los datos de aplicación, todas las sincronizaciones y las copias de seguridad completas crean un punto de recuperación.

En la ilustración siguiente se muestra cómo se asocia cada uno de los miembros del grupo de protección a su propio volumen de réplica y de punto de recuperación.

Miembros del grupo de protección, réplicas y puntos de recuperación



Los administradores recuperan datos de los puntos de recuperación disponibles mediante el asistente para la recuperación de DPM Administrator Console. Al seleccionar un origen de datos y un momento preciso a partir del que se inicia la recuperación, DPM notifica si los datos se encuentran en una cinta, si la cinta está conectada o desconectada y qué cintas son necesarias para completar la recuperación.

Los usuarios pueden recuperar versiones anteriores de archivos protegidos. Puesto que los puntos de recuperación conservan la misma estructura de carpetas y de archivos de los orígenes de datos protegidos, los usuarios pueden examinar volúmenes, carpetas y recursos compartidos conocidos para recuperar los datos que desean. La recuperación por el usuario final no está disponible para los datos de aplicación, como en el caso de un buzón de Exchange. Asimismo, las versiones de datos de archivo disponibles para la recuperación por el usuario final son las que están almacenadas en disco en el bloque de almacenamiento de DPM. Los datos de archivo que se han almacenado en cinta sólo los puede recuperar un administrador.

Los usuarios finales recuperan archivos protegidos por medio de un ordenador cliente que ejecuta el software cliente de copia simultánea. Los usuarios pueden recuperar versiones anteriores mediante recursos compartidos en los servidores de archivos, espacios de nombres DFS (sistema de archivos distribuido) o mediante un comando del menú **Herramientas** de las aplicaciones de Microsoft Office.

Consulte también

Proceso de sincronización de datos de aplicación

Proceso de sincronización de datos de archivo

Política de protección

DPM configura la *política de protección*o la programación de tareas de cada grupo de protección en función de los objetivos de recuperación especificados para ese grupo de protección. A continuación se ofrecen algunos ejemplos de objetivos de recuperación:

- "No perder más de 1 hora de datos de producción"
- "Conseguir un intervalo de retención de 30 días"
- "Hacer que los datos estén disponibles para su recuperación durante 7 años"

Los *objetivos de recuperación* cuantifican los requisitos de protección de datos de cada empresa. En DPM, los objetivos de recuperación se definen por el intervalo de retención, la tolerancia a la pérdida de datos, la programación de puntos de recuperación y, en el caso de aplicaciones de base de datos, la programación de copias de seguridad completas.

El *intervalo de retención* es el tiempo que se necesita que estén disponibles los datos almacenados en la copia de seguridad. Por ejemplo, si necesita que los datos actuales estén disponibles durante una semana, dos semanas o un año a partir del día de hoy.

La tolerancia a la pérdida de datos es la cantidad máxima de pérdida de datos, medida en tiempo, aceptable para los requisitos de la empresa que determinará la frecuencia con la que DPM debe sincronizarse con el servidor protegido recopilando las modificaciones de datos del servidor protegido. Puede cambiar la frecuencia de sincronización por cualquier intervalo comprendido entre 15 minutos y 24 horas. También puede seleccionar que la sincronización se produzca justo antes de que se cree un punto de recuperación, en vez de en un horario determinado.

La *programación de puntos de recuperación* establece cuántos puntos de recuperación de este grupo de protección deben crearse. En el caso de la protección de archivos, se seleccionan los días y las horas para los que se desea que se creen puntos de recuperación. Para la protección de datos de aplicaciones que admiten copias de seguridad incrementales, la frecuencia de sincronización determina la programación de puntos de recuperación. Para la protección de datos de aplicaciones que no admiten copias de seguridad incrementales, la programación de copias de seguridad completas determina la programación de puntos de recuperación.

Nota

Al crear un grupo de protección, DPM identifica el tipo de datos protegidos y ofrece únicamente las opciones de protección disponibles para estos datos.

Consulte también

Funcionamiento de DPM

Proceso de detección automática

La detección automática es el proceso diario por el cual DPM detecta automáticamente ordenadores nuevos o eliminados de la red. Una vez al día, a la hora que el usuario puede programar, DPM envía un paquete pequeño (de menos de 10 kilobytes) a la controladora de dominio más cercana. La controladora de dominio responde a la petición LDAP con los ordenadores de ese dominio y DPM identifica los ordenadores nuevos y los que se han eliminado. El tráfico de red generado por el proceso de detección automática es mínimo.

La detección automática no detecta los ordenadores nuevos o eliminados de otros dominios. Para instalar un agente de protección en un ordenador de otro dominio, debe identificar el ordenador mediante un nombre de dominio completamente calificado.

Consulte también

Funcionamiento de DPM

Estructura de directorios de DPM

Al empezar a proteger datos con DPM, se dará cuenta de que la ruta de instalación de DPM contiene tres carpetas en el directorio Volumes:

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

La carpeta DiffArea contiene volúmenes de copia simultánea montados que almacenan los puntos de recuperación para un origen de datos.

La carpeta Replica contiene volúmenes de réplica montados.

La carpeta ShadowCopy contiene copias de seguridad locales de la base de datos de DPM. Además, al utilizar DPMBackup.exe para crear copias de seguridad simultáneas de las réplicas para archivado mediante software de copia de seguridad de otro fabricante, las copias de seguridad simultáneas se almacenan en la carpeta ShadowCopy.

Consulte también

Funcionamiento de DPM

Requisitos del sistema

Para obtener información sobre los requisitos de hardware y software de DPM y de los ordenadores protegidos, consulte System Requirements (Requisitos del sistema) en http://go.microsoft.com/fwlink/?LinkId=66731.

Licencia de DPM

Se utiliza una única licencia para cada uno de los ordenadores protegidos por DPM. El tipo de licencia guarda relación con el tipo de datos protegidos.

DPM cuenta con dos tipos de licencia: standard (estándar) y enterprise (empresarial). La licencia estándar da derecho a proteger volúmenes, recursos compartidos y carpetas, así como el estado del sistema informático. La licencia empresarial da derecho a proteger datos de aplicación, como buzones y bases de datos de Exchange Server, además de archivos. En un clúster de servidor, DPM instala un agente en cada nodo del clúster. Se utiliza una licencia para cada nodo del servidor.

En la tabla siguiente se indican las licencias que se aplican a cada tipo de datos.

Licencias DPM utilizadas para los distintos tipos de datos

Tipo de datos protegidos	Licencia utilizada
Sólo archivos	Standard
Archivos en un solo nodo de un clúster de servidor	Standard
Estado del sistema	Standard
SQL Server. Un agente de protección de DPM en un ordenador que ejecuta SQL Server da derecho a proteger bases de datos para todas las instancias de SQL en ese ordenador.	Enterprise
Exchange Server	Enterprise
Windows SharePoint Services. En un conjunto de Windows SharePoint Services, se utiliza una licencia para cada servidor de backend y una licencia para el servidor web de aplicaciones para usuario.	Enterprise
Virtual Server. En un ordenador que ejecuta Virtual Server, un único agente de protección instalado en el ordenador permite proteger cualquier número de máquinas virtuales, o invitados, en el ordenador host. Para proteger determinados datos de aplicación dentro de una máquina virtual, como proteger bases de datos para una instancia de SQL Server que se ejecuta en una máquina virtual, debe instalar un agente de protección directamente en la máquina virtual. Al proteger datos en una máquina virtual que tiene instalado un agente de protección, se utiliza la licencia adecuada para el tipo de datos protegidos.	Enterprise
Otro servidor DPM	Enterprise
Datos para la recuperación bare-metal mediante la herramienta de recuperación del sistema DPM	Enterprise

No se utiliza una licencia al instalar un agente de protección en un ordenador. Sólo se aplica la licencia cuando se añaden datos de un ordenador a un grupo de protección. Si ya no va a proteger ningún dato de un ordenador determinado, puede reutilizar esa licencia en otro ordenador.

Cuando cambia el tipo de datos protegidos, DPM actualiza automáticamente el uso de la licencia. Por ejemplo, va a proteger un grupo de almacenamiento de Exchange y archivos de un único servidor, por lo que ha utilizado una licencia empresarial para proteger dicho servidor. Posteriormente, detiene la protección del grupo de almacenamiento de Exchange. Puesto que DPM ahora protege únicamente datos de archivo de ese servidor, el uso de la licencia deberá cambiar a una licencia estándar.

Si sólo dispone de licencias empresariales y necesita proteger datos de archivo en un ordenador nuevo, puede utilizar una licencia empresarial. Por ejemplo, cuenta con tres licencias estándar y tres licencias empresariales. Va a proteger datos de archivo de tres ordenadores. Añade datos de archivo de un cuatro ordenador a un grupo de protección. Dado que ya se han utilizado todas las licencias estándar, DPM aplicará una licencia empresarial.

Durante la instalación de DPM, introduzca el número de licencias que ha adquirido. Una vez finalizada la instalación, para actualizar la información de las licencias, en el área de tareas **Protection** (Protección) de DPM Administrator Console, en el panel **Actions** (Acciones), haga clic en **View DPM licenses** (Ver licencias de DPM) y, a continuación, cambie el número de licencias adquiridas según convenga.

Puede adquirir licencias de DPM adicionales a través de Microsoft Partner Program en http://go.microsoft.com/fwlink/?LinkId=71663.

Planificación de grupos de protección

Con el fin de crear un plan eficaz para la implantación de Microsoft System Center Data Protection Manager (DPM) 2007, debe analizar minuciosamente los requisitos de su empresa con respecto a la protección y recuperación de datos y sopesar dichos requisitos con las funciones de DPM.

En esta sección se ofrece la información necesaria para planificar la pertenencia y configuración de sus grupos de protección. Como parte de la configuración de los grupos de protección, deberá definir los objetivos de recuperación para los datos protegidos.

En el contexto de Microsoft Operations Framework (MOF), en esta sección se presupone que este cambio (es decir, la integración de DPM en su organización para proporcionar protección y recuperación de datos) ha sido aprobado y que su tarea es la de planificar cómo implementarlo.

Para obtener más información sobre la administración de cambios en MOF, consulte Service Management Functions: Change Management (Funciones de administración de servicios: administración de cambios) en http://go.microsoft.com/fwlink/?LinkId=68729.

Asimismo, esta sección da por sentado que va a integrar DPM en una estrategia de recuperación de desastres ya existente de su empresa. Para obtener más información sobre la planificación de una estrategia de recuperación de desastres, consulte Introduction to Backup and Recovery Services (Introducción a los servicios de copia de seguridad y recuperación) en http://go.microsoft.com/fwlink/?LinkId=71721.

En esta sección

¿Qué desea proteger?

Para iniciar la planificación de la implantación de DPM, en primer lugar debe decidir qué datos desea proteger. DPM 2007 ofrece protección para los tipos de datos siguientes, que se explican más detalladamente en temas posteriores:

- Datos de archivo, a nivel de volúmenes, carpetas y recursos compartidos, en servidores de archivos que ejecutan el sistema operativo Microsoft Windows Server 2003 o Windows Server 2008
- Datos de archivo en estaciones de trabajo que ejecutan Microsoft Windows XP Professional SP2 y todas las ediciones del sistema operativo Windows Vista, excepto la edición Home
- Datos de Microsoft Exchange Server 2003 SP2 y Exchange Server 2007, a nivel de grupos de almacenamiento
- Datos de Microsoft SQL Server 2000 SP4, SQL Server 2005 SP1 y SQL Server 2005 SP2, a nivel de bases de datos
- Windows SharePoint Services 3.0 y Microsoft Office SharePoint Server 2007, a nivel de conjuntos
- Configuraciones de host e invitado de Microsoft Virtual Server 2005 R2 SP1
- Estado del sistema

Consulte también

Datos de aplicación

Recursos agrupados en clúster

Datos de archivo en servidores y estaciones de trabajo

Estado del sistema

Datos de archivo en servidores y estaciones de trabajo

Puede proteger volúmenes accesibles a través de letras de unidad o puntos de montaje, carpetas y recursos compartidos.

La forma más sencilla de seleccionar los datos que desea proteger consiste en seleccionar todos los datos de archivo que incluya en sus copias de seguridad actuales. Otra posibilidad es seleccionar únicamente subconjuntos específicos de datos que desea proteger.

El principal factor que debe tenerse en cuenta al seleccionar los datos es la necesidad de recuperar rápidamente copias de los datos en un momento preciso si éstos se pierden o resultan dañados. Los principales candidatos a ser protegidos son archivos que cambian con frecuencia. Otros buenos candidatos son archivos a los que se accede con asiduidad, independientemente de la frecuencia con la que se modifican.

Importante

Aunque los volúmenes de servidores de archivos se suelen formatear como NTFS, proceso necesario para la protección de DPM, no resulta extraño que los volúmenes de estaciones de trabajo se formateen como FAT o FAT32. Para proteger estos volúmenes, debe convertirlos a NTFS. Para obtener instrucciones, consulte How to Convert FAT Disks to NTFS (Cómo convertir discos FAT a NTFS) en http://go.microsoft.com/fwlink/?LinkId=83022.

