Microsoft System Center 2012 R2

System Center 2012 R2 Data Protection Manager (DPM) Documentation

Microsoft Corporation

Published: November 1, 2013

Authors

Rayne Wiselman

Applies To

System Center 2012 – DPM

System Center 2012 Service Pack 1 (SP1) – DPM

System Center 2012 R2 – DPM

Feedback

Send suggestions and comments about this document to sc2012docs@microsoft.com.

Revision History

Release Date	Changes
October 17, 2013	Original release of this guide
November 1, 2013	Minor updates to this guide

Contents

Getting Started with System Center 2012 - DPM

This content provides information to help you get started with System Center 2012 – Data Protection Manager (DPM).

In This Section

System Requirements for DPM in System Center 2012

What's new in System Center 2012 - DPM

Help Overview for System Center 2012 - Data Protection Manager

Support Matrix for DPM Protection

Overview of DPM Features

Product Support Overview for System Center 2012 - Data Protection Manager

What's New in DPM

What's New topics summarize features included in major releases of DPM in System Center 2012.

- What's new in System Center 2012 R2 - DPM
- What's new in System Center 2012 SP1 - DPM
- What's new in System Center 2012 - DPM

What's new in System Center 2012 R2 - DPM

This topic summarizes the new features and enhancements that are available in System Center 2012 R2 Data Protection Manager (DPM).

- **Windows Azure Backup**—You can back up DPM data in System Center 2012 R2 and System Center 2012 SP1 to Windows Azure Backup. For more information, see Backing Up DPM using Windows Azure Backup.
- **SQL Server cluster support**—DPM now supports the use of clustered SQL Server nodes for its database. This removes the standalone limitation that existed in System Center 2012 and System Center 2012 SP1, and provides the following:
  - Reliability—Support for a SQL Server cluster mitigates the single point of failure when a standalone SQL server is used.
  - Scalability—As your DPM deployment grows, for every DPM server a new SQL Server database needs to be created. Increasing workloads on a single SQL Server can potentially cause performance problems and a higher risk of failure.

- Consistency—Support for a SQL Server cluster makes DPM consistent with other System Center 2012 components.

  In addition, the DPM reporting server can be installed on the same standalone or clustered SQL Server that is used for the DPM database, or you can install it on a different SQL Server.

- **Virtualized deployment**—DPM can be deployed in a virtual environment. You can install DPM on a virtual machine, and configure storage using .vhd storage pool disks that are shared through the VMM library.
- **Linux virtual machine backup**—DPM provides support for the protection and backup of Linux virtual machines, in addition to the support already provided for Hyper-V virtual machines. Note that for Linux backups only file-consistent snapshots are supported. Application-consistent snapshots are not. In addition, protection of Linux virtual machines is not supported using Windows Azure Backup.

What's new in System Center 2012 SP1 - DPM

This section introduces the new features and enhancements that are available in System Center 2012 – Data Protection Manager (DPM) in System Center 2012 Service Pack 1 (SP1).

- Improved backup performance of Windows Server 2012 Hyper-V over CSV 2.0 deployments

  Cluster Shared Volumes (CSVs) provide a distributed file access solution so that multiple nodes in the cluster can simultaneously access the same NTFS file system.

  In System Center 2012 Service Pack 1 (SP1) DPM, CSV 2.0 support allows the following benefits:

  - 900% improvement in Express Full backups.
  - Parallel backups.
  - No performance difference between backups from owner and non-owner nodes.
  - Support for SMB shares.

  For more information on deploying DPM protection for Hyper-V virtual machines, see Managing Hyper-V computers

- Protect Hyper-V over remote SMB share

  In Windows Server 2012, you can now use SMB file shares as remote storage for Hyper-V. With this new capability, Hyper-V can store virtual machine files, which includes configuration, virtual hard disk (VHD) files, and snapshots, on SMB file shares. This offers benefits like Ease of provisioning and management, increased flexibility, ability to take advantage of existing investment in a converged network, reduced capital expenditures, and reduced operating expenditures.

  In System Center 2012 Service Pack 1 (SP1) DPM, SMB shares support allows the following benefits:

  - More efficient Express Full backups.
  - Continued protection even after Live Migration.
  - Support for SMB shares in standalone and scaled-out deployments.

For more information on deploying DPM protection for Hyper-V virtual machines using SMB file shares, see Managing Hyper-V computers

- DPM now allows you to exclude virtual machine pagefiles from incremental backups to improve usage of storage and improve backup performance.
- Scale out support for Hyper-V virtual machines.
- Protect Windows 8 deduplicated volumes

  Data deduplication involves finding and removing duplication within data without compromising its fidelity or integrity. DPM allows optimized back of deduplicated volumes, both locally and over the network.

  For more information on protecting deduplicated volumes, see Protecting deduplicated volumes
- Support for Live Migration

  Live migration is a Hyper-V feature in Windows Server that allows you to transparently move running virtual machines from one node of the failover cluster to another node in the same cluster or another cluster without a dropped network connection or perceived downtime.

  In System Center 2012 Service Pack 1 (SP1) DPM, Live Migration support allows the following benefits:

  - Uninterrupted protection for migrated virtual machines.
  - Support for inter-cluster, cluster to standalone, and standalone to cluster migrations apart from intra-cluster migration.
  - Support for SMB shares.
- Integration with Windows Azure Online Backup

  Important
  Windows Azure Online Backup currently is currently on Preview and does not support production environments.

  - With System Center 2012 SP1, DPM can now backup data from the DPM server to an offsite storage managed by the Windows Azure Online Backup Service.
  - System Center customers can avail of this functionality by signing up for the Windows Azure Online Backup service. Customers will need to download and install the Windows Azure Online Backup agent on the DPM server which will be used to transfer the data between the DPM server(s) and Windows Azure Online Backup service.
  - Up to 120 DPM recovery points can be retained in Windows Azure Online Backup.
  - Support for Windows Server 2008 R2 – Online backup can be enabled on DPM servers running on Windows Server 2008 R2.
  - Support for protecting SQL Server.
- Support for protecting file server data.
- Support for protecting virtual machines.
- Support for protecting SQL Server 2012 databases that use the AlwaysOn feature.
- You can use a stand-alone instance of SQL Server 2012 to host the DPM database.
- Support for protecting file server using Resilient File System (ReFS).

- Support for protecting SharePoint 2013.
- Support for protecting Exchange Server 2013.

What's new in System Center 2012 - DPM

This topic summarizes the new features and enhancements that are available in System Center 2012 – Data Protection Manager (DPM) in System Center 2012.

1. Centralized management of multiple DPM servers.
2. Remote management of DPM servers.
3. Support for multiple DPM servers to share one instance of SQL Server for DPMDB.
4. Certificate-based authentication for computers in workgroups or untrusted domains.
5. Optimized item-level recovery for SharePoint farms.
6. Improved usage of tapes through protection group sets.
7. Support for protecting VMM hosts.

System Requirements for DPM in System Center 2012

Before you install System Center 2012 – Data Protection Manager (DPM), ensure that the computer you will use for your DPM server and all the computers and applications you want to protect meet or exceed the minimum hardware, software, and network requirements.

In This Section

System requirements for System Center 2012 R2 - DPM

System requirements for System Center 2012 SP1 - DPM

System requirements for System Center 2012 - DPM

System requirements for System Center 2012 R2 - DPM

This topic summarizes system requirements for System Center 2012 R2- Data Protection Manager (DPM) in Windows Server® 2012 R2.

DPM server hardware requirements

The following table lists the minimum and recommended hardware requirements for the DPM server.

Component	Minimum requirement	Recommended requirement
Processor	1 GHz, dual-core CPU or faster	2.33 GHz quad-core CPU

Component	Minimum requirement	Recommended requirement
RAM	4 GB	8 GB
Pagefile	1.5 times the amount of RAM on the computer.	0.2 percent of the combined size of all recovery point volumes, in addition to the minimum required size (1.5 times the amount of RAM on the computer).
Disk space for DPM installation	• DPM installation location: 3 GB • Database files drive: 900 MB • System drive: 1 GB The system drive disk space requirement is necessary if you choose to install the dedicated instance of SQL Server from DPM Setup. If you use a remote instance of SQL Server, this disk space requirement is considerably less.	DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a temporary DPM installation location; therefore, we recommend that the volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool The storage pool does not support Universal Serial Bus (USB)/1394 disks.	1.5 times the size of the protected data	2.5–3 times the size of the protected data
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot record (MBR) disks These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

DPM server operating system requirements

The table below summarizes supported operating systems for the DPM server. Note that only 64-bit operating systems are supported. 32-bit and Itanium architecture–based operating systems are not supported.

Supported operating system
Windows Server 2012 R2, Datacenter and Standard editions
Windows Server 2012, Datacenter and Standard editions
Windows Server 2008 R2 with SP1, Standard and Enterprise editions

DPM server installation requirements and limitations

- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system.
- DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:
  - A computer on which the Application Server role is installed.
  - A computer that is an Operations Manager management server
  - A computer on which Exchange Server is running.
  - A computer that is a cluster node.
- DPM is not supported on the Turkish language version of any of the listed Windows Server versions.
- The following prerequisites are required for installation:
  - Microsoft .NET Framework 4.0
  - Microsoft Visual C++ 2008 Redistributable Microsoft Visual C++ 2008 Redistributable
  - Windows PowerShell 3.0
  - Windows Installer 4.5 or later versions
  - Windows Single Instance Store (SIS)
  - Microsoft Application Error Reporting

  Setup automatically installs these if they are not already installed or enabled. If any pre-requisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.
- After you have installed DPM, we recommend that you run Windows Update on the DPM server and, if you use a remote database, on the remote computer where the DPM database is located, and install all important updates or hotfixes.

Disk requirements

DPM requires the following:

- A disk that is dedicated to the storage pool
- A disk that is dedicated to:
  - System files
  - DPM installation files
  - DPM prerequisite software
  - DPM database files

Note that:

- DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, disk is defined as any disk device manifested as a disk in Disk Management. For more information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool.
- If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that DPM will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.
- DPM in System Center 2012 R2 Preview can use the following types of storage:
  - .VHD disks that are managed in the VMM library (for virtualized deployments).
  - Pass-through disk with host direct attached storage (DAS)
  - Pass-through iSCSI LUN which is attached to host.
  - Pass-through FC LUN which is attached to host.
  - iSCSI target LUN which is connected to DPM virtual machine directly.
- Short-term or long-term backup to tape will be limited to using iSCSI attached tape libraries, and we recommend a separate NIC for that connection.
- You cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

SQL Server requirements

For the DPM database, DPM requires a dedicated instance of 64-bit SQL Server as follows:

- SQL Server 2012 with SP1 (11.0.3000)—Standard or Enterprise edition.
- SQL Server 2008 R2 with SP2 (10.50.4000)—Standard or Enterprise edition.

When you use a remote instance of SQL Server with the DPM installation, note the following requirements:

- You must install the remote instance of SQL Server before you install DPM.
- A remote instance of SQL Server on a domain controller is not supported.

- The computer that is running a remote instance of SQL Server must be located in the same domain and time zone as the DPM server.
- Setup creates the **DPMDBReaders$<DPM server name>** and **DPMDBAdministrators$<DPM server name>** local groups on the computer that is running the remote instance of SQL Server. You must add DPM administrators to these groups for DPM to use the remote instance of SQL Server.
- For the DPM server to access a remote instance of SQL Server through Windows Firewall, you must configure an exception on the computer that is running SQL Server to use port 80.
- You must install the DPM support files on the computer that is running the remote instance of SQL Server. For more information, see Setting up the DPM database.
- DPM in System Center 2012 R2 preview supports the use of a clustered instance of SQL Server 2012 to host a remote DPM database, or a reporting server.
- You cannot host the DPM database on a SQL Server AlwaysOn deployment.

In addition to installing programs that are required for DPM, SQL Server Setup installs the following programs, which are not required for DPM:

- Microsoft SQL Server Compact 3.5 SP1
- Microsoft SQL Server Compact 3.5 SP1 Query Tools
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft Visual Studio Tools for Applications 2.0
- Microsoft Office 2003 Web Components

These programs are not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall these programs manually.

Data source limits for the DPM server

The following table lists the data source limits that a DPM server can protect (if it meets the minimum hardware requirements) and the recommended disk space required for the DPM server.

Platform	Data source limit	Recommended disk space
64-bit computers	600 volumes, of which 300 are replica volumes and 300 are recovery point volumes Data sources are typically spread across approximately 75 servers and 150 client computers.	120 TB per DPM server, with 80 TB replica size with a maximum recovery point size of 40 TB

Protected computer requirements

For a complete list of DPM protection support for computers and workloads, see the Support Matrix for DPM Protection. Prerequisites for computers running the DPM protection agent are

summarized in the following table. If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Protected workload	Prerequisites
Computer volumes	• Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB. • Computers must have the Microsoft .NET Framework 3.5 with Service Pack 1 (SP1) installed.
File Servers	Before you can protect a file server running Windows Server 2008 R2, you must apply the hotfix KB977381
Exchange	Note the following when protecting Exchange: • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006. • The eseutil.exe and ese.dll versions that are installed on the most recent release of Exchange Server must be the same versions that are installed on the DPM server. So if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see **Eseutil.exe and Ese.dll**. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll: a. Install the Microsoft Exchange Server 2007 management tools on the DPM server. b. When you install the management tools,

Protected workload	Prerequisites
	ensure that you install the management tools for the latest version of Microsoft Exchange that you are protecting. For example, if one of your mail servers is running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2007 SP1, you must install the management tools for Microsoft Exchange 2007 SP1. c. At the command prompt, in the **<DPM installation folder>\Bin** directory, use the following syntax with the **fsutil** command to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>** On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"**

Hyper-V	To protect Hyper-V, note the following:
	• For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB975354
	• For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in KB975921
	• Before you can protect a computer running Windows Server 2008 with Hyper-V, you must apply the following updates:
	  • KB948465
	  • KB971394

SharePoint	When protecting SharePoint, note the following: • Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422 • If you use the **Office SharePoint Server Search** service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply the following updates: • KB951695

Protected workload	Prerequisites
	• KB941422

Remote administration requirements

In addition to managing DPM directly from the DPM server, you can use DPM Remote Administration or the Central Console.

DPM Remote Administration allows you to work on your DPM servers from any computer. It also supports task-based scripting.

With DPM Central Console you can monitor and manage multiple DPM servers from one location.

Operating system requirements are summarized in the following table.

Remote Administration Option	Supported Operating System
Remote Administration	• Windows 8.1 preview • Windows 8 • Windows 7 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2
Central Console	

In addition, computers from which you want to remotely administer DPM require the following prerequisites::

- DPM Central Console must be installed on Operations Manager server or a computer running Operations Manager Console. You can install it on the following operating systems:
- Microsoft .NET Framework 4.0 or 4.5
- If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Network requirements

The following are the network requirements for System Center 2012 – Data Protection Manager (DPM):

- DPM must be installed on a 64-bit computer that is located in a Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 Active Directory domain.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you can protect the computers using DPM's support for computers in workgroups or untrusted domains. For more information, see Managing Protected Computers in Workgroups and Untrusted Domains.

DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 forest mode.

- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM does not support disjointed namespaces.

System requirements for System Center 2012 SP1 - DPM

This topic summarizes system requirements for System Center 2012 – Data Protection Manager (DPM) in System Center 2012 Service Pack 1 (SP1).

DPM server hardware requirements

The following table lists the minimum and recommended hardware requirements for the DPM server.

Component	Minimum requirement	Recommended requirement
Processor	1 GHz, dual-core CPU or faster	2.33 GHz quad-core CPU
RAM	4 GB	8 GB
Pagefile	1.5 times the amount of RAM on the computer	0.2 percent of the combined size of all recovery point volumes, in addition to the minimum required size (1.5 times the amount of RAM on the computer).
Disk space for DPM installation	• DPM installation location: 3 GB • Database files drive: 900 MB • System drive: 1 GB **Note** The system drive disk space requirement is necessary if you choose to install the dedicated instance of SQL Server from DPM Setup. If you use a	**Note** DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a DPM temporary installation location; therefore, we recommend that the

Component	Minimum requirement	Recommended requirement
	remote instance of SQL Server, this disk space requirement is considerably less.	volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool **Note** The storage pool does not support Universal Serial Bus (USB)/1394 disks.	1.5 times the size of the protected data	2.5–3 times the size of the protected data
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot record (MBR) disks **Note** These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

DPM server operating system requirements

Supported operating systems

Supported operating system	Details	Required updates
Windows Server 2012, Datacenter and Standard editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	
Windows Server 2008 R2 SP1, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	

Supported operating system	Details	Required updates
Windows Server 2008 R2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	Before you install DPM on a computer that is running Windows Server 2008 R2, you must install the following updates and hotfixes: • KB983633 • KB2223201 **Important** If you are upgrading to Windows Server 2008 R2, you must remove any pre-release version of Windows PowerShell 2.0 before you upgrade.
Windows Server 2008 SP2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	
Windows Server 2008, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	• KB971254 • KB962975 • KB975759 • KB2279769 **Important** After installing all updates, restart the computer before you install DPM. For more information about Windows Server 2008 system requirements, see Windows Server 2008 System Requirements.

Disk requirements

DPM requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files
- DPM prerequisite software
- DPM database files

Note the following:

- DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, disk is defined as any disk device manifested as a disk in Disk Management. For more information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool.
- If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that DPM will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.
- The DPM storage pool disks cannot be .VHD – they must be either iSCSI attached disks or pass-through disks. The following types of disk configuration are supported as DPM storage pool:
  - Pass-through disk with host direct attached storage (DAS)
  - Pass-through iSCSI LUN which is attached to host.
  - Pass-through FC LUN which is attached to host.
  - iSCSI target LUN which is connected to DPM virtual machine directly.
- Short-term or long-term backup to tape will be limited to using iSCSI attached tape libraries, and we recommend a separate NIC for that connection.
- you cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

Installation requirements and limitations

This section summarizes installation requirements, prerequisites, and limitations.

DPM server requirements

- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system.
- DPM server DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:
  - A computer on which the Application Server role is installed.
  - A computer that is an Operations Manager management server
  - A computer on which Exchange Server is running.
  - A computer that is a cluster node.

- DPM is not supported on the Turkish language version of any of the listed Windows Server versions.
- The following prerequisites are required for installation:
  - Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)
  - Microsoft Visual C++ 2008 Redistributable
  - Windows PowerShell 2.0
  - Windows Installer 4.5 or later versions
  - Windows Single Instance Store (SIS)
  - Microsoft Application Error Reporting

  Setup automatically installs these if they are not already installed or enabled. If any pre-requisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.
- After you have installed DPM, we recommend that you run Windows Update on the DPM server and, if you use a remote database, on the remote computer where the DPM database is located, and install all important updates or hotfixes.

SQL Server requirements

For the DPM database, DPM requires a dedicated instance of the 64-bit version of SQL Server 2012 or SQL Server 2008 R2 or SQL Server 2008 R2 SP1, Enterprise or Standard Edition. During setup, you can select either to have DPM Setup install SQL Server 2008 R2 on the DPM server, or you can specify that DPM use a remote instance of SQL Server.

If you do not have a licensed version of SQL Server 2008 R2, you can install an evaluation version from the setup DVD. To install the evaluation version, do not provide the product key when you are prompted. However, you must buy a license for SQL Server if you want to continue to use it after the evaluation period.

When you use a remote instance of SQL Server with the DPM installation, note the following requirements:

- You must install the remote instance of SQL Server before you install DPM.

  Important
  A remote instance of SQL Server on a domain controller is not supported.
- The computer that is running a remote instance of SQL Server must be located in the same domain and time zone as the DPM server.
- Setup creates the **DPMDBReaders$<DPM server name>** and **DPMDBAdministrators$<DPM server name>** local groups on the computer that is running the remote instance of SQL Server. You must add DPM administrators to these groups for DPM to use the remote instance of SQL Server.
- For the DPM server to access a remote instance of SQL Server through Windows Firewall, you must configure an exception on the computer that is running SQL Server to use port 80.
- You must install the DPM support files on the computer that is running the remote instance of SQL Server. For more information, see Setting up the DPM database.

- You cannot user a clustered instance of SQL Server 2012 to host a remote DPM database.
- You cannot host the DPM database on a SQL Server AlwaysOn deployment.

In addition to installing programs that are required for DPM, SQL Server Setup installs the following programs, which are not required for DPM:

- Microsoft SQL Server Compact 3.5 SP1
- Microsoft SQL Server Compact 3.5 SP1 Query Tools
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft Visual Studio Tools for Applications 2.0
- Microsoft Office 2003 Web Components

Note

These programs are not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall these programs manually.

Data source limits for DPM server

The following table lists the data source limits that a DPM server can protect (if it meets the minimum hardware requirements) and the recommended disk space required for the DPM server.

Platform	Data source limit	Recommended disk space
64-bit computers	600 volumes, of which 300 are replica volumes and 300 are recovery point volumes Data sources are typically spread across approximately 75 servers and 150 client computers.	120 TB per DPM server, with 80 TB replica size with a maximum recovery point size of 40 TB

Requirements for protected computers

For a complete list of DPM protection support for computers and workloads, see the Support Matrix for DPM Protection. Prerequisites for computers running the DPM protection agent are summarized in the following table. If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Protected workload	Prerequisites
Computer volumes	• Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to

Protected workload	Prerequisites
	protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB. • Computers must have the Microsoft .NET Framework 3.5 with Service Pack 1 (SP1) installed.
File Servers	Before you can protect a file server running Windows Server 2008 R2, you must apply the hotfix KB977381 Before you can protect a file server running Windows Server 2008, you must apply the following updates: • KB977381 • KB975759
Exchange	Note the following when protecting Exchange: • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006. • The eseutil.exe and ese.dll versions that are installed on the most recent release of Exchange Server must be the same versions that are installed on the DPM server. So if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see **Eseutil.exe and Ese.dll**. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll: a. Install the Microsoft Exchange Server 2007 management tools on the DPM server. b. When you install the management tools, ensure that you install the management tools for the latest version of Microsoft

Protected workload	Prerequisites
	Exchange that you are protecting. For example, if one of your mail servers is running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2007 SP1, you must install the management tools for Microsoft Exchange 2007 SP1. c. At the command prompt, in the **<DPM installation folder>\Bin** directory, use the following syntax with the **fsutil** command to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>** On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"**

Hyper-V	To protect Hyper-V, note the following:
	• For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB975354
	• For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in KB975921
	• Before you can protect a computer running Windows Server 2008 with Hyper-V, you must apply the following updates:
	  • KB948465
	  • KB971394

SharePoint	When protecting SharePoint, note the following:
	• Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422
	• If you use the **Office SharePoint Server Search** service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply the following updates:
	  • KB951695
	  • KB941422

Protected workload	Prerequisites

	• Before you can protect a computer running Windows SharePoint Services 3.0, you must apply the update in KB941422.
	• Before you can protect Windows SharePoint Services 3.0 data, you must do the following:
	  • Start the Windows SharePoint Services VSS Writer service on the Windows SharePoint Services server and then provide the protection agent with credentials for the Windows SharePoint Services farm.
	  • Install the SQL Server Client components on the front-end Web server of the Windows SharePoint Services farm that DPM is going to protect. For information about installing SQL Server 2008 components, see How to: Install SQL Server 2008.
	If you use the **Office SharePoint Server Search** service, before you can protect Windows SharePoint Services 3.0 data, you must apply the following updates:
	  • KB951695
	  • KB941422

Administration options

In addition to managing DPM directly from the DPM server, you can use the following options:

- Use DPM Remote Administration
- Use DPM Central Console

DPM Remote Administration

DPM Remote Administration allows you to work on your DPM servers from any computer. It also supports task-based scripting. You can install it on the following operating systems:

- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2008 R2
- Windows Server 2008

Computers from which you want to remotely administer DPM require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

DPM Central Console

With DPM Central Console you can monitor and manage multiple DPM servers from one location. You can monitor and troubleshoot servers running both DPM 2010 QFE2 with feature pack and DPM. DPM Central Console must be installed on Operations Manager server or a computer running Operations Manager Console. You can install it on the following operating systems:

- Windows 7
- Windows Vista

Computers from which you want to run DPM Central Console require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Network requirements

The following are the network requirements for System Center 2012 – Data Protection Manager (DPM):

- DPM must be installed on a 64-bit computer that is located in a Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 Active Directory domain.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you can protect the computers using DPM's support for computers in workgroups or untrusted domains. For more information, see Managing Protected Computers in Workgroups and Untrusted Domains.

  DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 forest mode.
- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM does not support disjointed namespaces.

System requirements for System Center 2012 - DPM

This topic summarizes system requirements for System Center 2012 – Data Protection Manager (DPM) in System Center 2012.

DPM server hardware requirements

The following table lists the hardware requirements for the DPM server.

Component	Minimum requirement	Recommended requirement
Processor	1 GHz, dual-core CPU or faster	2.33 GHz quad-core CPU
RAM	4 GB	8 GB
Pagefile	1.5 times the amount of RAM on the computer.	0.2 percent of the combined size of all recovery point volumes, in addition to the minimum requirement size (1.5 times the amount of RAM on the computer).
Disk space for DPM installation	• DPM installation location: 3 GB • Database files drive: 900 MB • System drive: 1 GB **Note** The system drive disk space requirement is necessary if you choose to install the dedicated instance of SQL Server from DPM Setup. If you use a remote instance of SQL Server, this disk space requirement is considerably less.	**Note** DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a DPM temporary installation location; therefore, we recommend that the volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool **Note** The storage pool does not support Universal Serial Bus (USB)/1394 disks.	1.5 times the size of the protected data	2.5–3 times the size of the protected data
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot

Component	Minimum requirement	Recommended requirement
		record (MBR) disks **Note** These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

DPM server operating system requirements

Supported operating systems

Supported operating system	Details	Required updates
Windows Server 2008 R2 SP1, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	
Windows Server 2008 R2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	Before you install DPM on a computer that is running Windows Server 2008 R2, you must install the following updates and hotfixes: • KB983633 • KB2223201 **Important** If you are upgrading to Windows Server 2008 R2, you must remove any pre-release version of Windows PowerShell 2.0 before you upgrade.
Windows Server 2008 SP2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	

Supported operating system	Details	Required updates
Windows Server 2008, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	• KB971254 • KB962975 • KB975759 • KB2279769 **Important** After installing all updates, restart the computer before you install DPM. For more information about Windows Server 2008 system requirements, see Windows Server 2008 System Requirements.

Disk requirements

DPM requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files
- DPM prerequisite software
- DPM database files

Note the following:

- DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, disk is defined as any disk device manifested as a disk in Disk Management. For more information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool.
- If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that DPM will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.
- The DPM storage pool disks cannot be .VHD – they must be either iSCSI attached disks or pass-through disks. The following types of disk configuration are supported as DPM storage pool:

    - Pass-through disk with host direct attached storage (DAS)
    - Pass-through iSCSI LUN which is attached to host.
    - Pass-through FC LUN which is attached to host.
    - iSCSI target LUN which is connected to DPM virtual machine directly.
- Short-term or long-term backup to tape will be limited to using iSCSI attached tape libraries, and we recommend a separate NIC for that connection.
- you cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

Installation requirements and limitations

This section summarizes installation requirements, prerequisites, and limitations.