Consulte también

Exclusión de archivos y carpetas

Protección de datos en espacios de nombres DFS

Tipos de datos no admitidos

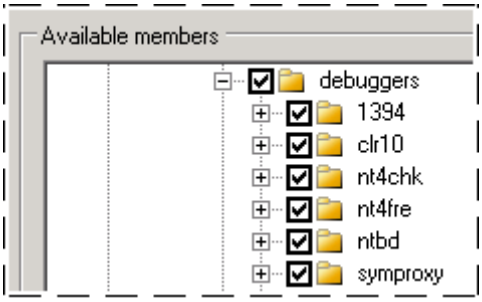
¿Qué desea proteger?

Exclusión de archivos y carpetas

Es posible configurar la protección de datos de tal modo que excluya carpetas especificadas y tipos de archivos según la extensión del nombre de archivo.

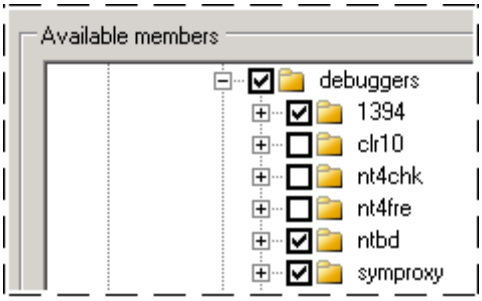
Al seleccionar un volumen o un recurso compartido que proteger, se seleccionan automáticamente todos los elementos secundarios que se pueden proteger de dicho volumen o recurso compartido, tal como se muestra en la ilustración siguiente.

Todos los elementos secundarios seleccionados automáticamente



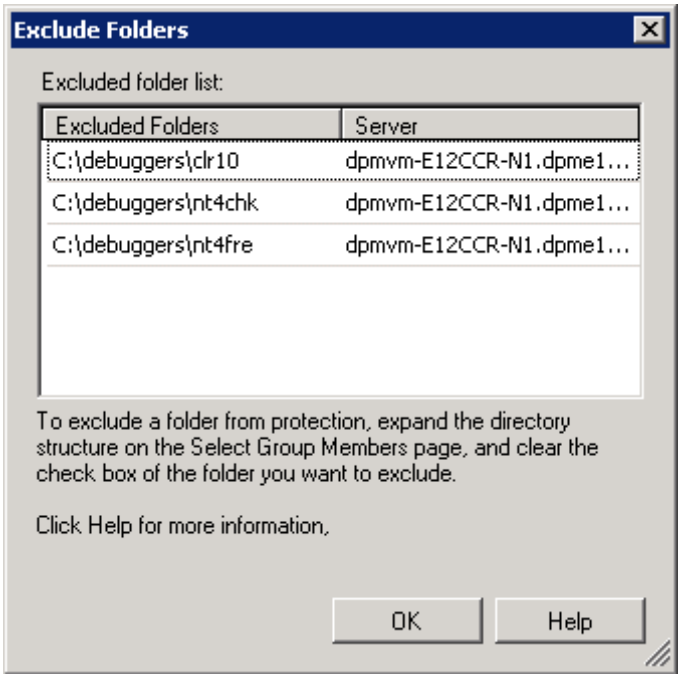
Para excluir una carpeta de la protección, asegúrese de que el elemento principal de la carpeta que no desea proteger está seleccionado y, a continuación, desactive la casilla de verificación de la carpeta que no desea proteger, tal como se muestra en la ilustración siguiente.

Carpeta excluida de la protección



Cuando haya seleccionado los miembros del grupo de protección, podrá ver las carpetas excluidas, tal como se muestra en la ilustración siguiente.

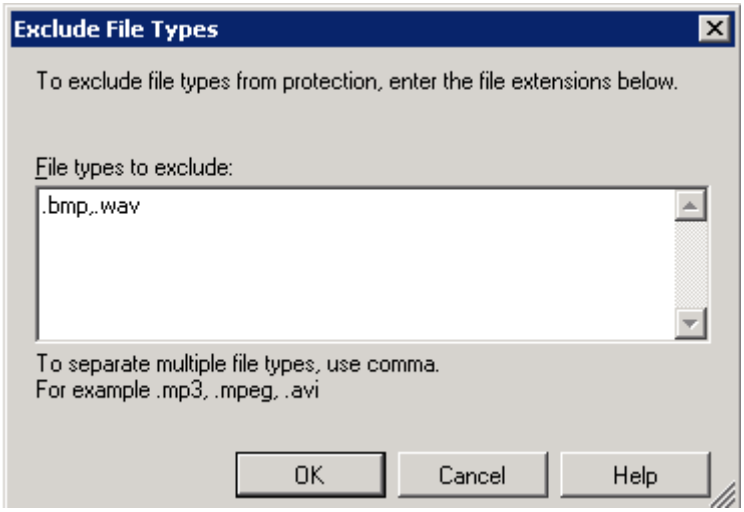
Vista de carpetas excluidas



También puede especificar extensiones de nombres de archivo para excluirlas de la protección en el nivel del grupo de protección. Por ejemplo, cabe la posibilidad de que un servidor de archivos contenga archivos de música o archivos personales para los que su empresa no desea destinar espacio de disco ni amplitud de banda de red para protegerlos. La exclusión por extensión de nombre de archivo se aplica a todos los miembros del grupo de protección.

En la ilustración siguiente se muestra cómo excluir archivos de la protección según la extensión de nombre de archivo.

Exclusión por extensión de nombre de archivo



Consulte también

Protección de datos en espacios de nombres DFS

Tipos de datos no admitidos

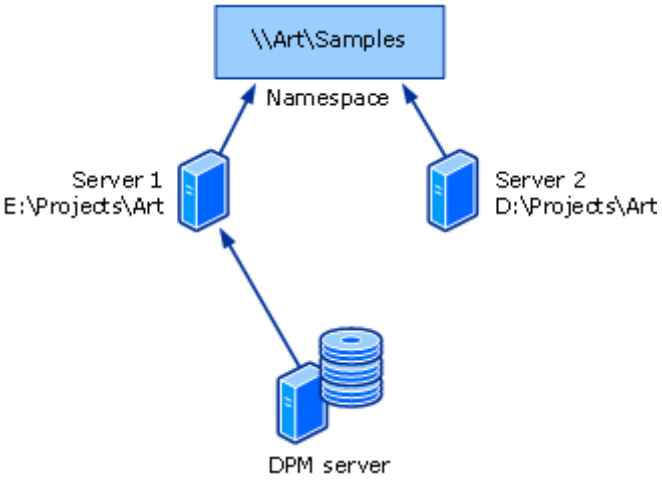
Protección de datos en espacios de nombres DFS

Puede proteger datos que formen parte de una jerarquía de espacios de nombres de un sistema de archivos distribuido (DFS). Sin embargo, no puede seleccionar recursos compartidos que proteger mediante la jerarquía de espacios de nombres DFS. En su lugar, puede seleccionar recursos compartidos que proteger sólo mediante sus rutas de destino.

Si el espacio de nombre incluye raíces o enlaces que tengan varios destinos con los mismos datos, recomendamos proteger únicamente uno de los destinos. No es necesario proteger varios destinos con los mismos datos.

En la ilustración siguiente se muestra la protección de un destino de espacios de nombres DFS mediante DPM.

Protección de un destino de espacios de nombres DFS mediante DPM



Cuando la recuperación por el usuario final de un destino protegido está activada, los usuarios pueden acceder a versiones anteriores de los archivos a través de la jerarquía de espacios de nombres DFS. Cuando los usuarios finales intentan acceder a versiones anteriores de archivos de un recurso compartido que tiene varios destinos, DPM los dirige de forma transparente al destino protegido.

Consulte también

Exclusión de archivos y carpetas

Tipos de datos no admitidos

Tipos de datos no admitidos

Si un origen de datos protegidos contiene un tipo de datos no admitido, DPM continúa protegiendo los tipos de datos admitidos del origen de datos afectado, pero no protege los datos no admitidos.

Si DPM detecta alguno de los siguientes tipos de datos en un origen de datos protegidos, los datos afectados no se protegen:

- Enlaces físicos
- Puntos de reanálisis sintáctico, incluidos los enlaces DFS y los puntos de unión

  Importante

  Un grupo de protección puede contener datos con puntos de montaje. Cuando un grupo de protección incluye puntos de montaje, DPM protege el volumen montado que es el destino del punto de montaje, pero no protege los metadatos del punto de montaje. Cuando recupere datos que contienen puntos de montaje, deberá recrear manualmente la jerarquía de puntos de montaje. DPM no admite la protección de volúmenes montados dentro de volúmenes montados.
- Papelera de reciclaje
- Archivos de paginación
- Carpeta de información de volumen del sistema

  Nota

  La carpeta de información de volumen del sistema no puede protegerse como origen de datos de archivo. Para proteger la información del sistema de un ordenador, debe seleccionar el estado del sistema del ordenador como miembro del grupo de protección en el asistente para la creación de un nuevo grupo de protección.
- Volúmenes no formateados con NTFS

Si un archivo contiene enlaces físicos o simbólicos desde Windows Vista, DPM no puede replicar ni recuperar los archivos.

DPM no puede proteger archivos que tengan cualquiera de las siguientes combinaciones de atributos de archivos:

- Cifrado y reanálisis
- Cifrado y SIS (Almacenamiento de una única instancia)
- Cifrado y distinción entre mayúsculas y minúsculas
- Cifrado y dispersión
- Distinción entre mayúsculas y minúsculas y SIS
- Dispersión y reanálisis
- Compresión y SIS

Consulte también

Exclusión de archivos y carpetas

Protección de datos en espacios de nombres DFS

Datos de aplicación

Puede utilizar DPM para proteger los siguientes tipos de datos de aplicación:

- **Grupos de almacenamiento de Exchange Server.** DPM puede proteger grupos de almacenamiento de Microsoft Exchange Server 2003 SP2 y Exchange Server 2007.
  - No puede excluir de la protección ninguna base de datos del grupo de almacenamiento seleccionado.
  - Todos los grupos de almacenamiento de un ordenador que ejecuta Exchange Server 2003 deben ser miembros del mismo grupo de protección o no podrá proteger estos grupos de almacenamiento.
  - Debe desactivar el registro circular de los grupos de almacenamiento protegidos.
- **Bases de datos de SQL Server.** DPM puede proteger bases de datos de Microsoft SQL Server 2000 SP4, SQL Server 2005 SP1 y SQL Server 2005 SP2.
  - Cada base de datos de una instancia de SQL Server puede pertenecer al mismo grupo de protección o a uno diferente.
  - No puede excluir de la protección ningún dato de la base de datos seleccionada.
- DPM no admite la copia de seguridad incremental para las siguientes bases de datos:
  - Bases de datos master de SQL Server 2000 y SQL Server 2005
  - Bases de datos msdb de SQL Server 2000
  - Bases de datos model de SQL Server 2000

- **Datos de Windows SharePoint Services.** DPM puede proteger conjuntos de servidores que ejecutan Windows SharePoint Services 3.0 u Office SharePoint Server 2007.
  - No puede excluir de la protección ningún dato del conjunto seleccionado.
- **Virtual Server y máquinas virtuales.** DPM puede proteger un host de Virtual Server (un ordenador que ejecuta Virtual Server 2005 R2 SP1) y a los *invitados*, o máquinas virtuales, que se ejecutan dentro del contexto de dicho host.

Además, DPM puede proteger los datos de aplicaciones que se ejecutan en el invitado. No obstante, los datos de las aplicaciones que se ejecutan en máquinas virtuales se deben proteger y recuperar como un origen de datos de la aplicación, no como un componente de una máquina virtual protegida. Por ejemplo, para proteger y recuperar datos para una instancia de SQL Server que se ejecuta en una máquina virtual, seleccione el origen de datos como base de datos de SQL Server. Cuando se protege una máquina virtual, también se protegen los datos de aplica-ción, pero éstos sólo los puede recuperar la propia máquina virtual.

Consulte también

Recursos agrupados en clúster

Datos de archivo en servidores y estaciones de trabajo

Estado del sistema

Recursos agrupados en clúster

DPM puede proteger clústeres de disco compartidos de las siguientes aplicaciones:

- Servidores de archivos
- SQL Server 2000 con Service Pack 4 (SP4)
- SQL Server 2005 con Service Pack 1 (SP1)
- Exchange Server 2003 con Service Pack 2 (SP2)
- Exchange Server 2007

DPM puede proteger clústeres de disco no compartidos de Exchange Server 2007 (réplica continua de clúster). DPM también puede proteger una aplicación Exchange Server 2007 configurada para una réplica continua local.

Consulte también

Datos de aplicación

Datos de archivo en servidores y estaciones de trabajo

Estado del sistema

Estado del sistema

DPM puede proteger el estado del sistema de cualquier ordenador en el que se pueda instalar un agente de protección de DPM, excepto aquellos ordenadores que ejecutan Windows Vista o Windows Server 2008.