DPM server requirements

- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system.
- DPM server DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:
    - A computer on which the Application Server role is installed.
    - A computer that is an Operations Manager management server
    - A computer on which Exchange Server is running.
    - A computer that is a cluster node.
- DPM is not supported on the Turkish language version of any of the listed Windows Server versions.
- The following prerequisites are required for installation:
    - Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)
    - Microsoft Visual C++ 2008 Redistributable
    - Windows PowerShell 2.0
    - Windows Installer 4.5 or later versions
    - Windows Single Instance Store (SIS)
    - Microsoft Application Error Reporting

    Setup automatically installs these if they are not already installed or enabled. If any pre-requisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.
- After you have installed DPM, we recommend that you run Windows Update on the DPM server and, if you use a remote database, on the remote computer where the DPM database is located, and install all important updates or hotfixes.

SQL Server requirements

For the DPM database, DPM requires a dedicated instance of the 64-bit version of SQL Server 2012 or SQL Server 2008 R2 or SQL Server 2008 R2 SP1, Enterprise or Standard

Edition. During setup, you can select either to have DPM Setup install SQL Server 2008 R2 on the DPM server, or you can specify that DPM use a remote instance of SQL Server.

If you do not have a licensed version of SQL Server 2008 R2, you can install an evaluation version from the setup DVD. To install the evaluation version, do not provide the product key when you are prompted. However, you must buy a license for SQL Server if you want to continue to use it after the evaluation period.

When you use a remote instance of SQL Server with the DPM installation, note the following requirements:

- You must install the remote instance of SQL Server before you install DPM.

  Important
  A remote instance of SQL Server on a domain controller is not supported.
- The computer that is running a remote instance of SQL Server must be located in the same domain and time zone as the DPM server.
- Setup creates the **DPMDBReaders$<DPM server name>** and **DPMDBAdministrators$<DPM server name>** local groups on the computer that is running the remote instance of SQL Server. You must add DPM administrators to these groups for DPM to use the remote instance of SQL Server.
- For the DPM server to access a remote instance of SQL Server through Windows Firewall, you must configure an exception on the computer that is running SQL Server to use port 80.
- You must install the DPM support files on the computer that is running the remote instance of SQL Server. For more information, see Setting up the DPM database.
- You cannot user a clustered instance of SQL Server 2012 to host a remote DPM database.
- You cannot host the DPM database on a SQL Server AlwaysOn deployment.

In addition to installing programs that are required for DPM, SQL Server Setup installs the following programs, which are not required for DPM:

- Microsoft SQL Server Compact 3.5 SP1
- Microsoft SQL Server Compact 3.5 SP1 Query Tools
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft Visual Studio Tools for Applications 2.0
- Microsoft Office 2003 Web Components

Note
These programs are not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall these programs manually.

Data source limits for DPM server

The following table lists the data source limits that a DPM server can protect (if it meets the minimum hardware requirements) and the recommended disk space required for the DPM server.

Platform	Data source limit	Recommended disk space
64-bit computers	600 volumes, of which 300 are replica volumes and 300 are recovery point volumes Data sources are typically spread across approximately 75 servers and 150 client computers.	120 TB per DPM server, with 80 TB replica size with a maximum recovery point size of 40 TB

Requirements for protected computers

For a complete list of DPM protection support for computers and workloads, see the Support Matrix for DPM Protection. Prerequisites for computers running the DPM protection agent are summarized in the following table. If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Protected workload	Prerequisites
Computer volumes	• Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB. • Computers must have the Microsoft .NET Framework 3.5 with Service Pack 1 (SP1) installed.
File Servers	Before you can protect a file server running Windows Server 2008 R2, you must apply the hotfix KB977381
Exchange	Note the following when protecting Exchange: • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006. • The eseutil.exe and ese.dll versions that are installed on the most recent release of Exchange Server must be the same versions

Protected workload	Prerequisites
	that are installed on the DPM server. So if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see **Eseutil.exe and Ese.dll**. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll: a. Install the Microsoft Exchange Server 2007 management tools on the DPM server. b. When you install the management tools, ensure that you install the management tools for the latest version of Microsoft Exchange that you are protecting. For example, if one of your mail servers is running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2007 SP1, you must install the management tools for Microsoft Exchange 2007 SP1. c. At the command prompt, in the **<DPM installation folder>\Bin** directory, use the following syntax with the **fsutil** command to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>** On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"**
Hyper-V	To protect Hyper-V, note the following: • For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB975354 • For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in KB975921

Protected workload	Prerequisites

	• Before you can protect a computer running Windows Server 2008 with Hyper-V, you must apply the following updates:
	  • KB948465
	  • KB971394

SharePoint	When protecting SharePoint, note the following:
	• Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422
	• If you use the **Office SharePoint Server Search** service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply the following updates:
	  • KB951695
	  • KB941422

Administration options

In addition to managing DPM directly from the DPM server, you can use the following options:

- Use DPM Remote Administration
- Use DPM Central Console

DPM Remote Administration

DPM Remote Administration allows you to work on your DPM servers from any computer. It also supports task-based scripting. You can install it on the following operating systems:

- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2008 R2
- Windows Server 2008

Computers from which you want to remotely administer DPM require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

DPM Central Console

With DPM Central Console you can monitor and manage multiple DPM servers from one location. You can monitor and troubleshoot servers running both DPM 2010 QFE2 with feature pack and

DPM. DPM Central Console must be installed on Operations Manager server or a computer running Operations Manager Console. You can install it on the following operating systems:

- Windows 7
- Windows Vista

Computers from which you want to run DPM Central Console require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Network requirements

The following are the network requirements for System Center 2012 – Data Protection Manager (DPM):

- DPM must be installed on a 64-bit computer that is located in a Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 Active Directory domain.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you can protect the computers using DPM's support for computers in workgroups or untrusted domains. For more information, see Managing Protected Computers in Workgroups and Untrusted Domains.

  DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 forest mode.
- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM does not support disjointed namespaces.

Support Matrix for DPM Protection

This topic summarizes the applications and data that can be protected by System Center 2012 – Data Protection Manager (DPM). Unless otherwise mentioned, support is for DPM in System Center 2012, System Center 2012 SP1, and in System Center 2012 R2).

Supported workload	Supported workload version	DPM in System Center 2012 R2	DPM in System Center 2012 SP1	DPM in System Center 2012	Protectable and recoverable data
Computers	Windows 8.1	Y	Y	N	Files

Supported workload	Supported workload version	DPM in System Center 2012 R2	DPM in System Center 2012 SP1	DPM in System Center 2012	Protectable and recoverable data
running client operating systems (64-bit, 32-bit) Note the following: • Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. • The volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a	Windows 8	Y	Y	Y	
	Windows 7	Y	Y	Y	
	Windows Vista with SP2	N	Y	Y	
	Windows Vista with SP1	N	N	Y	
	Windows Vista	N	N	Y	
	Windows XP with SP2	N	N	Y	

Supported workload	Supported workload version	DPM in System Center 2012 R2	DPM in System Center 2012 SP1	DPM in System Center 2012	Protectable and recoverable data
snapshot only if the volume size is greater than or equal to 1 GB.					

Computers running server operating systems
64-bit only. 32-bit or Itanium architecture–based operating systems are not supported
	Windows Server 2012 R2, Datacenter and Standard editions	Y	N	N	• Protectable data:
					  • Volume
					  • Share
					  • Folder
					  • System state
					• Recoverable data:
					  • Volume
					  • Share
					  • Folder
					  • Files
					  • System state

	Windows Server 2012, Datacenter and Standard editions	Y	Y	Y	
	Windows Server 2008 R2 with SP2, Standard and Enterprise editions	Y	Y	Y	
	Windows Server 2008 R2 SP1,	Y	Y	Y	

Supported workload	Supported workload version	DPM in System Center 2012 R2	DPM in System Center 2012 SP1	DPM in System Center 2012	Protectable and recoverable data
	Standard and Enterprise editions				
	Windows Server 2008 R2, Standard and Enterprise Editions	N	Y	Y	
	Windows Storage Server 2008	N	Y	Y	
	Windows Server 2003 R2 with SP2	N	Y	Y	
	Windows Server 2003 with SP2 - Core, Standard, Enterprise, and Datacenter Editions	N	Y	Y	
SQL Server	SQL Server 2012	Y	Y	Y	Database
	SQL Server 2008 R2	Y	Y	Y	
	SQL Server 2008	Y	Y	Y	

Exchange Server	Exchange Server 2013	Y	Y	N	Exchange 2007:
					• Protectable data:
					  • Storage group
					• Recoverable data:
					  • Storage group
					  • Database
					  • Mailbox
					Exchange 2010; Exchange 2013
					• Protectable data:
					  • Standalone Exchange Server 2010 servers

	Exchange Server 2010	Y	Y	Y	
	Exchange Server 2007	Y	Y	Y	

Supported workload	Supported workload version	DPM in System Center 2012 R2	DPM in System Center 2012 SP1	DPM in System Center 2012	Protectable and recoverable data

					• Databases under a database availability group (DAG)
					• Recoverable data:
					  • Mailbox
					  • Mailbox databases under a DAG

SharePoint	SharePoint 2013	Y	Y	N	• Protectable data:
					  • Farm
					  • SharePoint search
					  • Frontend Web server content
					• Recoverable data:
					  • Farm
					  • Database
					  • Web application
					  • File or list item
					  • SharePoint search
					  • SharePoint frontend Web server

	SharePoint 2010	Y	Y	Y	
	SharePoint 2007	Y	Y	Y	
	Windows SharePoint Server 3.0	Y	Y	Y	
Hyper-V	Windows Server 2012	Y	N	N	• Protectable data:

Supported workload	Supported workload version	DPM in System Center 2012 R2	DPM in System Center 2012 SP1	DPM in System Center 2012	Protectable and recoverable data
	R2, Datacenter and Standard editions with Hyper-V				• Hyper-V computers • Cluster shared volumes (CSV) • Recoverable data: Item-level recovery of: • Files and folders • Volumes • Virtual hard drives
	Windows Server 2012, Datacenter and Standard editions with Hyper-V	Y	Y	Y	
	Windows Server 2008 R2 SP2, Standard and Enterprise editions with Hyper-V	Y	Y	Y	
	Windows Server 2008 R2 SP1, Standard and Enterprise editions with Hyper-V	N	Y	Y	
	Windows Server 2008 with Hyper-V	N	Y	Y	

Overview of DPM Features

Data protection is essential to a business or organization, and System Center 2012 – Data Protection Manager (DPM) is an effective solution for providing that protection.

DPM includes the following features:

- Disk-based data protection and recovery.
- Command-line scripting using Windows PowerShell.
- Enterprise deployment methods for distributing the DPM agent.
- Enterprise monitoring with Operations Manager.
- Tape-based backup and archive solutions.
- Disaster recovery solutions, which provides bare-metal recovery of servers running Windows.

You can back up the DPM database to tape, or you can use a second DPM server in a geographically separated location to protect the primary DPM server.

If you use a second DPM server, you can restore data to protected computers directly from the secondary DPM server. The secondary DPM server can also protect computers until the primary DPM server is brought back online.

DPM provides protection of the following items:

- File data from volumes, shares, and folders.
- Application data, such as Microsoft Exchange Server storage groups, Microsoft SQL Server databases, Windows SharePoint Services farms, and Microsoft Virtual Server and its virtual machines.
- Files for workstations running Windows XP Professional SP2 and all Windows Vista editions except Home.
- Files and application data on clustered servers.
- System state for protected file and application servers.

In This Section

Protecting workloads with DPM

System Center 2012 – Data Protection Manager (DPM) protects Microsoft application workloads, computers, and servers. Computers and servers protected by DPM have the DPM agent installed on them.

Protecting applications

DPM provides protection for Microsoft workloads and applications, including Exchange, SharePoint Server, Hyper-V, File Server, and SQL Server. For a full list of the applications that are supported by DPM, and data that can be protected and recovered, see Support Matrix for DPM Protection.

Protecting servers and computers

DPM provides protection for computers running Microsoft client and server operating systems. For a full list of computers and servers that are supported by DPM, and data that can be protected and recovered, see Support Matrix for DPM Protection.

Protecting workgroup computers and computers in untrusted domains

DPM can support computers in workgroups and untrusted domains using certification authentication. DPM supports the following data sources for certificate-based authentication in workgroups or untrusted domains:

- SQL Server
- File Server
- Hyper-V

Both single server and clustered deployments are supported.

The following data sources are not supported:

- Exchange Server
- Computers running client operating systems
- SharePoint server
- Bare metal recovery
- System state

Protecting clustered servers

DPM supports shared disk clusters for File Servers and SQL Server 2008. DPM supports both non-shared disk clusters and shared disk clusters for Exchange Server 2007 and Exchange Server 2010.

DPM can protect shared disk clusters for the following:

- File Servers
- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012 (DPM in System Center 2012 SP1 and System Center 2012)
- Exchange Server 2007
- Exchange Server 2010

DPM can protect non-shared disk clusters for Exchange Server 2007 (cluster continuous replication). DPM can also protect Exchange Server 2007 configured for local continuous replication.

DPM in System Center 2012 SP1 and System Center 2012 cannot protect a SQL Server 2012 shared cluster using the SQL 2012 Always On (availablility group) feature.

For DPM protection agent installation, when you select a server that is a cluster node, DPM notifies you so that you can choose to install the protection agent on other nodes in the cluster as well.

End-user recovery is available for both clustered and non-clustered resources on clustered file servers.

On planned failover, DPM continues protection. On unplanned failover, DPM issues an alert that a consistency check is required.

Backup options

You can back up System Center 2012 – Data Protection Manager (DPM) data to disk-based storage, tape-based storage, a mixture of both disk and tape, a secondary DPM server, or to the

cloud using Windows Azure Backup. When you need to restore data recovery is fast and simple. You identify the data, and DPM locates the data and retrieves it.