Estado del sistema de una estación de trabajo o de un miembro del servidor

Cuando DPM realiza una copia de seguridad del estado del sistema de una estación de trabajo o de un miembro del servidor, se protegen los componentes siguientes:

- Los archivos de inicio
- La base de datos de registro de clase COM+
- El registro
- Los archivos del sistema que se encuentran en Protección de archivos de Windows

Estado del sistema de la controladora de dominio

Cuando DPM realiza una copia de seguridad del estado de una controladora de dominio, se protegen los componentes siguientes:

- Los servicios de dominio de Active Directory (NTDS)
- Los archivos de inicio
- La base de datos de registro de clase COM+
- El registro
- El volumen del sistema (SYSVOL)

Estado del sistema de Servicios de Certificate Server

Cuando DPM realiza una copia de seguridad del estado del sistema de un servidor miembro o una controladora de dominio con Servicios de Certificate Server instalado, además de los componentes del estado del sistema del servidor miembro o de la controladora de dominio se protege Servicios de Certificate Server.

Estado del sistema del servidor de clústeres

Cuando DPM realiza una copia de seguridad del estado del sistema de un servidor de clústeres, además de los componentes del estado del sistema del servidor miembro se protegen los metadatos del servicio de clúster.

Consulte también

Datos de aplicación

Recursos agrupados en clúster

Datos de archivo en servidores y estaciones de trabajo

¿Cuáles son sus objetivos de recuperación?

A la hora de planificar la protección de datos, debe establecer objetivos de recuperación realistas para cada origen de datos que desee proteger. No toda la información o datos mantenidos en los ordenadores de su empresa requieren el mismo grado de protección ni merecen el mismo tipo de inversión en protección. Su plan de implantación debe establecer objetivos de recuperación para cada origen de datos de acuerdo con sus necesidades empresariales con respecto a la protección de datos.

En DPM, los objetivos de recuperación se establecen en términos de *frecuencia de sincronización*, *programación de puntos de recuperación* e *intervalo de retención*, tal como se indica a continuación:

- La frecuencia de sincronización debe seleccionarse en función de la tolerancia a la pérdida de datos, o de la cantidad de datos que puede perder. Puede especificar que la sincronización de un grupo de protección tenga lugar con una frecuencia de 15 minutos. También es posible especificar sincronizaciones de menor frecuencia. Como mínimo, DPM debe sincronizar las réplicas de un grupo de protección al menos una vez entre puntos de recuperación.
- La programación de puntos de recuperación establece cuántos puntos de recuperación de estos datos deben crearse y cuándo. Un punto de recuperación es la fecha y la hora de una versión de un origen de datos que se puede recuperar de los medios administrados por DPM.
- El intervalo de retención es el tiempo que se necesita que estén disponibles los datos almacenados en la copia de seguridad. Para determinar el intervalo de retención necesario, tome en consideración el patrón de peticiones de recuperación que se da en su empresa. Si las peticiones se concentran en un plazo de dos semanas de la pérdida de datos, 10 días podría ser un intervalo de retención adecuado para usted. Si las peticiones se concentran más adelante, puede que necesite un intervalo de retención mayor.

Por ejemplo, los objetivos de recuperación de una base de datos específica de Exchange Server podrían ser que los datos más recientes nunca tengan más de 30 minutos, que sea posible seleccionar versiones creadas con intervalos de 30 minutos, que puedan recuperarse desde disco durante 14 días y que puedan recuperarse desde cinta durante 3 años.

Consulte también

Planificación de configuraciones de protección

Objetivos de recuperación de la protección basada en disco

Objetivos de recuperación de la protección basada en cinta

¿Qué desea proteger?

Objetivos de recuperación de la protección basada en disco

Aunque todos los miembros de un grupo de protección comparten la misma frecuencia de sincronización, el proceso de sincronización y la programación de puntos de recuperación resultante difieren en función del tipo de datos protegidos. Para obtener más información, consulte Funcionamiento de DPM.

Sincronización y puntos de recuperación de archivos

Para un volumen de archivo o un recurso compartido, el agente de protección del ordenador protegido realiza un seguimiento de los bloques modificados en el diario de cambios que forma parte del sistema operativo. Durante la sincronización, estos cambios se transfieren al servidor DPM y, a continuación, se aplican a la réplica para sincronizarla con el origen de datos.

Puede seleccionar un intervalo de frecuencia de sincronización comprendido entre 15 minutos y 24 horas. El valor predeterminado es 15 minutos. También puede seleccionar realizar una sincronización sólo antes de la creación de un punto de recuperación.

Los puntos de recuperación, que son copias simultáneas de la réplica de datos de archivo, se crean a partir de la réplica sincronizada en una programación configurable. Cada sincronización de archivo no tiene como resultado un punto de recuperación a menos que realice la sincronización únicamente antes de cada punto de recuperación; no obstante, puede crear manualmente un punto de recuperación a partir de la sincronización de archivo más reciente.

Por ejemplo, un volumen se sincroniza cada hora y se crea un punto de recuperación para el volumen a las 8:00, 12:00 y 18:00. Un usuario modifica un archivo del volumen a las 13:30; sin embargo, cuando otro usuario realiza cambios una hora más tarde, el archivo resulta dañado sin querer y se le solicita que recupere el archivo con los cambios del primer usuario. Debido a que los cambios de las 13:30 se realizaron después de crear el punto de recuperación más reciente a las 12:00, no es posible recuperar el archivo a partir del punto de recuperación más reciente. Sin embargo, sí es posible crear manualmente un punto de recuperación a partir de la sincronización correspondiente de dicha réplica y, a continuación, recuperar el archivo a partir del nuevo punto de recuperación.

La programación predeterminada crea puntos de recuperación a las 8:00, 12:00 y 18:00 cada día. Es posible modificar tanto las horas como los días específicos. No es posible, sin embargo, especificar diferentes horas para diferentes días. Por ejemplo, puede programar puntos de recuperación para las 2:00 y las 14:00 sólo de lunes a viernes; sin embargo, no es posible programar puntos de recuperación para las 2:00 de lunes a viernes y las 12:00 los fines de semana.

Intervalo de retención de archivos

El intervalo de retención es el periodo de tiempo durante el que se pueden recuperar los datos. Cuando el intervalo de retención de un punto de recuperación caduca, el punto de recuperación se elimina.

Puede seleccionar un intervalo de retención de entre 1 y 448 días para una protección basada en disco a corto plazo, de hasta 12 semanas para una protección basada en cinta a corto plazo y de hasta 99 años para una protección basada en cinta a largo plazo. DPM puede almacenar un máximo de 64 puntos de recuperación para cada archivo miembro de un grupo de protección.

Por ejemplo, si selecciona sincronizar antes de cada punto de recuperación, programa 6 puntos de recuperación al día y establece un intervalo de retención de 10 días, los puntos de recuperación de los archivos contenidos en dicho grupo de protección nunca superan los 64. Sin embargo, si selecciona una combinación que excede el límite de 64 puntos de recuperación, DPM le advierte durante el proceso de configuración de que puede modificar las selecciones ya que no es posible configurar una protección de archivos que exceda el límite de 64 puntos de recuperación.

Sincronización y puntos de recuperación de datos de aplicación

En el caso de los datos de aplicación, los cambios realizados en bloques de volúmenes que pertenecen a archivos de aplicación se someten a un seguimiento por parte del filtro de volúmenes. La sincronización de datos de aplicación es similar a una copia de seguridad incremental y crea una reflexión exacta de los datos de aplicación al combinarlos con la réplica.

Puede seleccionar un intervalo de frecuencia de sincronización comprendido entre 15 minutos y 24 horas. El valor predeterminado es 15 minutos. También puede seleccionar realizar una sincronización sólo antes de la creación de un punto de recuperación. Si selecciona sincronizar únicamente antes de crear un punto de recuperación, DPM lleva a cabo una copia de seguridad completa para sincronizar la réplica de acuerdo con la programación de puntos de recuperación.

En caso de aplicaciones que admitan copias de seguridad incrementales, la programación predeterminada tiene como resultado puntos de recuperación para cada sincronización (cada 15 minutos) y para la copia de seguridad completa a las 20:00 cada día. En caso de aplicaciones que no admitan copias de seguridad incrementales, la programación predeterminada tiene como resultado un punto de recuperación para la copia de seguridad completa a las 20:00 cada día.

Es posible modificar tanto las horas como los días específicos. No es posible, sin embargo, especificar diferentes horas para diferentes días. Por ejemplo, puede programar puntos de recuperación para las 2:00 y las 14:00 sólo de lunes a viernes; sin embargo, no es posible programar puntos de recuperación para las 2:00 de lunes a viernes y las 12:00 los fines de semana.

Excepción para algunas bases de datos de SQL Server

Las copias de seguridad de registros de transacciones, utilizadas por DPM para la sincronización incremental de datos de aplicación, no se pueden llevar a cabo para una base de datos de SQL Server que sea de sólo lectura, configurada para el trasvase de registros o para utilizar el modelo de recuperación simple. Para dichas bases de datos de SQL Server, los puntos de recuperación corresponden a cada copia de seguridad completa.

Comparación de la sincronización y la copia de seguridad completa

Con el fin de posibilitar un tiempo de recuperación más rápido, DPM llevará cabo periódicamente una copia de seguridad completa en lugar de una sincronización incremental. Una copia de seguridad completa es un tipo de sincronización que actualiza la réplica para incluir los bloques modificados.

Nota

Puede modificar la programación de copias de seguridad completas de cualquier grupo de protección que contenga datos de aplicación mediante la acción **Optimize performance** (Optimizar rendimiento) del área de tareas **Protection** (Protección) o mediante el asistente para la modificación de grupos.

Intervalo de retención de datos de aplicación

Puede seleccionar un intervalo de retención de entre 1 y 448 días para una protección basada en disco a corto plazo, de hasta 12 semanas para una protección basada en cinta a corto plazo y de hasta 99 años para una protección basada en cinta a largo plazo.

Por ejemplo, si selecciona sincronizar cada 15 minutos y establece un intervalo de retención de 10 días, dichos objetivos de recuperación darán como resultado un plan de protección que mantiene 960 puntos de recuperación para los datos de aplicación de dicho grupo de protección tras los 10 primeros días de protección de los datos.

Consulte también

Objetivos de recuperación de la protección basada en cinta

Objetivos de recuperación de la protección basada en cinta

DPM protege datos en cinta a través de una combinación de copias de seguridad completas e incrementales a partir del origen de datos protegidos (para una protección en cinta a corto plazo o una protección en cinta a largo plazo cuando DPM no protege los datos en disco) o bien a partir de la réplica de DPM (para una protección en cinta a largo plazo cuando la protección a corto plazo se realiza en disco).

Las opciones de intervalo de retención, frecuencia de las copias de seguridad y opciones de recuperación son diferentes para la protección a corto y a largo plazo.

Nota

Puede seleccionar protección a corto plazo en disco o cinta, pero no ambas.

Protección en cinta a corto plazo

Para la protección en cinta a corto plazo, puede seleccionar un intervalo de retención de 1 a 12 semanas. DPM permite administrar las cintas a través de alertas e informes y utiliza el intervalo de retención especificado para establecer la fecha de caducidad de cada cinta.

Las opciones para la frecuencia de la copia de seguridad son diaria, semanal o quincenal, dependiendo del intervalo de retención.

Si selecciona la protección en cinta a corto plazo mediante copias de seguridad incrementales y completas, el intervalo de retención será mayor que el especificado (un máximo de 1 semana más largo) debido a la dependencia existente entre las copias de seguridad completas e incrementales. Las cintas que contienen una copia de seguridad completa se reciclan únicamente después de reciclar todas las cintas incrementales dependientes. Dado que las copias de seguridad completas se llevan a cabo una vez a la semana y las incrementales una vez al día, la cinta de la copia de seguridad completa semanal debe esperar a que se reciclen las seis cintas de copia de seguridad incremental diarias antes de reciclar la cinta de copia de seguridad completa. Si se produce un error en la copia de seguridad incremental y no hay ninguna cinta incremental, la cinta de la copia de seguridad completa se reciclará antes.

Protección en cinta a largo plazo

Para la protección en cinta a largo plazo, también conocida como archivo de cinta, puede seleccionar un intervalo de retención de entre 1 semana y 99 años. DPM permite administrar los archivos de cinta a través de alertas e informes y utiliza el intervalo de retención especificado para establecer la fecha de caducidad de cada cinta.

La frecuencia de la copia de seguridad se basa en el intervalo de retención especificado, tal como se muestra en la siguiente lista:

- Cuando el intervalo de retención es de 1 a 99 años, puede seleccionar que las copias de seguridad se lleven a cabo cada día, semana, quincena, mes, trimestre, semestre o año.
- Cuando el intervalo de retención es de 1 a 11 meses, puede seleccionar que las copias de seguridad se lleven a cabo cada día, semana, quincena o mes.
- Cuando el intervalo de retención es de 1 a 4 semanas, puede seleccionar que las copias de seguridad se lleven a cabo cada día o semana.

Consulte también

Objetivos de recuperación de la protección basada en disco

Planificación de configuraciones de protección

Una vez que haya identificado los orígenes de datos que necesita proteger y determinado los objetivos de recuperación, el siguiente paso es analizar la información recopilada de tal manera que pueda organizar los orígenes de datos en grupos de protección.

Un n*grupo de protección* es un conjunto de orígenes de datos que comparten la misma configuración de protección. La *configuración de protección* está formada por el nombre del grupo de protección y la configuración de las asignaciones en disco, del método de creación de réplica y la transmisión comprimida.

Para planificar un grupo de protección, debe tomar las siguientes decisiones:

- ¿Qué orígenes de datos formarán parte del grupo de protección?
- ¿Qué método de protección (basado en disco, basado en cinta o ambos) utilizará para el grupo de protección?
- ¿Cuáles son los objetivos de recuperación de los miembros del grupo de protección?
- ¿Cuánto espacio de almacenamiento necesitará para proteger los datos seleccionados?
- ¿Qué cinta y qué biblioteca deben utilizarse?
- ¿Qué método utilizará para crear la réplica de los miembros del grupo de protección?

Los temas de esta sección proporcionan pautas para la toma de decisiones relativas a la creación de un grupo de protección.

En esta sección

Consulte también

Selección de los miembros del grupo de protección

Data Protection Manager (DPM) 2007 ofrece varios enfoques para organizar orígenes de datos en grupos de protección, incluidos los siguientes:

- **Por ordenador**, en el que todos los orígenes de datos de un ordenador pertenecen al mismo grupo de protección.
  - Una de las ventajas de este enfoque es que, al tener todos los datos de un ordenador en el mismo grupo de protección, dispone de un único punto de ajuste para las cargas de rendimiento.
  - Una limitación de este enfoque es que deben asignarse los mismos objetivos de recuperación a todos los orígenes de datos de un tipo en dicho ordenador.
- **Por tipo de datos**, separando los archivos y cada tipo de datos de aplicación en grupos de protección diferentes.
  - Una ventaja de este enfoque es que puede administrar tipos de datos como un grupo.
  - Una limitación de este enfoque es que la recuperación de un servidor puede necesitar varias cintas de distintos grupos de protección.

Por definición, todos los miembros de un grupo de protección comparten objetivos de recuperación; es decir, todos los orígenes de datos de un tipo incluidos en un grupo de protección deben tener el mismo intervalo de retención y la misma tolerancia a la pérdida de datos.

Si tiene sólo una cinta independiente, utilice un único grupo de protección para minimizar el esfuerzo de cambiar cintas. Múltiples grupos de protección requieren una cinta individual para cada grupo.

Pautas para grupos de protección

A la hora de diseñar la estructura de los grupos de protección, tenga en cuenta las siguientes pautas y restricciones:

- Los orígenes de datos de un ordenador deben estar protegidos por el mismo servidor DPM. En DPM, un origen de datos es un volumen, un recurso compartido, una base de datos o un grupo de almacenamiento que es miembro de un grupo de protección.
- En un grupo de protección puede incluir orígenes de datos que proceden de más de un ordenador.
- Al seleccionar una carpeta o un recurso compartido principal, las subcarpetas correspondientes quedan automáticamente seleccionadas. Puede designar subcarpetas para su exclusión, así como excluir tipos de archivo por extensión.
- Asegúrese de que no tiene más de 100 orígenes de datos que puedan protegerse en un único volumen. De ser así, distribuya los orígenes de datos en más volúmenes si es posible.
- Todos los miembros del grupo de protección del mismo tipo (archivos o datos de aplicación) tendrán los mismos objetivos de recuperación. Sin embargo, dentro del mismo grupo de protección, los archivos pueden tener objetivos de recuperación diferentes de los de los datos de aplicación.

  Excepción: Si una base de datos de SQL Server está configurada para que utilice el modelo de recuperación simple o es la base de datos principal de un par de trasvase de registros, los objetivos de recuperación de dicha base de datos se configurarán independientemente de los de otros datos de aplicación.
- Todos los grupos de almacenamiento de un ordenador que ejecuta Exchange Server 2003 deben ser miembros del mismo grupo de protección.
- Si selecciona un origen de datos que contiene un punto de reanálisis sintáctico (los puntos de montaje y los puntos de unión son orígenes de datos que contienen puntos de reanálisis sintáctico), DPM le solicitará que especifique si desea incluir el destino del punto de reanálisis sintáctico en el grupo de protección. El punto de reanálisis sintáctico no se replica; debe recrear manualmente el punto de reanálisis sintáctico al recuperar los datos.

Consideraciones especiales para la protección de datos en estaciones de trabajo

Los objetivos de recuperación de datos de las estaciones de trabajo del usuario pueden diferir de los objetivos de recuperación de datos de los servidores de archivos. Debería plantearse colocar los servidores de archivos y las estaciones de trabajo en diferentes grupos de protección para que pueda ajustar las programaciones de sincronización por separado. Por ejemplo, si sincroniza datos contenidos en servidores de archivos cada 15 minutos, las estaciones de trabajo que pertenecen al mismo grupo de protección que los servidores de archivos también se sincronizarán cada 15 minutos.

Consideraciones especiales para la protección de datos en una WAN

La regulación del uso de la amplitud de banda de red y la transmisión comprimida son funciones de optimización del rendimiento que resultan especialmente importantes en implantaciones en las que un servidor DPM protege datos en una red de área amplia (WAN) u otra red lenta.

La transmisión comprimida se configura en el nivel del grupo de protección.

La regulación del uso de la amplitud de banda de red se configura en el nivel del ordenador protegido. Además, puede especificar diferentes índices de regulación del uso de la amplitud de banda para horas de trabajo, horas de no trabajo y fines de semana, así como definir los tiempos para cada una de estas categorías.

Al proteger datos de aplicación como grupos de almacenamiento de Exchange o bases de datos de SQL Server en una WAN, considere reducir la programación de copias de seguridad completas.

Importancia de la decisión de pertenencia a un grupo de protección

Los miembros de un grupo de protección no pueden moverse entre distintos grupos. Si posteriormente decide que un miembro de un grupo de protección debe estar en un grupo de protección diferente, deberá extraer el miembro de su grupo de protección y, a continuación, añadirlo a un grupo de protección diferente.

Si determina que los miembros de un grupo de protección ya no necesitan protección, puede detener la protección del grupo. Al detener la protección, puede optar por retener los datos protegidos o bien eliminarlos.

- **Opción de retención de datos protegidos**: retiene la réplica en disco con las cintas y los puntos de recuperación asociados durante el intervalo de retención especificado.
- **Opción de eliminación de datos protegidos**: elimina la réplica del disco y los datos de las cintas caducan.

Consulte también

Planificación de configuraciones de protección

Selección de un método de protección de datos

Data Protection Manager (DPM) 2007 ofrece los métodos de protección de datos siguientes: basada en disco (D2D), basada en cinta (D2T), o bien una combinación de protección basada en disco y basada en cinta (D2D2T).

El método de protección de datos se configura en el nivel del grupo de protección. Si desea utilizar diferentes métodos para proteger dos orígenes de datos, estos orígenes no pueden pertenecer al mismo grupo de protección.

En la tabla siguiente se comparan las ventajas y las desventajas de cada método.

Comparación de los métodos de protección de datos

Método	Ventajas	Desventajas	Cuándo debe utilizarse
Sólo protección basada en disco	• Rapidez de la recuperación de datos. • Rapidez de la copia de seguridad de datos. • Menor probabilidad de que se produzcan errores en las copias de seguridad. • Capacidad para tener redundancia a la hora de gestionar errores mediante tecnologías como RAID. • Menor intervención manual, como cambios de cintas.	• Los discos no representan una solución sencilla para las necesidades de almacenamiento debido al coste de los discos y a la incomodidad de externalizar el almacenamiento.	• Cuando disponga de una tolerancia a la pérdida de datos limitada. • Cuando necesite tiempos de recuperación más rápidos.

Método	Ventajas	Desventajas	Cuándo debe utilizarse
Sólo protección basada en cinta	• Posibilidad de almacenamiento en una ubicación externa como medida de seguridad y para casos de recuperación de desastres. • Sencillo aumento de la capacidad mediante la incorporación de más cintas.	• Proceso de recuperación más lento y pesado. • Proclive a errores.	• Cuando la tolerancia a la pérdida de datos sea más generosa. • Cuando el tiempo de recuperación objetivo sea generoso. • Para datos que no cambian con frecuencia y que no necesitan una copia de seguridad con tanta asiduidad. • Para un periodo de retención prolongado.
Protección basada en disco y basada en cinta	• Combinación de las ventajas mencionadas anteriormente y compensación de las desventajas de cada método. • Un único punto de administración.		

Consulte también

Planificación de configuraciones de protección

Definición de los objetivos de recuperación

Después de seleccionar los miembros de un grupo de protección de DPM y los métodos que se van a utilizar para la protección de datos, debe definir los objetivos de recuperación de los datos de archivo y de aplicación de dicho grupo de protección.

Los objetivos de recuperación se definen mediante la configuración del intervalo de retención, la frecuencia de sincronización y la programación de puntos de recuperación. DPM proporciona una configuración predeterminada para los objetivos de recuperación; sin embargo, se puede modificar parte o la totalidad de dicha configuración.

Al menos una sincronización debe estar programada para que tenga lugar entre puntos de recuperación programados. Por ejemplo, especifique una frecuencia de sincronización de 45 minutos. Como resultado, no puede configurar que se creen puntos de recuperación a las 13:00 y a las 13:30 ya que no interviene ninguna sincronización entre los puntos de recuperación.

Cuando un servidor SQL se configura para que utilice el modelo de recuperación simple o bien es el servidor principal en un par de trasvase de registros, los puntos de recuperación de cualquier base de datos protegida incluida en dicho servidor se crean de acuerdo con la programación de copias de seguridad completas.

En los siguientes temas de esta sección se proporciona información detallada que le servirá para planificar los objetivos de recuperación:

- Opciones de objetivos de recuperación para cada método de protección
- Programación de puntos de recuperación para la protección a largo plazo
- Opciones de programación para la protección a largo plazo
- Personalización de objetivos de recuperación para la protección a largo plazo

Consulte también

Planificación de configuraciones de protección

Opciones de objetivos de recuperación para cada método de protección

En la siguiente tabla se muestran las opciones de objetivos de recuperación para cada método de protección de DPM.

Opciones de objetivos de recuperación para métodos de protección

Método de protección	Intervalo de retención	Frecuencia de sincronización o programación de copias de seguridad	Puntos de recuperación
En disco a corto plazo	De 1 a 448 días	Seleccione una frecuencia comprendida entre 15 minutos y 24 horas, o bien seleccione **Just before a recovery point** (Sólo antes de un punto de recuperación).	Cuando se selecciona una frecuencia de sincronización específica: • Los puntos de recuperación de archivos se crean de acuerdo con la programación configurada. • Los puntos de recuperación de datos de aplicación se crean después de cada sincronización. Si se selecciona **Just before a recovery point** (Sólo antes de un punto de recuperación), los puntos de recuperación de todos los miembros del grupo de protección se crean de acuerdo con la programación especificada.

Método de protección	Intervalo de retención	Frecuencia de sincronización o programación de copias de seguridad	Puntos de recuperación
En cinta a corto plazo	De 1 a 12 semanas	Seleccione realizar una copia de seguridad: • Cada día • Cada semana • Cada dos semanas	En lugar de puntos de recuperación, configure uno de los siguientes tipos de copia de seguridad: • Copias de seguridad completas e incrementales • Sólo copia de seguridad completa Si selecciona cada semana o cada dos semanas, sólo está disponible la copia de seguridad completa. Especifique el día y la hora. Si selecciona copias de seguridad completas diarias, debe especificar la hora. Si selecciona copias de seguridad diarias completas e incrementales, debe especificar el día y la hora de la copia de seguridad completa y de la copia de seguridad incremental.
En cinta a largo plazo	Mínimo: 1 semana Máximo: 99 años	Seleccione realizar una copia de seguridad: • Cada día • Cada semana • Cada quincena • Cada mes • Cada trimestre • Cada semestre • Cada año	Consulte Programación de puntos de recuperación para la protección a largo plazo y Personalización de objetivos de recuperación para la protección a largo plazo.

Consulte también

Definición de los objetivos de recuperación

Programación de puntos de recuperación para la protección a largo plazo

En la siguiente tabla se muestra la programación de puntos de recuperación de DPM para las diferentes combinaciones de protección a largo plazo.