The storage method you'll use depends on the protection requirements for your organization, and includes the following considerations:

- **How much data your organization can afford to lose.** Realistically, not all data is equally valuable. You should weigh the impact of loss against the costs of protection.
- **How quickly recovered data must be available.** Recovery of data that is critical to ongoing operations is typically more urgent than routine data. Additionally, identify servers providing essential services during working hours that must not be disrupted by recovery operations.
- **How long your organization must maintain data.** Long-term storage might be necessary for business operations, depending on the type and contents of the data. For example your organization might be subject to legal requirements for data retention.
- **How much your organization can spend on data protection.** When deciding how much to invest in data protection, you should include the cost of hardware and media, as well as the personnel costs for administration, management, and support.

Use the following table to help you understand the types of protection, and data protected, by each type of DPM backup.

Details	Backup to disk	Backup to tape	Backup to secondary DPM server	Backup to Windows Azure Backup
Short-term protection	Yes	Yes	Yes	Yes
Long-term protection	No	Yes	No	No
Offsite protection	No	Yes	Yes	Yes
Application protection support	Files, SQL Server, Exchange, SharePoint, Hyper-V, System State, Clients	Files, SQL Server, Exchange, SharePoint, Hyper-V, System State, Clients	Files, SQL Server, Exchange, SharePoint, Hyper-V, System State, Clients	Files, SQL Server, Hyper-V

Backing up to tape

Magnetic tape and similar storage media offer an inexpensive and portable form of data protection that is particularly useful for long-term storage.

In DPM, you can back up data from a computer directly to tape (D2T). You can also back up data from the disk-based replica (D2D2T). The advantage of creating your long-term backup on tape from the disk-based replica is that the backup operation can occur at any time with no impact on the computer being protected.

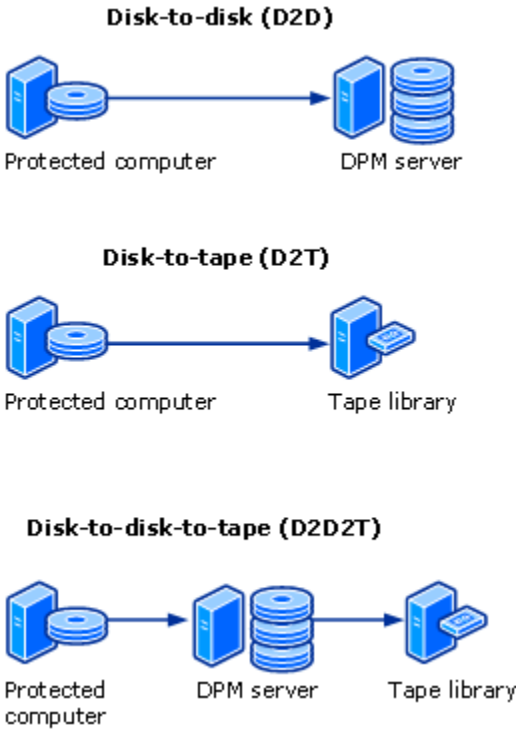
Additionally, a thorough disaster recovery plan includes offsite storage of critical information—you want to be able to recover your organization's data, should your facility be damaged or destroyed. Tape is a popular and convenient medium for offsite storage.

Using DPM, data can be backed up to tape as frequently as daily for short-term protection, and it can be maintained as long as 99 years for long-term protection.

Apart from this, software solutions from DPM partners allow you to use removable media such as a USB hard drive in place of tape.

Backing up to disk

Disk-based storage, also called *D2D,* for "disk-to-disk," is a type of backup in which data from one computer is stored on the hard disk of another computer. This contrasts with the more traditional method of backing up data from one computer to a storage media such as tape, also called *D2T,* for "disk-to-tape." For extra protection, the two methods can be combined in a disk-to-disk-to-tape (*D2D2T*) configuration that provides the rapid recovery benefits of disk-based storage in the short term and tape-based, archive storage for critical data in the long term. The following illustration shows the three storage methods.



One advantage of disk-based data protection is the potential time savings. Disk-based data protection requires none of the preparation time that tape-based protection does—locating the specific tape required for a job, loading the tape, positioning the tape to the correct starting point. The ease of using a disk encourages sending incremental data more frequently, which reduces the impact on the computer being protected and on network resources.

Data recovery with disk-based data protection is more reliable than that of tape-based systems. Disk drives typically have a much greater mean time between failure (MTBF) rating than tapes.

Recovery of data from disk is quicker and easier than recovery from tape. Recovering data from disk is a simple matter of browsing through previous versions of the data on the DPM server and copying selected versions directly to the protected computer. A typical file recovery from tape takes hours and can be costly, and administrators in a medium-size data center can usually expect to perform 10 to 20 or more of these recoveries each month.

Using DPM and disk-based data protection, data can be synchronized as frequently as every 15 minutes and maintained as long as 448 days.

Backing up to a secondary server

DPM server can be used as a backup for other DPM servers. The main DPM server that protects data sources directly is known as the primary DPM server. A DPM server that protects other DPM servers is known as the secondary DPM server. The secondary DPM server can protect both the databases and the replicas on the primary DPM server, to provide recovery if your primary DPM server fails. Note that a DPM server can act as both a primary server protecting data sources, and as a secondary server providing protection to a primary DPM server. There are a couple of deployment options for backup DPM servers. You can configure a single secondary server to back up a primary server, create a chain of DPM servers that protect one another, or configure cyclic protection where two DPM servers protect each other.

Backing up with Windows Azure Backup

DPM in System Center 2012 SP1 or System Center 2012 R2 can back up DPM data to the cloud using Windows Azure Backup. Cloud backup provides reduces costs, a simple and reliable service for storing short-term data offsite. Windows Azure Backup works with the DPM disk-based store. When online protection to Windows Azure is enabled, the disk-based replicas are backed up to an online location.

See Also

Backing up DPM

DPM Consoles and Tools

To facilitate the performance of key management tasks, System Center 2012 – Data Protection Manager (DPM) provides the following tools and capabilities for IT administrators:

- DPM Administrator Console
- DPM Central Console
- Reports and notifications
- Windows PowerShell integration
- Remote administration

- End-user recovery

DPM Administrator Console

DPM Administrator Console uses a task-based administration model that automates common tasks, enabling the administrator to get the job done with the fewest number of steps.

To simplify the management of data protection activities, DPM builds on Microsoft Management Console (MMC) functionality to provide a familiar, intuitive environment for performing configuration, management, and monitoring tasks.

DPM Administrator Console organizes tasks into five easily accessible task areas: monitoring, protection, recovery, reporting, and management. Wizards guide the administrator through basic configuration tasks such as adding disks, installing agents, and creating protection groups. Search and browse features are provided in the **Recovery** task area to assist in finding and recovering previous versions of files.

DPM Administrator Console provides both a **Jobs** tab and an **Alerts** tab for monitoring data protection activity. The **Jobs** tab provides the status and operational details for each scheduled, completed, running, canceled, or failed job. The **Alerts** tab aggregates informational alerts and error conditions to provide a summary view of activity for the entire system and provides recommended actions for each error.

DPM Central Console

The DPM Central Console in built on Operations Manager and deployed like a management pack. After you install Central Console, you can monitor your DPM servers from a central computer. You can even monitor from DPM servers from a desktop computer.

You can also open a remote DPM Administrator Console from the Central Console, and work with DPM objects.

Reports and Notifications

DPM provides a comprehensive set of reports that provide data about protection success and failures, recovery success and failures, and disk and tape utilization. You can also identify common errors and manage circulation of tapes. Summary reports aggregate information for all protected computers and protection groups. Detailed reports provide information about individual computers or protection groups. An administrator can use these reports to fine-tune protection after the initial DPM deployment.

DPM notifications provide a convenient way to stay informed when critical, warning, or informational alerts are generated. You choose the severity of alert that you want to be notified about; for example, you can choose to receive only critical alerts. You can also choose to receive notifications of the status of recovery jobs, and you can have scheduled DPM reports delivered as e-mail attachments so that you can monitor data protection trends and analyze data protection statistics at your convenience.

DPM Management Packs

Management Packs will be available for System Center 2012 – Data Protection Manager (DPM). As part of your data management strategy, you can use the Management Pack for DPM to centrally monitor data protection, state, health, and performance of multiple DPM servers, and the servers that they protect. From the Operations Manager Operations Console, an administrator can monitor DPM and network infrastructure simultaneously, analyzing issues with data protection in the context of other factors in system and network performance. The administrator also can monitor other mission-critical applications, such as SQL Server.

Windows PowerShell Integration

Windows PowerShell is an interactive command-line technology that also supports task-based scripting.

DPM provides its own set of Windows PowerShell commands that can be used for performing data protection management tasks. You access DPM cmdlets through DPM Management Shell.

A DPM administrator can use the cmdlets to perform all the administrative tasks that can be performed in the console, including sets of cmdlets designed to be used for the following tasks:

- To configure DPM
- To manage tapes and disks
- To manage protection groups
- To protect and recover data

In addition, the cmdlets enable administrators to perform the following tasks, which cannot be performed on the Administrator Console:

- To remove recovery points
- To customize the start time for library maintenance jobs, such as detailed inventory and cleaning
- To specify the local area network (LAN) configuration to be used for a backup job

Remote Administration

You can establish a Remote Desktop connection to a DPM server to manage DPM operations remotely.

DPM Management Shell can be installed on computers other than the DPM server, enabling you to administer multiple DPM servers remotely. You can also install DPM Management Shell on desktop computers running Windows XP or Windows Vista.

End-User Recovery

System Center 2012 – Data Protection Manager (DPM) allows you to protect your data on client computers. Client computers include desktop computers that are connected to the network, and laptop and notebook computers that are intermittently connected to your corporate environment. Backup administrators can centrally configure data protection for the client computers in their

environment using the DPM Client. Additionally, administrators can give their end users the ability to define and manage their own backups. DPM enables end users to perform their own recoveries by leveraging the Previous Versions feature in Windows.

See Also

Protection for clustered servers

Protecting workloads with DPM

Administrator Console Overview for DPM in System Center 2012

This section provides an overview of the System Center 2012 – Data Protection Manager (DPM) Administrator Console, including a console tour that describes the Administrator Console layout, and explains where you can find the controls for performing general tasks. It describes the five task areas of the Administrator Console, associated actions, and how you can use them to administer DPM.

Note
You must be a member of the local Administrators group to access the Administrator Console.

The Administrator Console is the central management tool for DPM, with a consolidated interface that gives you immediate access to the **Monitoring**, **Protection**, **Recovery**, **Reporting**, and **Management** task areas.

In This Section

About the DPM Administrator Console

Using DPM Administrator Console to administer DPM

Working with task areas

About the DPM Administrator Console

This topic describes the layout of the Administrator Console and explains where the controls for general tasks are located.

Navigation Bar

The navigation bar appears to the left side of the Administrator Console. It consists of five buttons – **Monitoring**, **Protection**, **Recovery**, **Reporting** and **Management**. Each of these buttons takes you to the respective workspace. The workspace takes up the largest area in the console. It shows you the objects you can work with for that function. It also changes the options available on the upper half of the Navigation bar.

Workspace

A *workspace* is a set of logically related objects.

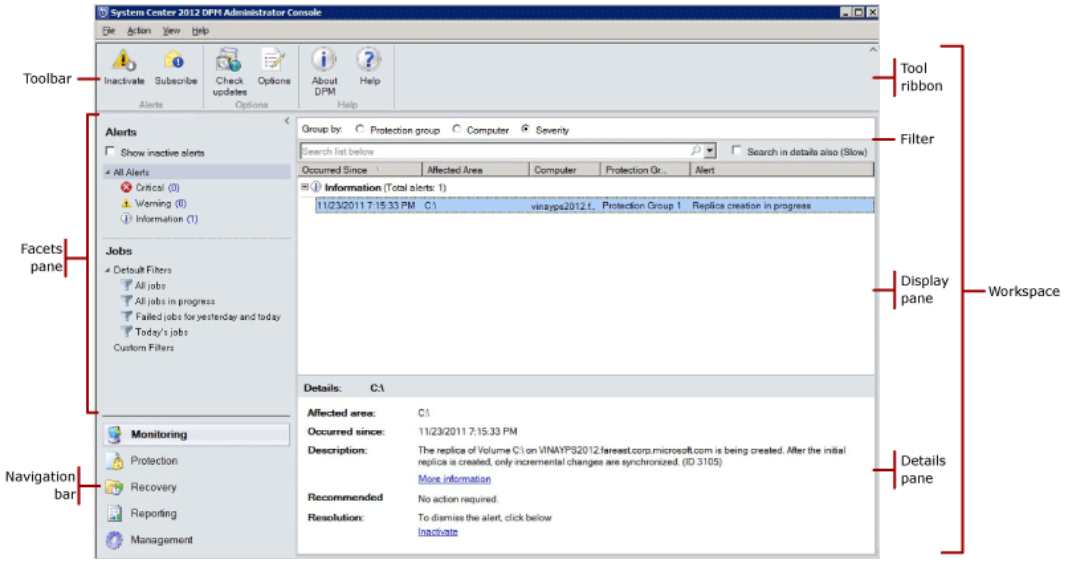
You can move from one workspace to the other using the navigation buttons.

The navigation pane for some workspaces allows you to look at various aspects of the objects. For example, when you are in the Monitoring workspace, you can view alerts or jobs using the Navigation pane

Following are descriptions of the type of information that appears in each pane:

- **Display pane**. Lists items associated with the current workspace. For example, the **Protection** workspace displays the names of protection groups and lists the members of those groups. The display pane for some task areas is subdivided into tabs that group subsets of functionality. The navigation pane for some workspaces allows you to look at various aspects of the objects. For example, when you are in the **Monitoring** workspace, you can view alerts or jobs using the Navigation pane
- **Details pane**. Provides details, such as properties and status information, for an item selected in the display pane. For example, the **Details** pane for the **Protection** task area displays status, recovery range, and other details about a selected protection group.
- **Tool ribbon**. The tool ribbon is a dynamic group of buttons which change based on the object you have selected. Using the buttons on the tool ribbon, you can carry out actions on the selected objects.

Layout of DPM Administrator Console



Menu Bar

The menu bar contains four menus: **File**, **Action**, **View**, and **Help**.

- **File menu**. Contains standard Microsoft Management Console (MMC) commands. For information about MMC, see MMC Help.
- **Action menu**. Contains the same commands as those displayed in the tool ribbon, as well as the **Help** command. The **Help** command provides access to both DPM Help and MMC Help.
- **View menu**. Provides an alternative method for moving between the task areas of the console, and a link to the DPM Community Web site.

- **Help menu**. Provides access to both DPM Help and MMC Help. To access DPM Help from this menu, click **Help Topics**, and then click **Data Protection Manager Help**. The **Help** menu also provides version information for MMC and abridged version information for System Center 2012 – Data Protection Manager (DPM).

Using DPM Administrator Console to administer DPM

To use the Administrator Console, you must be logged on to the DPM server with a domain account that is a member of the local Administrators group.

Note
You can also add DPM Administrator Console as a snap-in to a custom Microsoft Management Console (MMC). DPM Administrator Console is listed in the MMC Add/Remove Snap-in menu as System Center 2012 – Data Protection Manager (DPM).

DPM Administrator Console runs locally on the DPM server, but you can access the console remotely by using a Remote Desktop connection.

To run DPM Administrator Console on the DPM server

- On the **Start** menu, point to **All Programs**, point to **System Center 2012 – Data Protection Manager (DPM)**, and then click **System Center 2012 – Data Protection Manager (DPM)**.

  -Or-

  Double-click the **System Center 2012 – Data Protection Manager (DPM)** icon on the desktop.

Working with task areas

System Center 2012 – Data Protection Manager (DPM) Administrator Console contains five workspaces: **Monitoring**, **Protection**, **Recovery**, **Reporting**, and **Management**. The tool ribbon pane provides access to functionality associated with the current task and, in some cases, the item selected in the display pane.

The following table provides details about the actions that you can perform in each workspace.

Workspace	Actions
Monitoring	Use the **Monitoring** workspace to monitor the status of data protection, data recovery, and other DPM operations. The **Monitoring** workspace contains the following tabs: • **Alerts**—Displays errors, warnings, and informational messages. You can group alerts by protection group, computer, or severity, and you can choose to display

Workspace	Actions
	active alerts exclusively or to display both active alerts and a history of inactive alerts. You can also subscribe to notifications to receive alerts via e-mail. • **Jobs**—Displays the status of jobs and their associated tasks. You can group jobs by protection group, computer, status, or type, and you can filter jobs by time period. You can choose whether to include regularly scheduled synchronization operations in the list of jobs.
Protection	Use the **Protection** workspace to do the following: • Create, rename, and manage members of protection groups. • Manage protection schedules, disk allocations, and other options. • Run manual synchronization and consistency check jobs. • Manage recovery points. • Review and respond to results of Auto Discovery.
Recovery	Use the **Recovery** workspace to find and recover data from recovery points. The **Recovery** workspace contains the following tabs: • **Browse**—Enables you to browse for available recovery points by protected computer. • **Search**—Enables you to search for available recovery points based on data type, location, origin, and recovery point date.
Reporting	Use the **Reporting** workspace to do the following: • Generate and view reports on DPM operations. • Schedule automatic report generation. • Manage Reporting Services settings.

Workspace	Actions
Management	Use the **Management** workspace to manage protection agents, storage pool disks, and tape libraries. The **Management** workspace contains the following tabs: • **Agents**—Displays a list of protection agents deployed on computers and enables you to install, uninstall, and update the agents and agent licenses. • **Disks**—Displays a list of disks included in the storage pool and enables you to add and remove disks from the pool. • **Libraries**—Displays the tape libraries installed on the DPM server and enables you to manage the tapes in the library.

Product Support Overview for System Center 2012 - Data Protection Manager

Microsoft provides the following Web sites to help you learn about System Center 2012 – Data Protection Manager (DPM).

- To evaluate DPM as a potential solution for your data protection needs and to review news articles about recent data protection developments, see Microsoft System Center Data Protection Manager.
- For technical documentation to help you evaluate, plan, deploy, configure, operate, and troubleshoot DPM see System Center Data Protection Manager TechCenter.
- For answers to questions about DPM, search for “Data Protection Manager” at Microsoft Support Knowledge Base (KB).
- To find solutions to your technical problems, the latest news, key resources, and downloads and updates, or to contact a Microsoft support professional, see Microsoft Help and Support.

Communities

To share your experiences with other people who are using DPM, see the System Center Data Protection Manager Community.

To discuss DPM issues with other system administrators, Microsoft Most Valuable Professionals (MVPs), and Microsoft employees, search for “Data Protection Manager” at Microsoft Discussion Groups.

Planning a System Center 2012 - DPM Deployment

Before beginning to deploy System Center 2012 - Data Protection Manager (DPM) there are a number of planning steps you should complete.

- Plan for DPM server deployment—Decide how you'll deploy DPM servers—This includes the number of servers and their location, and the SQL Server database used by DPM.
- Plan for DPM storage—Determine the storage requirements you'll need to store replicas and recovery point for protected workloads.
- Plan for workload protection—Decide what workloads and applications you want to protect, plan for protection groups, and for backup and recovery.
- Plan for DPM security—Understand DPM security considerations, and learn about antivirus and firewall requirements, and the permissions model.

Plan for DPM server deployment

Planning deployment of your System Center 2012 - Data Protection Manager (DPM) servers includes a number of steps:

- Estimate how many DPM servers are required—Estimate how many DPM servers you need in accordance with data source limits, and learn about options for scaling DPM.
- Decide where to locate DPM servers—Learn about location requirements.
- Plan for the DPM SQL Server database—Learn about SQL Server options for the DPM database.

Estimate how many DPM servers are required

The number of System Center 2012 - Data Protection Manager (DPM) servers you'll need to deploy is based on the following factors:

- DPM limitations
- The workloads you want to protect
- How often data changes on protected workloads
- How often the data will be synchronized
- The amount of space in the storage pool
- Available bandwidth of each protected computer
- Aggregate bandwidth on the DPM server

DPM limitations

DPM imposes a number of limitations that will affect your deployment, including data size limits for different workloads, and snapshot limits.

Data limits for protected workloads

The following table lists the data source limits that a DPM server that meets the minimum hardware requirements can protect and the recommended disk space required per DPM server.

Data source	Data source limit per DPM server	Recommended disk space
SQL Server	Up to 2000 databases	80 TB
Client computers	3000 client computers	
Exchange Server		80 TB
SharePoint		25 TB

Snapshot limits

A DPM server can store up to 9,000 disk-based snapshots, including those retained when you stop protection of a data source. The snapshot limit applies to express full backups and file recovery points, but not to incremental synchronizations.

The snapshot limit applies per DPM server, regardless of storage pool size. When you configure protection groups, the DPM server is provisioned for the number of snapshots to accommodate the protection group configuration. You can use the following cmdlet in DPM Management Shell to identify the number of snapshots for which the server is provisioned:

$server=Connect-DPMServer *Name of the DPM server*

$server.CurrentShadowCopyProvision

When planning your DPM deployment, consider the snapshot limit as part of the DPM server capacity. The following table lists examples of the number of snapshots that result from different protection policies.

Protection policy	Snapshots
Exchange storage group: daily express full backup and 15-minute incremental synchronization with a retention range of 5 days	5
Volume on a file server: 3 daily recovery points with a retention range of 21 days	63
SQL Server database: 2 express full backups daily with a retention range of 14 days	28
Total:	**96**

Estimating the data change rate

To get an estimate of your data change rate, you can review an incremental backup for a recent, average day. The percentage of your data included in an incremental backup is usually indicative of your data change rate. For example, if you have a total of 100 GB of data and your incremental backup is 10 GB; your data change rate is likely to be approximately 10 percent per day.

However, because the method that DPM uses to record changes to data is different from that of most backup software, incremental backup size is not always a precise indicator of data change rate. To refine your estimate of your data change rate, consider the characteristics of the data you want to protect.

For example, while most backup software records data changes at the file level, DPM records changes at the byte level. Depending on the type of data that you want to protect, this can translate to a data change rate that is lower than the incremental backup might suggest.

Decide where to locate DPM servers

When considering locations for System Center 2012 - Data Protection Manager (DPM) deployment, note the following:

- DPM must be deployed in Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 or Windows Server 2003 Active Directory Domain Services (AD DS) to support its protection and recovery operations.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you must have a separate DPM server for each domain.
- DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2008 forest mode.

  When deciding where to locate your DPM server, consider the network bandwidth between the DPM server and the protected computers. If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM supports teamed network adapters (NICs) . Teamed NICs are multiple physical adapters that are configured to be treated as a single adapters by the operating system. Teamed NICs provide increased bandwidth by combining the bandwidth available using each adapter, and failover to the remaining adapter when an adapter fails. DPM can use the increased bandwidth achieved by using teamed adapter on the DPM server.
- Another consideration for the location of your DPM servers is the need to manage tapes and tape libraries manually, such as adding new tapes to the library or removing tapes for offsite archive.

Plan for the DPM SQL Server database

A System Center 2012 - Data Protection Manager (DPM) deployment requires an instance of SQL Server to host the DPM database. DPM in System Center 2012 can use the following versions of SQL Server:

- SQL Server 2012
- SQL Server 2008 R2 with SP1
- SQL Server 2008 R2

When you select a SQL Server during DPM installation, you can use either of the following:

- A existing local instance of SQL Server installed on the computer on which you are installing DPM—If you select to use a local instance during DPM Setup, a DPM account that does not expire will be created to run the required SQL Server and SQL Server Agent accounts.
- A remote instance of SQL Server—If you want to use a remote instance, note the following:
    - The server running SQL Server and the DPM server should be located in the same domain.
    - The remote instance of SQL should not be running on a domain controller.
    - The remote instance of SQL Server should be running the following components only:
        - SQL Server Database Engine
        - Reporting Services
    - The remote instance of SQL Server should not run as Local System.
    - Use the following SQL Server settings: default failure audit; enable password policy checking; default Windows Authentication mode.
    - Run SQL Server using a low-privileged domain user account.
    - For the DPM server to access a remote instance of SQL Server through Windows Firewall, on the remote computer, you must configure an incoming exception for sqlservr.exe for the specific instance that you use for the DPM database to allow use of the TCP protocol on port 80.
    - After the installation of SQL Server is complete, enable the TCP/IP protocol for the specific instance that you use for the DPM database.

After installation, your DPM database will be named DPMDB_<DPMServername> or DPMDB_<DPMServername><GUID>.

Plan for DPM storage

System Center 2012 - Data Protection Manager (DPM) offers a number of storage options for backing up protected workloads:

- Back up from disk of protected computer to tape—You can back up data from a protected computer disk directly to tape.
- Back up from disk of protected computer to another disk—This solution backs up data from a protected computer to another hard disk. You then can further back up the second disk to tape.
- Backup to the cloud using Windows Azure Backup

The following table compares the advantages and disadvantages of tape and disk-based protection.

Method	Advantages	Disadvantages	When to use
Disk	• Speed of data recovery • Speed of data backup. • Ability to have redundancy to handle failure using technologies such as RAID. • Less manual intervention, such as changing tapes.	• Disks are not a simple solution for archive needs, because of the cost of disks and the inconvenience of storing offsite. • Maximum retention for disk is 448 days.	• For short-term storage • When you have a limited data loss tolerance. • When you need faster recovery times
Tape	• Can be stored offsite for security and as a contingency for disaster recovery. • Easy to increase capacity by adding more tapes.	• Slower and more cumbersome recovery process. • Might require manual intervention such as manual tape rotations. • Requires a compatible tape library. For a list of these see Compatible Tape Libraries for System Center 2012 DPM in the TechNet wiki.	• For long-term storage, or for lengthy short-term storage. • When recovery time objective (RTO) is generous. • For data that doesn't change frequently and thus doesn't require frequent backup.

For an overview of all methods, see Backup options.

Selecting a backup method

These backup methods should be used in accordance with your backup requirements, as summarized in the following table.

Type of protection	Disk storage	Tape storage	Windows Azure Backup	
Short-term	Yes	Yes	Yes	

Type of protection	Disk storage	Tape storage	Windows Azure Backup	
protection				
Long-term protection	No	Yes	No	Maximum retention in Windows Azure Backup is 120 days. This setting is dependent upon synchronization settings. If you backup twice a day then retention is 60 days. Windows Azure Backup synchronize is up to twice a day.
Offsite protection	No	Yes	Yes	
Protected workloads	Files, SQL Server, Exchange, SharePoint, Hyper-V, system state, clients	Files, SQL Server, Exchange, SharePoint, Hyper-V, system state, clients	Files, SQL Server, Hyper-V	

See Also

Plan for disk-based backups

Plan for tape-based backups

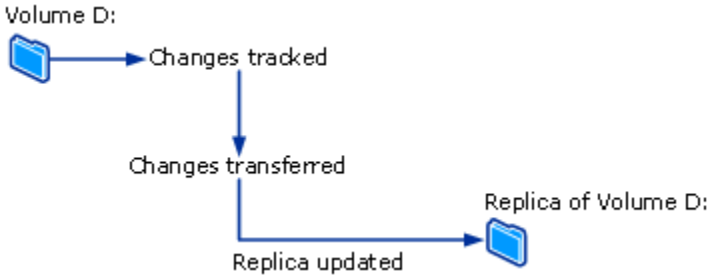
Plan for disk-based backups

To provide disk-based protection the DPM server creates and maintains a replica of protected workload data, and saves it to the DPM storage pool. The storage pool is a set of disks or volume that you set up as part of the DPM server configuration. DPM creates recovery points (snapshots) that are a point-in-time copy of a replica stored in a storage pool. DPM synchronizes by transferring data changes from a data source to a DPM server, and then applies the changes to the replica. DPM can perform incremental synchronization that checks what's changed and updates the replica, or synchronization with a consistency check which is the same as an incremental synchronization with an additional block-level check of the replica to verify data consistency. For more information, see Plan the storage pool.