Programación de puntos de recuperación para la protección a largo plazo

Frecuencia de la copia de seguridad e intervalo de retención	Programación de puntos de recuperación
Cada día, de 1 a 4 semanas	Copia de seguridad completa diaria
Cada día, de 1 a 11 meses	1 copia de seguridad completa cada día durante 4 semanas 1 copia de seguridad completa cada mes después de las 4 primeras semanas
Cada día, de 1 a 99 años	1 copia de seguridad completa cada día durante 4 semanas 1 copia de seguridad completa cada mes después de las 4 primeras semanas, hasta el mes 12 1 copia de seguridad completa cada año después de los 11 primeros meses
Cada semana, de 1 a 4 semanas	Copia de seguridad completa semanal
Cada semana, de 1 a 11 meses	1 copia de seguridad completa cada semana durante 4 semanas 1 copia de seguridad completa cada mes después de las 4 primeras semanas
Cada semana, de 1 a 99 años	1 copia de seguridad completa cada semana durante 4 semanas 1 copia de seguridad completa cada mes después de las 4 primeras semanas, hasta el mes 12 1 copia de seguridad completa cada año después de los 11 primeros meses

Frecuencia de la copia de seguridad e intervalo de retención	Programación de puntos de recuperación
Cada quincena, de 1 a 11 meses	1 copia de seguridad completa cada 2 semanas durante 4 semanas 1 copia de seguridad completa cada mes después de las 4 primeras semanas
Cada quincena, de 1 a 99 años	1 copia de seguridad completa cada 2 semanas durante 4 semanas 1 copia de seguridad completa cada mes después de las 4 primeras semanas, hasta el mes 12 1 copia de seguridad completa cada año después de los 11 primeros meses
Cada mes, de 1 a 11 meses	Copia de seguridad completa mensual
Cada mes, de 1 a 99 años	1 copia de seguridad completa cada mes, hasta el mes 12 1 copia de seguridad completa cada año después de los 11 primeros meses
Cada trimestre, de 1 a 99 años	1 copia de seguridad completa cada 3 meses, hasta el mes 12 1 copia de seguridad completa cada año después de los 11 primeros meses
Cada semestre, de 1 a 99 años	1 copia de seguridad completa cada 6 meses, hasta el mes 12 1 copia de seguridad completa cada año después de los 11 primeros meses
Cada año, de 1 a 99 años	Copia de seguridad completa anual

Consulte también

Definición de los objetivos de recuperación

Opciones de programación para la protección a largo plazo

En la tabla siguiente se muestran las opciones de programación que puede modificar para la protección a largo plazo con DPM.

Opciones de programación para la protección a largo plazo

Para esta frecuencia de copia de seguridad	Dependiendo del intervalo de retención, puede configurar
Cada día	• La hora de la copia de seguridad diaria • El día específico o el día de la semana y la hora de la copia de seguridad mensual • El día específico o la fecha y la hora de la copia de seguridad anual
Cada semana	• La hora y el día de la semana de la copia de seguridad semanal • El día específico o el día de la semana y la hora de la copia de seguridad mensual • El día específico o la fecha y la hora de la copia de seguridad anual
Cada quincena	• La hora y el día de la semana de la copia de seguridad quincenal • El día específico o el día de la semana y la hora de la copia de seguridad mensual • El día específico o la fecha y la hora de la copia de seguridad anual
Cada mes	• El día específico o el día de la semana y la hora de la copia de seguridad mensual • El día específico o la fecha y la hora de la copia de seguridad anual
Cada trimestre	• La hora y la fecha de la copia de seguridad trimestral; las copias de seguridad trimestrales se llevan a cabo en enero, abril, julio y octubre, el día especificado del mes. • El día específico o la fecha y la hora de la copia de seguridad anual

Para esta frecuencia de copia de seguridad	Dependiendo del intervalo de retención, puede configurar
Cada semestre	• La hora, el día específico o la fecha y los meses de la copia de seguridad semestral • El día específico o la fecha y la hora de la copia de seguridad anual
Cada año	• El día específico o la fecha y la hora de la copia de seguridad anual

Consulte también

Definición de los objetivos de recuperación

Personalización de objetivos de recuperación para la protección a largo plazo

Cuando especifica un intervalo de retención y una frecuencia de la copia de seguridad, DPM genera una programación de trabajos de copia de seguridad. Para obtener más información, consulte Programación de puntos de recuperación para la protección a largo plazo. También puede personalizar la programación de trabajos de copia de seguridad según sus objetivos de recuperación con el fin de sustituir la programación predeterminada.

Si personaliza la programación de trabajos de copia de seguridad de un grupo de protección, debe especificar un objetivo de recuperación para cada intervalo de copia de seguridad. Las opciones de intervalos de frecuencia de la copia de seguridad son los siguientes:

- Cada día
- Cada semana
- Cada mes
- Cada año

Puede especificar un objetivo de recuperación para un máximo de tres intervalos de frecuencia de copia de seguridad. Para cada intervalo de frecuencia de la copia de seguridad, debe especificar el intervalo de retención de la cinta, el número de copias que deben realizarse de la cinta y la etiqueta de la cinta.

Por ejemplo, al personalizar los objetivos de recuperación de un grupo de protección, podría configurar que las copias de seguridad se llevaran a cabo de acuerdo con la siguiente programación:

- Una copia de las copias de seguridad semanales, retenida durante dos semanas
- Dos copias de las copias de seguridad mensuales, retenidas durante seis meses
- Una copia de la copia de seguridad anual, retenida durante cinco años

Consulte también

Planificación de configuraciones de protección

Asignación de espacio para grupos de protección

Cuando cree un grupo de protección y seleccione la protección basada en disco, debe asignar espacio en el bloque de almacenamiento para las réplicas y los puntos de recuperación de cada origen de datos que haya seleccionado para que formen parte del grupo; también debe asignar espacio en estaciones de trabajo o servidores de archivos protegidos para el diario de cambios.

DPM proporciona asignaciones de espacio predeterminadas para los miembros del grupo de protección. En la tabla siguiente se muestra cómo DPM calcula las asignaciones predeterminadas.

Cómo DPM calcula las asignaciones de espacio predeterminadas

Componente	Asignación predeterminada	Ubicación
Volumen de réplicas	Para archivos: • (Tamaño del origen de datos x 3) / 2 Para datos de Exchange: • Tamaño del origen de datos x (1 + cambio de registro) / (umbral de alerta - ,05) Para datos de SQL Server: • Tamaño del origen de datos x (1 + cambio de registro) / (umbral de alerta - ,05) Para datos de Windows SharePoint Services: • Tamaño total de todas las bases de datos / (umbral de alerta - ,05) Para datos de Virtual Server: • Tamaño del origen de datos x 1,5 Para el estado del sistema: • (Tamaño del origen de datos x 3) / 2	Bloque de almacenamiento de DPM o volumen personalizado

Componente	Asignación predeterminada	Ubicación
Volumen de puntos de recuperación	Para archivos: • (Tamaño del origen de datos x intervalo de retención en días x 2) / 100 + 1 600 MB Para datos de Exchange: • 4,0 x intervalo de retención en días x cambio de registro x tamaño del origen de datos + 1 600 MB Para datos de SQL Server: • 2,5 x intervalo de retención en días x cambio de registro x tamaño del origen de datos + 1 600 MB Para datos de Windows SharePoint Services: • 1,5 x intervalo de retención en días x cambio de registro x tamaño total de todas las bases de datos + 1 600 MB Para datos de Virtual Server: • (Tamaño del origen de datos x intervalo de retención en días x 0,02) + 1 600 MB Para el estado del sistema: • (Tamaño del origen de datos x intervalo de retención en días x 2) / 100 + 1 600 MB	Bloque de almacenamiento de DPM o volumen personalizado
Diario de cambios (sólo para protección de archivos)	300 MB	Volumen protegido en el servidor de archivos o la estación de trabajo

Los valores utilizados en la tabla anterior se definen de la siguiente manera:

- **% de alerta:** se trata de un umbral de alerta asociado al aumento de réplicas, normalmente del 90%.
- **Cambio de registro:** se trata de la frecuencia de cambio de la base de datos o del grupo de almacenamiento en cuestión. Este valor varía mucho, pero a efectos de la recomendación predeterminada de DPM, se supone que es de un 6% para datos de Exchange y SQL Server y un 10% para datos de Windows SharePoint Services.
- **Intervalo de retención:** se trata del número de puntos de recuperación almacenados; se supone que es 5 a efectos de la recomendación predeterminada de DPM.
- **Tamaño del origen de datos del estado del sistema:** se supone que el tamaño del origen de datos es 1 GB.

Al crear un grupo de protección, en el cuadro de diálogo **Modify Disk Allocation** (Modificar asignación de disco), la columna **Data Size** (Tamaño de datos) muestra un enlace **Calculate** (Calcular) para cada origen de datos. Para la asignación inicial de espacio, DPM aplica las fórmulas predeterminadas al tamaño del volumen en el que está ubicado el origen de datos. Para aplicar la fórmula al tamaño real del origen de datos seleccionado, haga clic en el enlace **Calculate** (Calcular). DPM determinará el tamaño del origen de datos y volverá a calcular la asignación en disco para el punto de recuperación y los volúmenes de réplica de ese origen de datos. Esta operación puede tardar varios minutos en completarse.

Se recomienda aceptar las asignaciones de espacio predeterminadas a no ser que esté seguro de que no le sirven para sus propósitos. La sustitución de las asignaciones predeterminadas puede dar lugar a la asignación de muy poco o demasiado espacio.

La asignación de muy poco espacio para los puntos de recuperación puede impedir que DPM almacene suficientes puntos de recuperación para satisfacer los objetivos de intervalo de retención. Por otra parte, la asignación de demasiado espacio desaprovecha la capacidad del disco.

Si, después de haber creado un grupo de protección, descubre que ha asignado muy poco espacio a uno de los orígenes de datos de dicho grupo, puede aumentar las asignaciones para los volúmenes de réplica y de punto de recuperación de cada origen de datos.

Asimismo, si descubre que ha asignado demasiado espacio al grupo de protección, la única manera de reducir las asignaciones para un origen de datos es eliminar el origen de datos del grupo de protección, eliminar la réplica y, a continuación, volver a añadir el origen de datos al grupo de protección con asignaciones más pequeñas.

Para ayudarle a realizar una estimación del espacio de almacenamiento que necesita, descargue la calculadora de almacenamiento de DPM (http://go.microsoft.com/fwlink/?LinkId=104370).

Consulte también

Planificación de configuraciones de protección

Especificación de detalles de cinta y biblioteca

Si selecciona la protección basada en cinta, debe especificar el número de copias que DPM debe crear de cada cinta, así como las opciones de configuración de las cintas de copia de seguridad. Puede elegir una de las opciones siguientes:

- **Compress data (Comprimir datos)**

  Si selecciona esta opción, DPM comprime los datos que se escriben en la cinta, lo que reduce el espacio necesario en la cinta y aumenta el número de trabajos de copia de seguridad que se pueden almacenar en la misma cinta. La compresión no aumenta de forma significativa el tiempo necesario para completar el trabajo de copia de seguridad. La velocidad de compresión varía según el tipo de datos.

- **Encrypt data (Cifrar datos)**

  Si selecciona esta opción, DPM cifra los datos que se escriben en la cinta, lo que aumenta la seguridad de los datos archivados. El cifrado no aumenta de forma significativa el tiempo necesario para completar el trabajo de copia de seguridad.

  Nota

  Para activar el cifrado, debe haber un certificado de cifrado válido en el servidor DPM. Para obtener instrucciones, consulte "How to Encrypt Data in a Protection Group" (Cómo cifrar los datos de un grupo de protección) en la ayuda de DPM.

Consulte también

Planificación de configuraciones de protección

Selección de un método de creación de réplicas

Al crear un grupo de protección, debe seleccionar un método para crear las réplicas de los volúmenes incluidos en el grupo. La creación de réplicas consiste en copiar todos los datos seleccionados para la protección en el servidor DPM y, a continuación, ejecutar la sincronización con comprobación de coherencia en cada una de las réplicas.

DPM puede crear las réplicas automáticamente a través de la red o bien se pueden crear manualmente mediante la restauración de los datos a partir de soportes multimedia extraíbles, como una cinta. La creación automática de réplicas es un proceso más fácil; no obstante, en función del tamaño de los datos protegidos y de la velocidad de la red, es posible que la creación manual sea más rápida.

Para ayudarle a seleccionar el método de creación de réplicas más adecuado, en la siguiente tabla se proporciona una estimación del tiempo que tarda DPM en crear una réplica automáticamente a través de la red según el tamaño de los datos protegidos y la velocidad de la red. En esta estimación se presupone que la red funciona a velocidad completa y que las demás cargas de trabajo no afectan a la amplitud de banda. Los tiempos se muestran en horas.

Horas en completar la creación automática de réplicas a diferentes velocidades de red

Tamaño de los datos protegidos	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	1 137	284	71	18	6
500 GB	2 844	711	178	45	15

Importante

Si va a implantar DPM para proteger los datos a través de una WAN y el grupo de protección incluye más de 5 GB de datos, se recomienda seleccionar el método manual para crear las réplicas.