Synchronize file data

In DPM, for a file volume or share on a server, the protection agent uses a volume filter and the change journal to determine which files have changed, and then performs a checksum procedure for these files to synchronize only the changed blocks. During synchronization, these changes are transferred to the DPM server and then applied to the replica to synchronize the replica with the data source. The following figure illustrates the file synchronization process.

File Synchronization Process



If a replica becomes inconsistent with its data source, DPM generates an alert that specifies which computer and which data sources are affected. To resolve the problem, the administrator repairs the replica by initiating synchronization with a consistency check on the replica. During the consistency check, DPM performs a block-by-block verification and repairs the replica to bring it back into consistency with the data source.

You can schedule a daily consistency check for protection groups or initiate a consistency check manually.

At regular intervals that you can configure, DPM creates a *recovery point* for the protection group member. A recovery point is a version of the data from which data can be recovered. For files, a recovery point consists of a shadow copy of the replica, which is created by using the Volume Shadow Copy Service (VSS) functionality of the operating system on the DPM server.

Synchronize application data

For application data, after the replica is created by DPM, changes to volume blocks that belong to application files are tracked by the volume filter.

How changes are transferred to the DPM server depends on the application and the type of synchronization. The operation that is labeled *synchronization* in DPM Administrator Console is analogous to an incremental backup, and it creates an accurate reflection of the application data when combined with the replica.

During the type of synchronization that is labeled *express full backup* in DPM Administrator Console, a full Volume Shadow Copy Service (VSS) snapshot is created but only changed blocks are transferred to the DPM server.

Each express full backup creates a recovery point for application data. If the application supports incremental backups, each synchronization also creates a recovery point. The synchronization type supported by each type of application data is summarized as follows:

- For protected Exchange data, synchronization transfers an incremental VSS snapshot using the Exchange VSS writer. Recovery points are created for each synchronization and express full backup.
- SQL Server databases that are log-shipped, in read-only mode, or that use the simple recovery model do not support incremental backup. Recovery points are created for each express full backup only. For all other SQL Server databases, synchronization transfers a transaction log backup, and recovery points are created for each incremental synchronization and express full backup. The transaction log is a serial record of all the transactions that have been performed against the database since the transaction log was last backed up.
- Windows SharePoint Services and Microsoft Virtual Server do not support incremental backup. Recovery points are created for each express full backup only.

Incremental synchronizations require less time than performing an express full backup. However, the time required to recover data increases as the number of synchronizations increases. This is because DPM must restore the last full backup and then restore and apply all the incremental synchronizations up to the point in time selected for recovery.

To enable faster recovery time, DPM regularly performs an express full backup, a type of synchronization that updates the replica to include the changed blocks.

During the express full backup, DPM takes a snapshot of the replica before updating the replica with the changed blocks. To enable more frequent recovery point objectives, as well as to reduce the data loss window, DPM also performs incremental synchronizations in the time between two express full backups.

As with the protection of file data, if a replica becomes inconsistent with its data source, DPM generates an alert that specifies which server and which data source are affected. To resolve the problem, the administrator repairs the replica by initiating a synchronization with consistency check on the replica. During a consistency check, DPM performs a block-by-block verification and repairs the replica to bring it back into consistency with the data sources.

You can schedule a daily consistency check for protection groups or initiate a consistency check manually.

Plan for tape-based backups

When you configure backup methods, you can only specify to use tape for long-term protection. None of the other methods are currently suitable for long-term backup. For short-term protection you can also select to use tape backups. With these settings enabled DPM backs up the data directly from the protected computer to tape. Note the following:

- For long-term protection to tape full backups are always used.
- For short-term protection to tape you can use a full backup or a full/incremental backup (when backups are set to **Daily**).
- If you don’t have a tape or tape library attached to the DPM server you’ll only be able to select **Disk** for short-term protection.
- When protecting client computers you can only use **Disk** for short-term protection.

- If you're using tape for both long-term and short-term protection, DPM creates copies of the latest short-term full backup in order to generate the long-term tape backup. We recommend that you schedule the short-term protection backup to run a day before the long-term backup. That way you can be sure you're using the latest short-term backup in order to create the long-term backup.
- If you're using disk for short-term back up and tape for long-term, the long-term backup will be taken from the disk replica.

Tape library requirements

DPM can backup to tape libraries or standalone tape drives. These must be attached to the DPM server with storage area network (SAN) or SCSI. The tape capacity you need will depend on the size of the protected data and the number of tape backup jobs you'll need to run. To plan for the number of tapes required for a protection group, multiply the required backup frequency by the retention range (specifies from how far back data can be recovered).

For a list of compatible tape libraries, see Compatible Tape Libraries for System Center 2012 DPM in the TechNet wiki.

Long-term storage requirements

Long-term backups to tape allocate a tape for each full backup job, so that each long-term backup recovery point is always on a new tape. Available free tapes are decremented as tapes are allocated to long-term or short-term backup. If no new tape is available for a long-term backup an alert is issued.

Short-term storage requirements

If short-term backups are configured to use tape and the full backup option is used, each full backup job will require a new free tape.

If short-term backups are configured to use tape and the full/incremental option is used, the full backups will require a new free tape, and the incremental backups will be appended to a single separate tape.

Example: If a full backup to tape is scheduled weekly and incremental backups to tape are scheduled daily, then the first full backup will go to a new free tape and all subsequent incremental backups will be appended to another new free tape. If a full backup job fails before it completes, all subsequent incremental jobs will use the existing tape that has valid previous incremental backups.

If you trigger two different "create recovery point (tape)" actions for two protection group members, DPM create two tape backup jobs, and two tapes will be required. If you trigger a single "create recovery point (tape)" action for two protection group members, a single tape it used. This ensure that data for selected protection group members is collocated for ad-hoc backups to the same tape.

Freeing up tapes

You can't free up or erase a tape that contains valid recovery points from any data source. To free up a tape you must either removes the sources from the protection group and expiry recovery points on the tape, or modify the protection group settings to clear tape protection. Then you'll need to select to **Remove inactive protection** for previously protected data.

To restore data from an expired tape you'll need to mark the tape as free and then unmark it, and then recatalog the tape.

Standalone tape drives

If you're using a standalone tape drive all short-term backups are appended to a single tape. All long-term backups are appended to a single that that is different from the short-term backup tape.

See Also

Plan for disk-based backups

Compatible tape libraries

The latest list of compatible tape libraries for System Center 2012 – Data Protection Manager (DPM) DPM is located in the TechNet Wiki.

For more information about methods used to verify compatibility, see Verifying tape library compatibility.

Verifying tape library compatibility

Windows 2008 provides a tape library compatibility certification test. This is no longer provided for Windows 2012. However, if the tape for which you want to verify compatibility is listed in the Windows Server Catalog in the Hardware, Storage section, and is shown as compatible with Windows 2008 64-bit, or Windows 2008 it will probably work with DPM. Note that any driver incompatibilities with Windows 2012 would need to be addressed by the vendor.

In addition, you can use the System Center Data Protection Manager Tape Library Compatibility Test tool to check whether your tape library is compatible with DPM. This tool runs a set of standard tests on your standalone tape or tape library.

Obtain and use the tool as follows:

1. Download the DPM Tape Library Compatibility Test tool from Download DPM Tape Library Compatibility Test Tool.
2. Extract the files in the compressed folder to a folder on your computer.
3. Before you run the tool, do the following:
    - Ensure your target tape library and tape drives are visible in Device Manager.
    - Insert a read/write data tape in slot 0. The contents of this tape will be overwritten.
    - Insert a cleaning tape in slot 1. The tapes must be in consecutive slots, failing which there should be no tapes in the slots between the tapes. The data tape is in a slot preceding the cleaning tape.N

4. Run the tool as follows:
    a. Open an elevated command prompt.
    b. Change your current folder to the one where you extracted the tool.
    c. To check that the tape is visible to the tool, type **DPMLibraryTest.exe /CERTIFY /LL**
    d. To certify as follows:
        - To certify a tape library, type **DPMLibraryTest.exe /CERTIFY /TL** <tape library name> **/AT**
        - To certify a standalone tape drive, type **DPMLibraryTest.exe /CERTIFY /TL** <device name> **/SA**
    e. The tool runs the following tests:
        - Test 1: Basic configuration—This test scans the system for attached devices, and identifies standalone tape drives and tape libraries. The tool provides a summary at the end of the test. For each device you'll see a Device Name, Serial Number, Vendor Name, Product Name, Firmware Revision, and SCSI properties. You should verify that the summary information is correct. If there are errors check the following:
            - Check all devices are listed in Device Manager.
            - Ensure that device drivers are up-to-date.
            - If the drive mappings are incorrect, use the DPMDriveMapping.exe tool in the <DPM installation folder>/bin folder to correct the mappings. If you do not have DPM installed on the computer, copy the DPMLA.xml that DPMDriveMapping.exe creates to the folder to which you extracted the Tape Library Certification tool.
        - Test 2: Mount/dismount—This test selects a tape from the first available slot and performs a mount///dismount of the tape to and from a drive.
        - Test 3: Drive cleaning—This test performs a cleaning test using the cleaning tape. If you are using Firestreamer to a VTL where you can't remove or change tapes, use the /ST flag syntax to skip this test.
        - Test 4: I/E media—This test selects the first available tape and moves it to the I/E port and back. If your library/VTL doesn't have I/E ports, the tool will automatically skip the test.
        - Test 5: I/O—This test selects the first writable tape, writes a few buffers to it, and then attempts to read what's been written. This test only checks read/write capabilities. Any specific errors in the drive should be inspected using the advanced mode.
5. After the tool completes the test, log information will be provided in the LibraryTestTool-*Curr.errlog files located in the folder from which you ran the tool.

Tool syntax

The syntax for the tool is:

```
DPMLibraryTest.exe /CERTIFY /<switch_1> [/switch_2]
```

Switch	Description
/LL	List available tape libraries and drives.
/LT	List all test cases.
/TL	Test a particular library.
/AT	Run all test cases.
/ST	Run specific tests.
/SA	Run standalone drive test cases.
/EX	Show examples.
/Help or /?	Show help.

Examples

Example	Command
List all available libraries.	DPMLibraryTest.exe /CERTIFY /LL
Run all tests on a physical library.	DPMLibraryTest.exe /CERTIFY /TL \\.\Changer0 /AT
Run only tests 3 and 4 on a physical library.	DPMLibraryTest.exe /CERTIFY /TL \\.\Changer0 /ST 3 4
Run all tests except cleaner test.	DPMLibraryTest.exe /CERTIFY /TL \\.\Changer0 /ST 1 2 4 5
Standalone drive test.	DPMLibraryTest.exe /CERTIFY /TL \\.\Tape21745678 /SA

Plan the storage pool

The storage pool is a set of disks on which the DPM server stores the replicas and recovery points for the protected data. You can use any of the following for the storage pool:

- Direct attached storage (DAS)
- Fiber Channel storage area network (SAN)
- iSCSI storage device or SAN

Note the following:

- The storage pool supports most disk types, including Integrated Drive Electronics (IDE), Serial Advanced Technology Attachment (SATA), and SCSI, and it supports both the master boot record (MBR) and GUID partition table (GPT) partition styles. We strongly recommend that you use GPT disks for the DPM storage pool.

- If you use a SAN for the storage pool, we recommend that you create a separate zone for the disk and tape used on DPM. Do not mix the devices in a single zone.
- You cannot add USB/1394 disks to the DPM storage pool.
- You cannot use Storage Spaces for the DPM disk storage pool.
- Some original equipment manufacturers (OEMs) include a diagnostic partition that is installed from media that they provide. The diagnostic partition might also be named the OEM partition, or the EISA partition. EISA partitions must be removed from disks before you can add the disk to the DPM storage pool.
- You can also substitute custom volumes that you define in Disk Management for volumes in the storage pool.

Planning the storage pool involves the following:

- Calculate capacity requirements
- Plan the disk configuration
- Define custom volumes

DPM

Calculate capacity requirements

Capacity requirements for the DPM storage pool are variable and depend primarily on the size of the protected data, the daily recovery point size, expected volume data growth rate, and retention range objectives.

Daily recovery point size refers to the total size of changes made to protected data during a single day. It is roughly equivalent to the size of an incremental backup. Retention range refers to the number of days for which you want to store recovery points of protected data on disk. For files, DPM can store a maximum of 64 recovery points for each volume included in a protection group, and it can create a maximum of 8 scheduled recovery points for each protection group each day.

Note
The limit of 64 recovery points for files is a result of the limitations of the Volume Shadow Copy Service (VSS), which is necessary for the end-user recovery functionality of DPM. The recovery point limit does not apply to application data.

In general, we recommend making the storage pool two times the size of the protected data for protection of files. This recommendation is based on an assumed daily recovery point size of approximately 10 percent of the protected data size and a retention range of 10 days (two weeks, excluding weekends).

If your daily recovery point size is larger or smaller than 10 percent of your protected data size, or if your retention range objectives are longer or shorter than 10 days, you can adjust the capacity requirements for your storage pool accordingly.

Regardless of how much capacity you decide to allow for the storage pool in your initial deployment, we recommend that you use extensible hardware so that you have the option of adding capacity should the need arise.

The sections that follow provide guidelines for determining your daily recovery point size and retention range objectives.

Estimating Daily Recovery Point Size

Our recommendation to make the storage pool two times the size of the protected data assumes a daily recovery point size of 10 percent of the protected data size. Daily recovery point size is related to data change rate and refers to the total size of all recovery points created during a single day. To get an estimate of the daily recovery point size for your protected data, you can review an incremental backup for a recent, average day. The size of the incremental backup is usually indicative of the daily recovery point size. For example, if the incremental backup for 100 GB of data includes 10 GB of data, your daily recovery point size will probably be approximately 10 GB.

Determining Retention Range Objectives

Our recommendation to make the storage pool two times the size of the protected data assumes a retention range objective of 10 days (two weeks, excluding weekends). For the typical enterprise, requests for recovery of data are concentrated within two to four weeks after data loss events. A retention range of 10 days provides for recovery of data up to two weeks after a data loss event.

The longer your retention range objective, the fewer recovery points you can create each day. For example, if your retention range objective is 64 days, you can create just one recovery point each day. If your retention range objective is eight days, you can create eight recovery points each day. With a retention range objective of 10 days, you can create approximately six recovery points each day.

Plan the disk configuration

If you are using direct-attached storage for the DPM storage pool, you can use any hardware-based configuration of redundant array of independent disks (RAID), or you can use a "just a bunch of disks" (JBOD) configuration. Do not create a software-based RAID configuration on disks that you will add to the storage pool.

To decide on the configuration for the disks, consider the relative importance of capacity, cost, reliability, and performance in your environment. For example, because JBOD does not consume disk space for storing parity data, a JBOD configuration makes maximum use of storage capacity. For the same reason, the reliability of JBOD configurations is poor; a single disk failure inevitably results in data loss.

For the typical DPM deployment, DPM recommends a RAID 5 configuration, which offers an effective compromise between capacity, cost, reliability, and performance.

To help you evaluate options for configuring the disks in your storage pool, the following table compares the trade-offs between JBOD and the various levels of RAID, on a scale from 4 (very good) to 1 (acceptable).

Comparison of Configuration Options for Storage Pool Disks

Disk Configuration	Capacity	Cost	Reliability	Performance and Scalability
JBOD	4	4	1	4
RAID 0	4	4	1	4
RAID 1	1	1	4	3
RAID 5	3	3	3	3
RAID 10	1	1	4	4

For more information about RAID, see Achieving Fault Tolerance by Using RAID.

Define custom volumes

In System Center 2012 – Data Protection Manager (DPM), you can assign a *custom volume* to a protection group member, in place of the DPM storage pool. A custom volume is a volume that is not in the DPM storage pool and is specified to store the replica and recovery points for a protection group member.

Although the DPM-managed storage pool is sufficient for most business needs, you might want a greater amount of control over storage for specific data sources. For example, you have critical data that you want to store using a high-performance logical unit number (LUN) on a storage area network.

Any volume that is attached to the DPM server can be selected as a custom volume in the Create New Protection Group Wizard, except the volume that contains the system and program files. To use custom volumes for a protection group member, two custom volumes must be available: one volume to store the replica and one volume to store the recovery points.

DPM cannot manage the space in custom volumes. If DPM alerts you that a custom replica volume or recovery point volume is running out of space, you must manually change the size of the custom volume by using Disk Management.

You cannot change the selection of storage pool or custom volume for a protection group member after the group is created. If you must change the storage location for a data source's replica or recovery points, you can do so only by removing the data source from protection and then adding it to a protection group as a new protection group member.

Plan for workload protection

System Center 2012 - Data Protection Manager (DPM) protects workloads, including client computers, servers, file servers, and Microsoft applications. To create an effective plan for deploying System Center 2012 – Data Protection Manager (DPM), you must carefully consider your organization's requirements for data protection and recovery against the capabilities of DPM.

To plan for workload protection, do the following:

1. Identify workloads and applications that DPM can protect. For more information, see Support Matrix for DPM Protection.
2. Read the topics in this section to understand which data can be protected:
   - Plan for file data protection on computers and servers
   - Plan for Exchange data protection
   - Plan for SharePoint data protection
   - Plan for cluster data protection
   - Plan for system state protection
   - Plan for Hyper-V virtual machine protection

Plan for file data protection on computers and servers

On client computers and servers System Center 2012 - Data Protection Manager (DPM) can protect files in volumes, folders, and shares. Note the following:

- For a list of supported client and server operating systems, see Support Matrix for DPM Protection.
- For computers running client operating systems, you can back up file data in volumes (accessed through drive letters or mount points), folders, and shares. You can't backup system state using DPM, but as a workaround you can run a Complete PC Back up to a folder or network share and protect files on the share using DPM. Windows Backup can be configured from **Backup and Restore** in the Control Panel.
- For computers running server operating systems, you can back up file data in volumes (accessed through drive letters or mount points), folders, and shares; and system state.
- Before you can protect a file server running Windows Server 2008 R2, you must apply the update described in Microsoft article 977381.
- From DPM SP1 onwards deduplicated volumes can be protected. When you configure protection for a full volume that is deduplicated, recognizes that it is a deduplicated volume and copies the content efficiently, providing network and storage saving. For more information, see SC2012 SP1 – DPM: Efficient Protection of Windows 2012 Dedup Volume.
- Computers running client operating systems that you want to protect must have a two-way trust relationship with the domain in which the DPM server is located.
- If Windows Firewall is running on client computers, the DPM protection agent will configured the required firewall exceptions. If you need to reset the firewall at any time, running SetDPMServer.exe. If you're running any other firewall ensure the ports required for DPM are open.
- In addition to protecting client computers in the corporate network, DPM can back up client computers using a VPN connection. VPN protocols PPTP, SSTP, and L2TP are supported. To perform backups over VPN, ICMP must be enabled.

Unprotected data

There are a number of resources on client computers and servers that are not protected by DPM:

- Volumes that aren't formatted with NTFS. To protect FAT or FAT32 volumes, you must convert them to NTFS. For instructions, see How to Convert FAT Disks to NTFS (http://go.microsoft.com/fwlink/?LinkId=83022).
- Volumes that are less than 1 GB in size. This is because DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of protected data and VSS only creates a snapshot when the volume size is equal to or greater than 1 GB.
- Hard links
- Recycle Bin
- Paging files
- System Volume Information folder. To protect system information for a computer, you'll need to select the computer's system state as a protection group member when you create a protection group.
- Files with any of the following combinations of file attributes: Encryption and reparse, Single instance Storage (SIS), case sensitivity, or sparse; Case sensitivity and SIS, sparse and resparce, or compression and SIS.

Excluding files from protection

The simplest approach to selecting data for protection is to select all file data for protection. Alternatively, you can select only specific subsets of your data for protection by excluding specific folders or file name extensions.

When deciding what to protect consider how important it is for you to quickly recover point-in-time copies of the data if data is lost or corrupted. Key candidates for protection are files that change frequently, or files with high business impact. Other good candidates are files that are frequently accessed, regardless of how often they change.

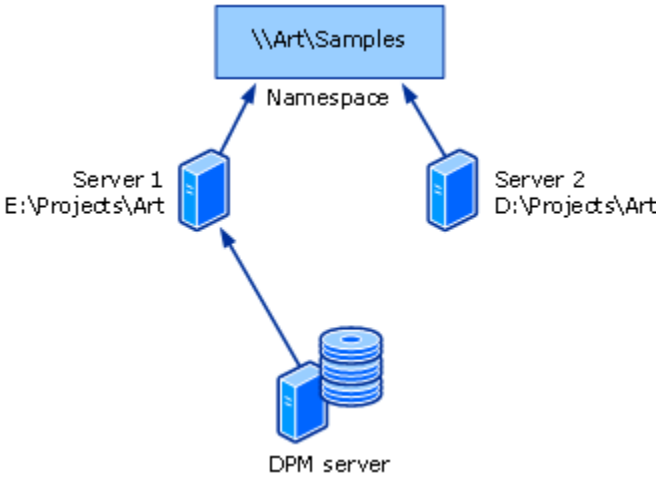
Protecting data in DFS namespaces

You can protect data that is part of a Distributed File System (DFS) Namespaces hierarchy. However, you cannot select shares for protection through the DFS Namespaces hierarchy. Instead, you can select shares for protection only by their target paths.

If your namespace includes roots or links that have multiple targets with the same data, we recommend that you protect only one of the targets. Protecting multiple targets with the same data is redundant.

The following illustration shows DPM protection of a DFS Namespaces target.

Protecting a DFS Namespaces Target by Using DPM



When end-user recovery is enabled for a protected target, users can access previous versions of files through the DFS Namespaces hierarchy. When end users attempt to access previous versions of files on a share that has multiple targets, DPM transparently directs them to the protected target.

Plan for Exchange data protection

System Center 2012 - Data Protection Manager (DPM) can protect Microsoft applications, including Exchange.

For a list of the Exchange versions that DPM 2012 can support, see Support Matrix for DPM Protection.

Protecting Exchange data

DPM 2012 protects the following Exchange data:

Version	Protectable data
Exchange 2013	Standalone Exchange 2013 servers Databases under a database availability group (DAG)
Exchange 2010	Standalone Exchange 2010 servers Databases under a database availability group (DAG)
Exchange 2007	Storage group

Note the following:

- You can’t exclude any database in selected storage groups for protection.
- You should disable circular logging for protected storage groups.

- Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006.
- Install the Exchange Server management tools on the DPM server.Ensure you install the management tools for the latest version of Microsoft Exchange that you are protecting. For example, if one of your mail servers is running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2010, you must install the management tools for Exchange 2010.
- The eseutil.exe and ese.dll versions that are installed on the Exchange Server must be the same versions as those installed on the DPM server. For example, if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll.

  If eseutil.exe and ese.dll are updated on the Exchange Server after applying an upgrade or update, update them on the DPM For more information about updating eseutil.exe and ese.dll, see Eseutil.exe and Ese.dll. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll:

  a. At the command prompt, navigate to the <DPM installation folder>\Bin directory,
  b. Type the fsutil command as follows to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>**

     On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe**"

Plan for SharePoint data protection

System Center 2012 - Data Protection Manager (DPM) can protect Microsoft applications, including SharePoint.

For a list of the SharePoint versions that DPM 2012 can support, see Support Matrix for DPM Protection.

Protecting SharePoint data

DPM 2012 protects the following SharePoint data:

Version	Protectable data
SharePoint 2013 SharePoint 2010 SharePoint 2007 Windows SharePoint Server 3.0	Farm SharePoint search Frontend Web server content

Note the following:

- Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422

- If you use the Office SharePoint Server Search service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply updated in Microsoft KB articles:
  - 951695
  - 941422

Plan for SQL Server data protection

System Center 2012 - Data Protection Manager (DPM) can protect Microsoft applications, including SQL Server.

For a list of the SQL Server versions that DPM 2012 can support, see Support Matrix for DPM Protection.

Protecting SharePoint data

DPM 2012 protects the following SharePoint data:

Version	Protectable data
SQL Server 2012 SQL Server 2008 R2 SQL Server 2008	Database

Note the following:

- If you have a database with files on a remote file share, protection will fail with Error ID 104. DPM does not support protection for SQL Server data on a remote file share.
- DPM cannot protect databases that are stored on remote SMB shares.
- Ensure that the availability group replicas are configured as read-only.
- You must explicitly add the system account NTAuthority\System to the Sysadmin group on SQL Server.
- When you perform an alternate location recovery for a partially contained database, you must ensure that the target SQL instance has the Contained Databases feature enabled.

Protect SQL Server with AlwaysOn enabled

SQL Server 2012 introduces a new high availability feature, named AlwaysOn. You can add your databases to Availability Groups, which are basically containers for databases that are configured for failover. System Center 2012 SP1 DPM supports protection of databases that are part of Availability Groups. The salient features of the DPM support for the AlwaysOn feature are:

- DPM detects Availability Groups when running inquiry at protection group creation.
- DPM detects a failover and continues protection of the database.
- DPM supports multi-site cluster configurations for an instance of SQL Server.

When you protect databases that use the AlwaysOn feature, DPM has the following limitations:

- DPM will honor the backup policy for availability groups that is set in SQL Server based on the backup preferences, as follows:
  - Prefer secondary—Backups should occur on a secondary replica except when the primary replica is the only replica online. If there are multiple secondary replicas available then the node with the highest backup priority will be selected for backup. In the case that only primary replica is available then backup should occur on the primary replica.
  - Secondary only—Backup shouldn't be performed on the primary replica. If the primary replica is the only one online, the backup shouldn't occur.
  - Primary—Backups should always occur on the primary replica.
  - Any Replica—Backups can happen on any of the availability replicas in the availability group. The node to be backed up from will be based on the backup priorities for each of the nodes.
- Note the following:
  - Backups can happen from any readable replica i.e. primary, synchronous secondary, asynchronous secondary.
  - If any replica is excluded from backup, for example Exclude Replica is enabled or is marked as not readable, then that replica will not be selected for backup under any of the options.
  - If multiple replicas are available and readable then the node with the highest backup priority will be selected for backup.
  - If the backup fails on the selected node then the backup operation fails.
  - Recovery to the original location is not supported.

See Also

Protecting Data in DFS Namespaces

Unsupported Data Types

Plan for Hyper-V virtual machine protection

System Center 2012 - Data Protection Manager (DPM) can protect Microsoft applications, including Hyper-V

For a list of the Hyper-V versions that DPM 2012 can support, see Support Matrix for DPM Protection.

Protecting Hyper-V virtual machines

DPM 2012 protects the following Hyper-V data:

Version	Protectable data
Hyper-V on Windows Server 2012 R2 Hyper-V on Windows Server 2012	Standalone Hyper-V host servers Clustered Hyper-V host servers/Cluster Shared

Hyper-V on Windows Server 2008 R2 Hyper-V on Windows Server 2008	Volumes (CSVs)

Note the following:

- DPM supports both host-based protection for Hyper-V where the agent is installed on the host computer, and guest-based where the agent is installed directly on the virtual machine.
- For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB 975354.
- For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in 975921.
- Before you can protect a computer running Windows Server 2008 with Hyper-V, apply the updates described in Microsoft articles 948465 and 948465.971394.

Plan for cluster data protection

System Center 2012 - Data Protection Manager (DPM)DPM can protect data that resides on shared disk clusters for the following applications

- File servers
- SQL Server
- Hyper-V
- Exchange Server

DPM can protect non-shared disk clusters for supported Exchange Server versions (cluster continuous replication), and can also protect Exchange Server configured for local continuous replication.