Creación automática de réplicas

En trabajos de creación de réplicas de gran envergadura, podría programar el trabajo para que se ejecutara únicamente durante periodos de poco tráfico en la red.

Creación manual de réplicas

Si selecciona la creación manual de réplicas, DPM especifica las ubicaciones exactas en el servidor DPM en las que debe crear las réplicas. Normalmente, las réplicas se crean mediante la restauración de la copia de seguridad más reciente del origen de datos desde el soporte multimedia extraíble, como por ejemplo una cinta. Después de restaurar los datos, el proceso se completa con la ejecución de la sincronización con comprobación de coherencia de cada réplica.

Al restaurar los datos en el servidor DPM para crear la réplica, es fundamental que conserve la estructura de directorio y las propiedades originales del origen de datos, como las marcas de tiempo y los permisos de seguridad. Cuantas más discrepancias existan entre las réplicas y el origen de datos protegidos, más tiempo tarda la parte de comprobación de coherencia del proceso. Si no conserva la estructura de directorio y las propiedades originales, la creación manual de réplicas puede tardar tanto como la automática.

Consulte también

Planificación de configuraciones de protección

Planificación de la implantación de DPM

A la hora de crear el plan de implantación de Microsoft System Center Data Protection Manager (DPM) 2007, deberá planificar en primer lugar los grupos de protección, dado que las necesidades de dichos grupos (tamaño, velocidad de cambio de datos, ubicación, objetivos de recuperación) serán la base para la toma de decisiones con respecto a la creación y ubicación de los servidores y las bibliotecas de cintas de DPM.

Una vez planificados los grupos de protección, puede completar el plan de implantación determinando las configuraciones de los servidores DMP necesarias para proteger los datos de la manera más eficiente posible. En los temas de esta sección se incluyen consideraciones sobre la seguridad y la administración que podrían afectar al plan de implantación.

En esta sección

Planificación de las configuraciones del servidor DPM

Consideraciones sobre la recuperación por el usuario final

Consideraciones sobre seguridad

Consulte también

Planificación de grupos de protección

Planificación de las configuraciones del servidor DPM

En el plan de implantación se debe especificar el número de servidores DPM necesarios para proteger los datos, así como la ubicación de cada servidor DPM en la red.

Asimismo, se debe especificar la instancia de Microsoft SQL Server que usará cada servidor DPM. DPM requiere una instancia de SQL Server para las bases de datos de DPM y de informes. DPM instalará SQL Server durante la instalación en el servidor DPM, pero también puede usar una instancia existente de SQL Server en un ordenador remoto.

Uno de los componentes críticos de la configuración del servidor DPM es el *bloque de almacenamiento*, un conjunto de discos que almacenan réplicas y puntos de recuperación para los datos protegidos. La capacidad del bloque de almacenamiento y de los volúmenes personalizados que asigne al DPM debe ser suficiente para proporcionar protección basada en disco de los orígenes de datos seleccionados.

Si el plan de implantación requiere protección basada en cinta de los orígenes de datos, tendrá que conectar una biblioteca de cintas o una unidad de cinta independiente al servidor DPM.

Si va a proteger un conjunto de Windows SharePoint Services de gran tamaño, deberá instalar DPM en un volumen que disponga de espacio en disco suficiente para la base de datos de DPM. La base de datos de DPM requiere aproximadamente 1 GB por cada millón de elementos que existan en el conjunto. Por ejemplo, si protege un conjunto de 5 millones de elementos, planificaría unos 5 GB de almacenamiento en la base de datos de DPM para mantener el catálogo de dicho conjunto. Este requisito de espacio se suma al espacio de almacenamiento que requiere DPM para los catálogos de copia de seguridad en cinta, los registros de trabajos, etc.

En esta sección

Consulte también

Selección del número de servidores DPM

Cuando considere el número de servidores DMP que necesita su empresa, tenga en cuenta que no existe una fórmula exacta para determinarlo. En la práctica, el número de servidores y la cantidad de datos que puede proteger un solo servidor DPM variará según los factores siguientes:

- La velocidad de cambio de los orígenes de datos que se van a proteger
- La cantidad de espacio disponible en el bloque de almacenamiento
- La frecuencia con que se sincronizan los datos
- La amplitud de banda disponible en cada ordenador protegido
- La amplitud de banda agregada al servidor DPM

Para obtener una estimación de la velocidad de cambio de los datos, puede examinar una copia de seguridad incremental de un día promedio reciente. El porcentaje de los datos incluidos en una copia de seguridad incremental suele ser indicativo de la velocidad de cambio de los datos. Por ejemplo, si tiene un total de 100 GB de datos y la copia incremental incluye 10 GB, es probable que la velocidad de cambio de los datos sea del 10 por ciento aproximadamente cada día.

No obstante, como el método que utiliza DPM para registrar los cambios en los datos es diferente al de la mayoría del software de copia de seguridad, el tamaño de la copia de seguridad incremental no siempre es un indicador preciso de la velocidad de cambio de los datos. Para obtener una estimación más precisa de la velocidad de cambio de los datos, tenga en cuenta las características de los datos que desea proteger.

Por ejemplo, mientras que la mayoría de los datos de los registros de software de copia de seguridad cambian a nivel de archivo, los registros de DPM cambian a nivel de byte. Esto se puede traducir en una velocidad de cambio de los datos inferior a la que podría sugerir la copia de seguridad incremental, según el tipo de datos que desee proteger.

En la siguiente tabla se muestran los límites de origen de datos que un servidor DPM que satisface los requisitos mínimos de hardware puede proteger, así como el espacio en disco recomendado necesario para cada servidor DPM.

Plataforma	Límite de origen de datos	Espacio en disco recomendado
Ordenadores de 32 bits	150 orígenes de datos. Se recomienda entre unos 30 y 40 servidores que dependan de un solo servidor DPM.	10 TB **Nota** En los sistemas operativos x86 de 32 bits, existe una limitación del bloque no paginado del servicio de cópia simultánea de volumen (VSS). Si va a proteger los datos mediante un servidor DPM secundario, el espacio en disco recomendado es de sólo 6 TB.
Ordenadores de 64 bits	300 orígenes de datos. Los orígenes de datos se distribuyen normalmente entre 50 y 75 servidores físicos.	40 TB

Límite de instantáneas

Un servidor DPM puede almacenar hasta 9.000 instantáneas basadas en disco, incluidas las que se retienen cuando se detiene la protección de un origen de datos. El límite de instantáneas se aplica a copias de seguridad completas y puntos de recuperación de archivos, pero no a sincronizaciones incrementales.

El límite de instantáneas se aplica por servidor DPM, independientemente del tamaño del bloque de almacenamiento. Al configurar grupos de protección, se prevé el servidor DPM para el número de instantáneas con el fin de acomodar la configuración del grupo de protección. Puede utilizar el siguiente cmdlet del shell de DPM Management para identificar el número de instantáneas que se prevé para el servidor:

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

A la hora de planificar la implantación de DPM, es necesario tener en cuenta el límite de instantáneas como parte de la capacidad del servidor DPM. En la siguiente tabla se muestran ejemplos del número de instantáneas generadas según las diferentes políticas de protección.

Política de protección	Instantáneas
Grupo de almacenamiento de Exchange: copia de seguridad completa diaria y sincronización incremental de 15 minutos con un intervalo de retención de 5 días	5
Volumen en un servidor de archivos: 3 puntos de recuperación diarios con un intervalo de retención de 21 días	63
Base de datos de SQL: 2 copias de seguridad completas diarias con un intervalo de retención de 14 días	28
Total:	**96**

Consulte también

Planificación de las configuraciones del servidor DPM

Ubicación de los servidores DPM

DPM requiere una estructura de servicios de directorio de Servicios de dominio de Active Directory de Windows Server 2003 para respaldar sus operaciones de protección y recuperación.

DPM puede proteger los servidores y las estaciones de trabajo que estén ubicados en el mismo dominio que el servidor DPM o en uno que tenga una relación de confianza bidireccional con el dominio en el que está ubicado el servidor DPM.

A la hora de decidir dónde ubicar el servidor DPM, tenga en cuenta la amplitud de banda de red entre dicho servidor y los ordenadores protegidos.

DPM admite tarjetas de interfaz de red (NIC) agrupadas. Las tarjetas NIC agrupadas son varias tarjetas NIC físicas que están configuradas para que el sistema operativo las trate como una sola tarjeta. Las tarjetas NIC agrupadas proporcionan una mayor amplitud de banda al combinar la amplitud de banda disponible que utiliza cada tarjeta y la sustitución tras error por la que cuando una NIC falla se pasa al resto de NIC. DPM puede utilizar la mayor amplitud de banda conseguida con el uso de tarjetas NIC agrupadas en el servidor DPM.

Otro aspecto a tener en cuenta con respecto a la ubicación de los servidores DPM es la necesidad de administrar cintas y bibliotecas de cintas manualmente, lo que incluye actividades como añadir nuevas cintas a la biblioteca o eliminar cintas del archivo externo.

Consulte también

Planificación de las configuraciones del servidor DPM

Selección de la instancia de SQL Server

Una instalación típica de DPM incluye una instancia de SQL Server instalada por el programa de configuración de DPM. Dicha instancia se incluye en el software de DPM y no requiere el uso de otra licencia de SQL Server.

No obstante, al instalar DPM 2007, puede especificar que DPM utilice una instancia remota de SQL Server en lugar de la predeterminada que se incluye con DPM.

Para utilizar una instancia remota de SQL Server, el servidor que ejecuta SQL Server y el servidor DPM deben estar ubicados en el mismo dominio. Sólo un servidor DPM puede utilizar una instancia específica de SQL Server. La instancia remota de SQL Server no puede estar en un ordenador que se ejecute como controladora de dominio.

Nota

Si la instancia remota de SQL Server se ejecuta como una cuenta de dominio, debe activar el protocolo de canalizaciones con nombre para permitir la comunicación con el servidor DPM. Para obtener instrucciones sobre cómo configurar el protocolo de canalizaciones con nombre, consulte Configuring Client Network Protocols (Configuración de los protocolos de red de cliente) en http://go.microsoft.com/fwlink/?LinkId=87976.

La instancia remota de SQL Server debe ejecutar los Servicios de Internet Information Server (IIS) y SQL Server 2005 Standard o Enterprise Edition con SP2, incluidos los componentes siguientes:

- SQL Server Database Engine
- Reporting Services

Se recomienda utilizar la siguiente configuración en la instancia remota de SQL Server:

- Utilice el valor predeterminado en la auditoría de errores.
- Utilice el modo de autenticación predeterminado de Windows.
- Asigne una contraseña segura a la cuenta sa.
- Active la comprobación de directiva de contraseñas.
- Instale sólo los componentes SQL Server Database Engine y Reporting Services.
- Una instancia remota de SQL Server no se debe ejecutar como sistema local.
- Ejecute SQL Server con una cuenta de usuario de dominio con pocos privilegios.

Consulte también

Planificación de las configuraciones del servidor DPM

Planificación del bloque de almacenamiento

El bloque de almacenamiento es un conjunto de discos en el que el servidor DPM almacena las réplicas y los puntos de recuperación de los datos protegidos. Planificar el bloque de almacenamiento supone calcular los requisitos de capacidad y diseñar la configuración de los discos.

También se pueden sustituir los volúmenes personalizados definidos en Administración de discos por volúmenes del bloque de almacenamiento.

DPM puede utilizar cualquiera de estos elementos para el bloque de almacenamiento:

- Almacenamiento de conexión directa (DAS)
- Red de área de almacenamiento (SAN) Fibre Channel
- Dispositivo de almacenamiento iSCSI o SAN

El bloque de almacenamiento admite la mayoría de tipos de discos, como electrónica de unidad integrada (IDE), dispositivo conector de tecnología avanzada serie (SATA) y SCSI, así como los estilos de partición de registro maestro de inicio (MBR) y tabla de particiones GUID (GPT).

Si utiliza una SAN para el bloque de almacenamiento, se recomienda crear una zona aparte para el disco y la cinta utilizados en DPM. No mezcle los dispositivos en una sola zona.

No se pueden añadir discos USB/1394 al bloque de almacenamiento DPM.

Se recomienda utilizar discos con una capacidad que no sea superior a 1,5 terabytes. Dado que un volumen dinámico puede abarcar hasta 32 discos, si utiliza discos de 1,5 terabytes, DPM puede crear volúmenes de réplica de hasta 48 terabytes.

Importante

Algunos fabricantes de equipos originales (OEM) incluyen una partición de diagnóstico que se instala con el soporte multimedia que facilitan. La partición de diagnóstico se puede denominar también partición OEM o partición EISA. Las particiones EISA deben eliminarse de los discos antes de poder añadirlos al bloque de almacenamiento DPM.

En esta sección

Cálculo de los requisitos de capacidad

Planificación de la configuración del disco

Definición de volúmenes personalizados

Consulte también

Planificación de las configuraciones del servidor DPM

Cálculo de los requisitos de capacidad

Los requisitos de capacidad del bloque de almacenamiento DPM son variables y dependen principalmente del tamaño de los datos protegidos, del tamaño del punto de recuperación diario, de la velocidad de crecimiento esperado de los datos del volumen y de los objetivos del intervalo de retención.

El tamaño del punto de recuperación diario hace referencia al tamaño total de los cambios realizados en los datos de protección durante un día. Es más o menos equivalente al tamaño de una copia de seguridad incremental. El intervalo de retención hace referencia al número de días que desea almacenar los puntos de recuperación de los datos protegidos en el disco. En el caso de archivos, DPM puede almacenar un máximo de 64 puntos de recuperación para cada volumen incluido en un grupo de protección y puede crear hasta 8 puntos de recuperación programados cada día para cada grupo de protección.

Nota

El límite de 64 puntos de recuperación para archivos es el resultado de las limitaciones del servicio de copia simultánea de volumen (VSS), que es necesario para la función de recuperación por el usuario final de DPM. El límite de puntos de recuperación no se aplica a los datos de aplicaciones.

En general, para la protección de los archivos, se recomienda crear un bloque de almacenamiento que tenga dos veces el tamaño de los datos protegidos. Esta recomendación se basa en un tamaño de punto de recuperación diario que equivale aproximadamente al 10 por ciento del tamaño de los datos protegidos y a un intervalo de retención de 10 días (dos semanas, sin contar los fines de semana).

Si el tamaño del punto de recuperación diario es superior o inferior al 10 por ciento del tamaño de los datos protegidos o los objetivos de intervalo de retención son más largos o más cortos de 10 días, puede ajustar los requisitos de capacidad de su bloque de almacenamiento según corresponda.

Independientemente de la capacidad que decida asignar al bloque de almacenamiento en su implantación inicial, se recomienda utilizar hardware ampliable para que tenga la opción de añadir capacidad en caso necesario.

En las secciones siguientes se proporcionan pautas para determinar el tamaño del punto de recuperación diario y los objetivos del intervalo de retención.

Estimación del tamaño del punto de recuperación diario

Nuestra recomendación de crear un bloque de almacenamiento con un tamaño dos veces superior al de los datos protegidos presupone un tamaño del punto de recuperación diario del 10 por ciento del tamaño de los datos protegidos. El tamaño del punto de recuperación diario está relacionado con la velocidad de cambio de los datos y hace referencia al tamaño total de todos los puntos de recuperación creados en un solo día. Para obtener una estimación del tamaño del punto de recuperación diario para los datos protegidos, puede examinar una copia de seguridad incremental de un día promedio reciente. El tamaño de la copia de seguridad incremental suele ser indicativo del tamaño del punto de recuperación diario. Por ejemplo, si la copia de seguridad incremental de 100 GB de datos incluye 10 GB de datos, el tamaño del punto de recuperación diario será aproximadamente de 10 GB.

Determinación de los objetivos del intervalo de retención

Nuestra recomendación de crear un bloque de almacenamiento con un tamaño dos veces superior al de los datos protegidos presupone un objetivo del intervalo de retención de 10 días (dos semanas, sin contar los fines de semana). A nivel de empresa, las peticiones de recuperación de datos se concentran por lo general entre las dos y las cuatro semanas posteriores a la pérdida de datos. Un intervalo de retención de 10 días proporciona recuperación de los datos hasta dos semanas después de un caso de pérdida de datos.

Cuanto más largo sea el objetivo del intervalo de retención, menos puntos de recuperación podrá crear cada día. Por ejemplo, si el objetivo del intervalo de retención es de 64 días, sólo puede crear un punto de recuperación cada día. Si el objetivo del intervalo de retención es de ocho días, puede crear ocho puntos de recuperación cada día. Con un objetivo de intervalo de retención de 10 días, puede crear aproximadamente seis puntos de recuperación cada día.

Consulte también

Definición de volúmenes personalizados

Planificación de la configuración del disco

Planificación de las configuraciones del servidor DPM

Planificación de la configuración del disco

Si para el bloque de almacenamiento DPM utiliza almacenamiento de conexión directa, puede utilizar cualquier configuración de hardware de matriz redundante de discos independientes (RAID) o bien una configuración de concatenación de discos (JBOD). No cree una configuración RAID basada en software en discos que vaya a añadir al bloque de almacenamiento.

Para decidir la configuración de los discos, tenga en cuenta la importancia relativa de la capacidad, el coste, la fiabilidad y el rendimiento en su entorno. Por ejemplo, como JBOD no consume espacio en disco para el almacenamiento de datos de paridad, una configuración de este tipo utiliza al máximo la capacidad de almacenamiento. Por este motivo, las configuraciones JBOD no tienen mucha fiabilidad; el error de un solo disco dará lugar a la pérdida inevitable de los datos.

En la implantación típica de DPM, una configuración RAID 5 ofrece un compromiso efectivo entre capacidad, coste, fiabilidad y rendimiento. Sin embargo, como la carga de trabajo del servidor DPM está formada principalmente por operaciones de escritura, es probable que RAID 5 reduzca el rendimiento de un servidor DPM de forma más marcada que en el caso de un servidor de archivos. Esta disminución del rendimiento puede afectar a su vez a la escalabilidad de DPM. La capacidad de DPM para proteger los datos de manera efectiva disminuye conforme se reduce el rendimiento.

La tabla siguiente sirve de ayuda para evaluar las opciones de configuración de los discos del bloque de almacenamiento. En ella se comparan las ventajas y desventajas de JBOD y los diversos niveles de RAID, en una escala del 4 (muy bueno) al 1 (aceptable).

Comparación de opciones de configuración para discos del bloque de almacenamiento

Configuración de disco	Capacidad	Coste	Fiabilidad	Rendimiento y escalabilidad
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

Para obtener más información sobre RAID, consulte Achieving Fault Tolerance by Using RAID (Obtención de tolerancia a errores mediante RAID) en http://go.microsoft.com/fwlink/?LinkId=46086.

Consulte también

Cálculo de los requisitos de capacidad

Definición de volúmenes personalizados

Planificación de las configuraciones del servidor DPM

Definición de volúmenes personalizados

En DPM 2007, puede asignar un *volumen personalizado* a un miembro del grupo de protección en lugar de al bloque de almacenamiento DPM. Un volumen personalizado es un volumen que no está en el bloque de almacenamiento DPM y que se especifica para almacenar la réplica y los puntos de recuperación de un miembro del grupo de protección.

Aunque el bloque de almacenamiento administrado por DPM es suficiente para satisfacer la mayoría de las necesidades empresariales, es posible que desee ejercer un mayor control sobre el almacenamiento en determinados orígenes de datos. Por ejemplo, tiene datos críticos que desea almacenar mediante un número de unidad lógica (LUN) de alto rendimiento en una red de área de almacenamiento.

Cualquier volumen conectado al servidor DPM se puede seleccionar como volumen personalizado en el asistente para la creación de un nuevo grupo de protección, a excepción del volumen que contiene los archivos de programa y del sistema. Para utilizar volúmenes personalizados para un miembro del grupo de protección, deben estar disponibles dos volúmenes personalizados: uno para almacenar la réplica y otro para almacenar los puntos de recuperación.

DPM no puede administrar el espacio de los volúmenes personalizados. Si DPM le avisa de que un volumen de réplica o de punto de recuperación personalizado se está quedando sin espacio, deberá cambiar manualmente el tamaño del volumen personalizado mediante Disk Management (Administración de discos).

Una vez que haya creado el grupo, no se puede cambiar la selección del bloque de almacenamiento o del volumen personalizado de un miembro del grupo de protección. Si tiene que cambiar la ubicación de almacenamiento de la réplica o de los puntos de recuperación de un origen de datos, la única forma de hacerlo es eliminar el origen de datos de la protección y, a continuación, añadirlo a un grupo de protección como nuevo miembro del grupo.

Consulte también

Cálculo de los requisitos de capacidad

Planificación de la configuración del disco

Planificación de las configuraciones del servidor DPM

Planificación de la configuración de bibliotecas de cintas

Puede añadir bibliotecas de cintas y unidades de cinta independientes a DPM de forma que sea posible la protección a corto y a largo plazo de los datos en una cinta. Las bibliotecas de cintas y las unidades de cinta independientes deben estar físicamente conectadas al servidor DPM.

Nota

El término *bibliotecas de cintas* hace referencia al hardware de cinta multiunidad y a las unidades de cinta independientes.

A la hora de planificar la capacidad de la biblioteca de cintas, tenga en cuenta el número de trabajos de copia de seguridad en cinta y el tamaño de los datos protegidos. Además, deberá tener en cuenta las características del hardware: una biblioteca de cintas sin cargador automático requiere giros de cinta manuales durante la ejecución de los trabajos.

Para planificar el número de cintas que va a necesitar para cada grupo de protección, deberá multiplicar la frecuencia de copia de seguridad por el intervalo de retención.

Las etiquetas de las cintas utilizadas para la protección a largo plazo se asignan cuando se crea un grupo de protección. DPM asigna una etiqueta de cinta predeterminada con este formato: **DPM - <NombreGrupoProtección> - long-term tape <número>**. Antes de comenzar a crear grupos de protección, deberá planificar el esquema de denominación de las cintas si no desea utilizar el esquema predeterminado.

Para obtener más información, consulte Managing Tape Libraries (Administración de bibliotecas de cintas) en http://go.microsoft.com/fwlink/?LinkId=91964.

Consulte también

Planificación de las configuraciones del servidor DPM

Consideraciones sobre la recuperación por el usuario final

En el plan de implantación deben especificarse los datos para los que se va a activar la recuperación por el usuario final, así como los servidores DPM que se deben configurar en los servicios de dominio de Active Directory para proporcionar la recuperación por el usuario final.

La recuperación por el usuario final permite a los usuarios finales recuperar datos de forma independiente al recuperar versiones anteriores de sus archivos. Los usuarios finales pueden recuperar versiones anteriores mediante recursos compartidos en los servidores de archivos, espacios de nombres DFS o mediante un comando del menú **Herramientas** de las aplicaciones de Microsoft Office 2003.

Si actualmente tiene activada la función de copia simultánea de carpetas compartidas en un ordenador protegido con DPM, puede desactivarla y así recuperar el espacio en disco que utiliza. Los usuarios finales y los administradores podrán recuperar archivos desde los puntos de recuperación del servidor DPM.

La activación de la recuperación por el usuario final requiere la configuración del esquema de los servicios de dominio de Active Directory, la activación de esta función en el servidor DPM y la instalación del software cliente del punto de recuperación en los ordenadores cliente.

Configuración de los servicios de dominio de Active Directory

La configuración de los servicios de dominio de Active Directory para admitir la recuperación por el usuario final implica cuatro operaciones:

1. Extensión del esquema
2. Creación de un contenedor
3. Concesión de permisos al servidor DMP para cambiar el contenido del contenedor
4. Adición de asignaciones entre recursos compartidos de origen y recursos compartidos de las réplicas

El esquema sólo se extiende una vez; no obstante, debe configurar la extensión de esquema de Active Directory para cada servidor DPM. Si activa la recuperación por el usuario final en otros servidores DPM del dominio, el proceso ejecuta los pasos 3 y 4 para cada uno de ellos. Si es necesario, DPM actualizará la asignación de recursos compartidos (paso 4) después de cada sincronización.

Los administradores de DPM que sean administradores de esquema y de dominio en los servicios de dominio de Active Directory pueden realizar estos pasos con tan solo hacer clic en DPM Administrator Console. Sin embargo, los administradores de DPM que no sean administradores de esquema y de dominio deberán indicar a uno de estos tipos de administradores que ejecuten la herramienta DPMADSchemaExtension.

La herramienta DPMADSchemaExtension está almacenada en el servidor DPM en la carpeta Microsoft Data Protection Manager\2006\End User Recovery. Los usuarios que sean administradores de esquema y de dominio pueden ejecutar la herramienta en cualquier ordenador con Windows Server 2003 que sea miembro del dominio en el que se ha implantado el servidor DPM. Al ejecutar la herramienta, el administrador debe especificar el nombre del servidor DPM.

Si utiliza la herramienta DPMADSchemaExtension para activar la recuperación por el usuario final, deberá ejecutarla una vez por cada servidor DPM.

Instalación del software cliente de instantáneas

Para que los usuarios finales puedan comenzar a recuperar de manera independiente las versiones anteriores de sus archivos, es necesario tener instalado el software cliente del punto de recuperación DPM en el ordenador. Si un cliente de copia simultánea de carpetas compartidas está presente en el ordenador, se deberá actualizar el software cliente para admitir DPM.

El software cliente del punto de recuperación se puede instalar en ordenadores que ejecutan el sistema operativo Windows XP con Service Pack 2 (SP2) o superior y Windows Server 2003 con o sin SP1.

Consulte también

Planificación de las configuraciones del servidor DPM

Consideraciones sobre seguridad

Consideraciones sobre seguridad

DPM actúa en la red como un servidor con privilegios. Como ayuda para garantizar la seguridad del servidor DPM, la arquitectura de seguridad de DPM se basa en las funciones de seguridad de Windows Server 2003 y los servicios de dominio de Active Directory, SQL Server 2005 y SQL Server Reporting Services.

Para mantener la arquitectura de seguridad de DPM:

- Acepte la configuración de seguridad predeterminada.
- No instale software innecesario en el servidor DPM.
- No cambie la configuración de seguridad tras la implantación de DPM. En concreto, no cambie la configuración de SQL Server 2005, de los Servicios de Internet Information Server (IIS), de DCOM ni de los usuarios y grupos locales que DPM crea durante la instalación del producto.
- Una instancia remota de SQL Server no se debe ejecutar como sistema local.

La instalación de software innecesario y la modificación de la configuración de seguridad predeterminada pueden comprometer gravemente la seguridad de DPM.

En esta sección

Configuración del software antivirus

Configuración de servidores de seguridad

Consideraciones sobre seguridad para la recuperación por el usuario final

Concesión de privilegios de usuario adecuados

Consulte también

Consideraciones sobre la recuperación por el usuario final

Planificación de las configuraciones del servidor DPM

Configuración del software antivirus

DPM es compatible con los productos de software antivirus más conocidos. Sin embargo, los productos antivirus pueden afectar al rendimiento de DPM y, si no están configurados correctamente, pueden dañar los datos de las réplicas y de los puntos de recuperación. En esta sección se proporcionan instrucciones para paliar estos problemas.

Configuración de la supervisión de virus en tiempo real

Para minimizar la disminución del rendimiento en el servidor DPM, desactive la supervisión antivirus en tiempo real de las réplicas de todos los orígenes de datos protegidos; para ello, desactive la supervisión en tiempo real del proceso de DPM msDPMprotectionagent.exe, que está ubicado en la carpeta Microsoft Data Protection Manager\DPM\bin. La supervisión en tiempo real de las réplicas reduce el rendimiento porque hace que el software antivirus explore todos los archivos afectados cada vez que DPM aplica cambios a las réplicas.

Además, si experimenta una disminución del rendimiento durante el uso de DPM Administrator Console, desactive la supervisión en tiempo real del proceso csc.exe, que está ubicado en la carpeta Windows\Microsoft.net\Framework\v2.0.50727. El proceso csc.exe es el compilador C#. La supervisión en tiempo real del proceso csc.exe puede reducir el rendimiento porque hace que el software antivirus explore los archivos que emite el proceso csc.exe al generar mensajes XML.

Para obtener instrucciones sobre cómo configurar la supervisión en tiempo real para los procesos individuales, consulte la documentación del producto antivirus.

Configuración de las opciones para los archivos infectados

Para evitar que los datos de las réplicas y de los puntos de recuperación resulten dañados, configure el software antivirus en el servidor DPM para que elimine los archivos infectados en lugar de limpiarlos o ponerlos en cuarentena automáticamente. La limpieza y puesta en cuarentena automática pueden dañar los datos dado que estos procesos hacen que el software antivirus modifique los archivos con cambios que DPM no puede detectar. Cada vez que DPM intente sincronizar una réplica que otro programa ha modificado, los datos de la réplica y de los puntos de recuperación pueden resultar dañados. La configuración del software antivirus para que elimine los archivos infectados evita este problema. Tenga en cuenta, sin embargo, que cada vez que el software antivirus elimine archivos de una réplica, deberá ejecutar la sincronización manual con comprobación de coherencia. Para obtener instrucciones sobre cómo configurar el software antivirus para eliminar los archivos infectados, consulte la documentación del producto.

Consulte también

Consideraciones sobre seguridad

Configuración de servidores de seguridad

Si los ordenadores que desea proteger residen detrás de un servidor de seguridad, debe configurar éste para que permita la comunicación entre el servidor DPM, los ordenadores que está protegiendo y las controladoras de dominio.

Protocolos y puertos

Es posible que, según la configuración de la red, necesite configurar el servidor de seguridad para permitir la comunicación entre DPM, los servidores protegidos y las controladoras de dominio. En la tabla siguiente se proporcionan detalles sobre los protocolos y los puertos que DPM utiliza para ayudarle en la configuración del servidor de seguridad.

Protocolos y puertos utilizados por DPM

Protocolo	Port	Detalles
DCOM	135/TCP Dinámico	El protocolo de control de DPM utiliza DCOM. DPM emite comandos al agente de protección invocando llamadas de DCOM en el agente. El agente de protección responde invocando llamadas de DCOM en el servidor DPM. El puerto TCP 135 es el punto de resolución del punto final DCE utilizado por DCOM. De manera predeterminada, DCOM asigna dinámicamente los puertos comprendidos en el rango de puertos TCP entre 1024 y 65535. Sin embargo, este rango puede configurarse mediante Servicios de componente. Para obtener más información, consulte Using Distributed COM with Firewalls (Uso de COM distribuido con servidores de seguridad) en http://go.microsoft.com/fwlink/?LinkId=46088.
TCP	5718/TCP 5719/TCP	El canal de datos de DPM se basa en TCP. Tanto DPM como el ordenador protegido inician conexiones para permitir operaciones de DPM, como la sincronización y la recuperación. DPM se comunica con el coordinador de agentes en el puerto 5718 y con el agente de protección en el puerto 5719.
DNS	53/UDP	Se utiliza entre DPM y la controladora de dominio, así como entre el ordenador protegido y la controladora de dominio para la resolución de nombres de host.
Kerberos	88/UDP 88/TCP	Se utiliza entre DPM y la controladora de dominio, así como entre el ordenador protegido y la controladora de dominio para la autenticación del punto final de conexión.
LDAP	389/TCP 389/UDP	Se utiliza entre DPM y la controladora de dominio para las consultas.
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	Se utiliza entre DPM y el ordenador protegido, entre DPM y la controladora de dominio, y entre el ordenador protegido y la controladora de dominio para diversas operaciones. Se utiliza en el SMB directamente alojado en TCP/IP para funciones de DPM.

Servidor de seguridad de Windows

El servidor de seguridad de Windows se incluye en Windows Server 2003 SP1. Si activa el servidor de seguridad de Windows en el servidor DPM antes de instalar DPM, el programa de configuración de DPM configurará de correctamente el servidor de seguridad de DPM. Si lo hace después de instalar DPM, deberá configurar manualmente el servidor de seguridad para permitir la comunicación entre el servidor DPM y los ordenadores protegidos. Para configurar el servidor de seguridad de Windows en un servidor DPM, abra el puerto 135 al tráfico TCP y especifique el servicio DPM (Microsoft Data Protection Manager/DPM/bin/MsDPM.exe) y el agente de protección (Microsoft Data Protection Manager/DPM/bin/Dpmra.exe) como excepciones a la política del servidor de seguridad de Windows.

Para obtener instrucciones sobre cómo configurar el servidor de seguridad de Windows, busque "Firewall de Windows" en Ayuda y soporte técnico de Windows para Windows Server 2003.

Consulte también

Consideraciones sobre seguridad

Consideraciones sobre seguridad para la recuperación por el usuario final

Si bien puede activar la recuperación de datos de archivos por el usuario final, no lo puede hacer para datos de aplicaciones. Utilice únicamente grupos de seguridad basados en dominios para los permisos de archivos y carpetas en los que piensa activar la recuperación por el usuario final. Si depende de grupos de seguridad locales, DPM no puede garantizar la coherencia entre el acceso del usuario final a los datos de los ordenadores protegidos y el acceso del usuario final a los puntos de recuperación de esos datos en el servidor DPM.

Por ejemplo, si el conjunto de usuarios incluido en el grupo de usuarios locales del ordenador protegido es diferente del conjunto de usuarios incluido en el grupo de usuarios locales del servidor DPM, ambos conjuntos de usuarios tendrán acceso a los datos del ordenador protegido y a los puntos de recuperación de esos datos.

Consulte también

Consideraciones sobre seguridad

Concesión de privilegios de usuario adecuados

Antes de comenzar una implantación de DPM, compruebe que se hayan concedido los privilegios necesarios a los usuarios adecuados para realizar las diversas tareas. En la tabla siguiente se muestran los privilegios de usuario necesarios para realizar las principales tareas asociadas con DPM.

Privilegios de usuario necesarios para realizar tareas de DPM

Tarea	Privilegios necesarios
Añadir un servidor DPM a un dominio de Active Directory	Cuenta de administrador de dominio o derechos de usuario para añadir una estación de trabajo a un dominio
Instalación de DPM	Cuenta de administrador en el servidor DPM
Instalar el agente de protección DPM en un ordenador	Cuenta de dominio que sea miembro del grupo de administradores locales en el ordenador
Abrir DPM Administrator Console	Cuenta de administrador en el servidor DPM
Extender el esquema de los servicios de dominio de Active Directory para activar la recuperación por el usuario final	Privilegios de administrador de esquema en el dominio
Crear un contenedor de servicios de dominio de Active Directory para activar la recuperación por el usuario final	Privilegios de administrador de dominio en el dominio
Conceder permisos a un servidor DPM para cambiar el contenido del contenedor	Privilegios de administrador de dominio en el dominio
Activar la función de recuperación por el usuario final en un servidor DPM	Cuenta de administrador en el servidor DPM
Instalar software cliente del punto de recuperación en un ordenador cliente	Cuenta de administrador en el ordenador cliente
Acceder a versiones anteriores de datos protegidos en el ordenador cliente	Cuenta de usuario con acceso al recurso compartido protegido
Recuperar datos de Windows SharePoint Services	Cuenta de administrador del conjunto Windows SharePoint Services que sea también una cuenta de administrador en el servidor web de aplicaciones para usuario en el que está instalado el agente de protección

Consulte también

Consideraciones sobre seguridad

Lista de verificación y líneas maestras del plan de implantación

En esta lista de verificación se incluyen las tareas de planificación necesarias para preparar la implantación de Data Protection Manager (DPM) 2007.

Tarea	Referencia
Identifique los orígenes de datos que se van a proteger, incluida la información siguiente: • Tipo de origen de datos (archivo, Microsoft Exchange, Microsoft SQL Server, Microsoft Windows SharePoint Services, Microsoft Virtual Server, estado del sistema) • Tamaño del origen de datos • Las carpetas o las extensiones de nombre de archivo que se van a excluir de la protección • Nombre de dominio completamente calificado (FQDN) del ordenador • Nombre del clúster (si corresponde)	¿Qué desea proteger?
Identifique uno de los métodos siguientes para cada grupo de protección: • Protección basada en disco a corto plazo • Protección basada en cinta a corto plazo • Protección basada en cinta a largo plazo • Protección basada en disco a corto plazo y protección basada en cinta a largo plazo • Protección basada en cinta a corto plazo y protección basada en cinta a largo plazo	Selección de un método de protección de datos

Tarea	Referencia
Para cada origen de datos, determine los objetivos de recuperación de los métodos de protección de datos que utilizará. Para la protección basada en disco a corto plazo, identifique la información siguiente: • Intervalo de retención • Frecuencia de sincronización • Número de puntos de recuperación Para la protección basada en cinta a corto plazo, identifique la información siguiente: • Intervalo de retención • Programación de copia de seguridad • Tipo de copia de seguridad • Número de copias de seguridad • Esquema de etiquetado de cintas Para la protección basada en cinta a largo plazo, identifique la información siguiente: • Intervalo de retención • Programación de copia de seguridad y opciones de programación • Número de copias de seguridad • Esquema de etiquetado de cintas	¿Cuáles son sus objetivos de recuperación? Definición de los objetivos de recuperación
Organice los orígenes de datos en grupos de protección.	Selección de los miembros del grupo de protección
Determine sus necesidades de almacenamiento en función de la información sobre los orígenes de datos protegidos y los objetivos de recuperación.	Asignación de espacio para grupos de protección
Si utiliza la protección basada en cinta, decida si desea comprimir o cifrar los datos de las cintas.	Especificación de detalles de cinta y biblioteca
Decida el método de creación de réplicas que utilizará para cada grupo de protección.	Selección de un método de creación de réplicas

Tarea	Referencia
Identifique las configuraciones del servidor DPM necesarias, incluida la información siguiente: • El número de servidores DPM • La ubicación de cada servidor DPM • La instancia de SQL Server que utilizará cada servidor DPM	Planificación de las configuraciones del servidor DPM
Determine las configuraciones de disco que cada servidor DPM necesitará para satisfacer las necesidades de almacenamiento de los grupos de protección. Incluya los volúmenes personalizados que utilizarán los orígenes de datos específicos.	Planificación del bloque de almacenamiento
Identifique los servidores DPM que necesitarán bibliotecas de cintas y la capacidad de cada biblioteca.	Planificación de la configuración de bibliotecas de cintas
Identifique los servidores DPM en los que se activará la recuperación por el usuario final, así como los clientes que necesitarán la instalación del software cliente del punto de recuperación.	Consideraciones sobre la recuperación por el usuario final

Consulte también

Introducción a Data Protection Manager 2007

Planificación de la implantación de DPM

Planificación de grupos de protección