Plan for system state protection

DPM can protect the system state for any computer on which a DPM protection agent can be installed, except client computers.

Workstation and Member Server System State

When DPM backs up the system state of a workstation or member server, the following components are protected:

- The boot files
- The COM+ class registration database
- The registry
- System files that are under Windows File Protection

Domain Controller System State

When DPM backs up the system state of a domain controller, the following components are protected:

- Active Directory Domain Services (NTDS)
- The boot files
- The COM+ class registration database
- The registry
- The system volume (SYSVOL)

Certificate Services System State

When DPM backs up the system state of a member server or domain controller with Certificate Services installed, Certificate Services is protected in addition to the member server or domain controller system state components.

Cluster Server System State

When DPM backs up the system state of a cluster server, the cluster service metadata is protected in addition to the member server system state components.

Plan for protection groups

In System Center 2012 - Data Protection Manager (DPM) you organize workloads and resources you want to protect into *protection group*. A protection group is a collection of data sources that share the same protection configuration and settings.

A is

To plan a protection group, you must make the following decisions:

- Which data sources will belong to the protection group?
- Which protection method (disk-based, tape-based, or both) will you use for the protection group?
- What are your recovery goals for the members of the protection group?
- How much storage space will be needed to protect the selected data?
- Which tape and library should be used?
- What method will you use to create the replica for the members of the protection group?

The topics in this section provide guidelines for making the decisions involved in creating a protection group.

Guidelines for planning protection groups

As you design the structure of your protection groups, keep the following guidelines and restrictions in mind:

- Data sources on a computer must be protected by the same DPM server. In DPM, a data source is a volume, share, database, or storage group that is a member of a protection group.
- You can include data sources from more than one computer in a protection group.

- Protection group members cannot be moved between protection groups. If you decide later that a protection group member needs to be in a different protection group, you must remove the member from its protection group and then add it to a different protection group.
- If you determine that the members of a protection group no longer require protection, you can stop protection of the protection group. When you stop protection, your options are to retain protected data or to delete protected data.
    - **Retain protected data option**: Retains the replica on disk with associated recovery points and tapes for the specified retention range.
    - **Delete protected data option**: Deletes the replica on disk and expires data on the tapes.
- When you select a parent folder or share, its subfolders are automatically selected. You can designate subfolders for exclusion and also exclude file types by extension.
- Verify that you do not have more than a 100 protectable data sources on a single volume. If you do, distribute your data sources across more volumes if possible.
- All protection group members of the same type (file or application data) will have the same recovery goals. However, within the same protection group, files can have different recovery goals than application data.

  Exception: If a SQL Server database is configured to use the Simple Recovery Model or is the primary database in a log shipping pair, the recovery goals for that database will be configured separately from the recovery goals for all other application data.
- When you select a data source that contains a reparse point (mount points and junction points are data sources that contain reparse points), DPM prompts you to specify whether you want to include the target of the reparse point in the protection group. The reparse point itself is not replicated; you must manually re-create the reparse point when you recover the data.

Special considerations for protecting data over a WAN

Network bandwidth usage throttling and on-the-wire compression are performance optimization features that are particularly important for deployments in which a DPM server protects data over a wide area network (WAN) or other slow network.

On-the-wire compression is configured at the protection-group level.

Network bandwidth usage throttling is configured at the protected-computer level. In addition, you can specify different network bandwidth usage throttling rates for work hours, non-work hours, and weekends, and you define the times for each of those categories.

When protecting application data such as Exchange storage groups or SQL Server databases over a WAN, consider reducing the schedule for express full backups.

Selecting protection group members

There are several approaches you can take to organize data sources into protection groups, including the following:

- **By computer**, with all data sources for a computer belonging to the same protection group.
    - An advantage of this approach is that with all data from a computer in the same protection group, you have a single point of adjustment for performance loads.

    - A constraint of this approach is that all data sources of a type on that computer must be assigned the same recovery goals.
- **By data type**, separating files and each application data type into different protection groups.
    - An advantage of this approach is that you can manage data types as a group.
    - A constraint of this approach is that recovering a server can require multiple tapes from several protection groups.

By definition, all members of a protection group share recovery goals—that is, all data sources of a type in a protection group must have the same retention range and data loss tolerance.

If you have only a single stand-alone tape, use a single protection group to minimize the effort to change tapes. Multiple protection groups require a separate tape for each protection group.

Allocating space for protection groups

When you create a protection group and select disk-based protection, you must allocate space on the storage pool for the replicas and recovery points for each data source that you have selected for membership in the group, and you must allocate space on protected file servers or workstations for the change journal.

DPM provides default space allocations for the members of the protection group. The following table shows how DPM calculates the default allocations.

How DPM Calculates Default Space Allocations

Component	Default Allocation	Location
Replica volume	For files: • (Data source size x 3) / 2 For Exchange data: • Data source size x (1 + log change) / (alert threshold - .05) For SQL Server data: • Data source size x (1 + log change) / (alert threshold - .05) For Windows SharePoint Services data: • Total size of all databases/ (alert threshold - .05) For Virtual Server data: • Data source size x 1.5 For system state: • (Data source size x 3) / 2	DPM storage pool or custom volume

Component	Default Allocation	Location
	For Hyper-V • Data source size x 1.5	
Recovery point volume	For files: • (Data source size x retention range in days x 2) / 100 + 1600 MB For Exchange data: • 4.0 x retention range in days x log change x data source size + 1600 MB For SQL Server data: • 2.5 x retention range in days x log change x data source size + 1600 MB For Windows SharePoint Services data: • 1.5 x retention range in days x log change x total size of all databases + 1600 MB For Virtual Server data: • (Data source size x retention range in days x 0.02) + 1600 MB For system state: • (Data source size x retention range in days x 2) / 100 + 1600 MB For Hyper-V • (Data source size * recovery range in days * 0.1) + 1600 MB	DPM storage pool or custom volume
Change journal (for file protection only)	300 MB	Protected volume on the file server or workstation

The values used in the preceding table are defined as follows:

- **Alert%—**Threshold for the alert associated with replica growth; typically 90%.

- **Log change—**This is the change rate on the database or storage group in question. This varies widely, but for the purposes of the default recommendation in DPM, it is assumed to be 6% for Exchange and SQL Server data and 10% for Windows SharePoint Services data.
- **Retention range (RR)—**This is the number of recovery points stored; it is assumed to be 5 for purposes of the DPM default recommendation.
- **System state data source size—**The data source size is assumed to be 1 GB.

When you create a protection group, in the **Modify Disk Allocation** dialog box, the **Data Size** column for each data source displays a **Calculate** link. For the initial disk allocation, DPM applies the default formulas to the size of the volume on which the data source is located. To apply the formula to the actual size of the selected data source, click the **Calculate** link. DPM will determine the size of the data source and recalculate the disk allocation for the recovery point and replica volumes for that data source. This operation can take several minutes to perform.

We recommend that you accept the default space allocations unless you are certain that they do not meet your needs. Overriding the default allocations can result in allocation of too little or too much space.

Allocation of too little space for the recovery points can prevent DPM from storing enough recovery points to meet your retention range objectives. Allocation of too much space wastes disk capacity.

If, after you have created a protection group, you discover that you have allocated too little space for a data source in the protection group, you can increase the allocations for the replica and recovery point volumes for each data source.

If you discover that you have allocated too much space for the protection group, the only way to decrease allocations for a data source is to remove the data source from the protection group, delete the replica, and then add the data source back to the protection group with smaller allocations.

To help you estimate your storage space needs, download the DPM storage calculator.

Identifying backup storage options

DPM offers a number of storage options. For more information, see Plan for DPM storage.

If you want to back up to tape, you can choose to compress and encrypt data. Compressing data reduces the space needed on the tape and increases the number of backup jobs that can be stored on the same tape. Compression doesn’t significantly increase the tme required to complete the backup job. Encryption increases data security, and also doesn’t significantly increase the time required for the backup job. Encryption requires a valid certificate on the DPM server.

Selecting a replica creation method

When you create a protection group, you must choose a method for creating the replicas for the volumes included in the group. Replica creation involves copying all the data selected for protection to the DPM server and then running synchronization with consistency check for each of the replicas.

DPM can create the replicas automatically over the network, or you can create the replicas manually by restoring the data from removable media such as tape. Automatic replica creation is easier, but, depending on the size of the protected data and the speed of the network, manual replica creation can be faster.

To help you choose a replica creation method, the following table provides estimates for how long DPM takes to create a replica automatically over the network given different protected data sizes and network speeds. The estimates assume that the network is running at full speed and that other workloads are not competing for bandwidth. Times are shown in hours.

Hours to Complete Automatic Replica Creation at Different Network Speeds

Size of Protected Data	512 Kbps	2 Mbps	8 Mbps	32 Mbps	100 Mbps
1 GB	6	1.5	< 1	< 1	< 1
50 GB	284	71	18	5	1.5
200 GB	1137	284	71	18	6
500 GB	2844	711	178	45	15

Important
If you are deploying DPM to protect data over a WAN and your protection group includes more than 5 GB of data, we recommend that you choose the manual method for creating the replicas.

Create replicas manually

If you choose manual replica creation, DPM specifies the precise locations on the DPM server where you must create the replicas. Typically, you create the replicas by restoring your most recent backup of the data source from removable media such as tape. After you restore the data, you complete the process by running synchronization with consistency check for each of the replicas.

It is crucial that when you restore the data to the DPM server to create the replica, you retain the original directory structure and properties of the data source, such as time stamps and security permissions. The more discrepancies that exist between the replicas and the protected data source, the longer the consistency checking part of the process takes. If you do not preserve the original directory structure and properties, manual replica creation can take as long as automatic replica creation.

Plan for workload recovery

In System Center 2012 - Data Protection Manager (DPM) recovery is the process of retrieving data that has been backed up for protected workloads.

DPM uses recovery points to recover data. Recovery points, also referred to as snapshots, are a point-in-time copy of the workload data protected by DPM. Recovery points fit into the DPM protection process as follows: In the recovery process, you select the recovery point you want, and DPM recovers the data to the protected resource.

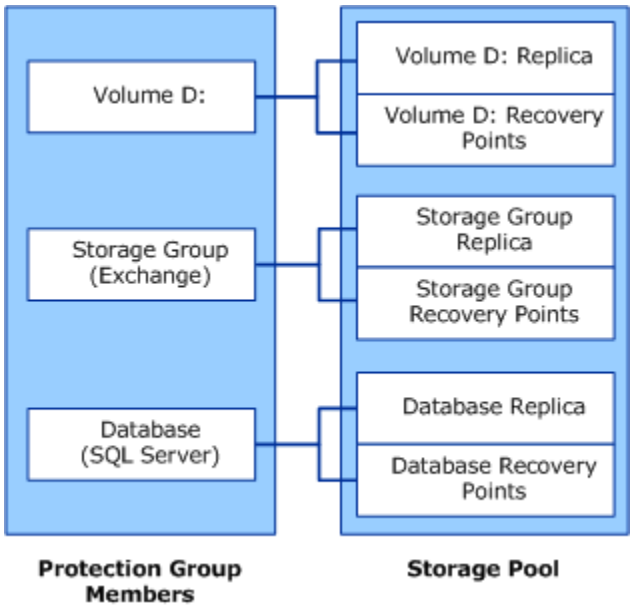
1. **Create initial replica**—When you configure a resource as a member of a protection group, you are prompted to create an initial replica of the data. This initial replica creates a baselines copy of the protected data. This baseline replica is used to create a recovery point, and when DPM synchronizing data changes and differences.
2. **Synchronize**—To synchronize, DPM checks the replica to see if changes have occurred, and then updates the replica with the changes.
3. **Create recovery point**—Creating a recovery point creates a point-in-time copy of a replica that can be used for the purpose of recovery if required.

Note the following:

- DPM can store a maximum of 64 recovery points for each file member of a protection group. For application data sources, DPM can store up to 448 express full backups and up to 96 incremental backups for each express full backup. When storage area limits have been reached and the retention range for the existing recovery points is not met yet, protection jobs will fail.
- DPM creates recovery points for file data by taking a shadow copy of the replica on a schedule that you configure. For application data, each synchronization and express full backup creates a recovery point.
- You recover data from available recovery points by using the Recovery Wizard in DPM Administrator Console. When you select a data source and point in time from which to recover, DPM notifies you if the data is on tape, whether the tape is online or offline, and which tapes are needed to complete the recovery.
- To support end-user recovery, the recovery points for files are limited to 64 by Volume Shadow Copy Service (VSS).

The following illustration shows how each protection group member is associated with its own replica volume and recovery point volume.

Protection Group Members, Replicas, and Recovery Points



Plan for end-user recovery

End-user recovery enables users to independently recover previous versions of their files. Users can recover files using shares on file servers, or DFS Namespaces.

Your deployment plan should consider the following:

- Which data users will be able to recover.
- AD DS configuration requirements—

Note the following:

- If you currently have Shadow Copies of Shared Folders enabled on a computer that you protect with DPM, you can disable that feature and regain the disk space that it uses. End-users and administrators will be able to recover files from the recovery points on the DPM server.
- Steps for configuring end-user recovery include configuring the AD DS schema, enabling the end-user recovery feature on the DPM server, and installing the recovery point client software on the client computers.

Configuring AD DS

Configuring Active Directory Domain Services to support end-user recovery involves four operations:

1. Extending the schema— The schema is extended only once; however, you must configure the Active Directory schema extension for each DPM server.
2. Creating a container
3. Granting the DPM server permissions to change the contents of the container
4. Adding mappings between source shares and shares on the replicas

Note the following:

- When you enable end-user recovery for additional DPM servers in the domain, the process performs steps 3 and 4 for each additional server. DPM will update the share mapping (step 4) after each synchronization, if needed.
- DPM administrators who are both schema and domain administrators in the Active Directory Domain Services domain can complete these steps with a single click in DPM Administrator Console. DPM administrators who are not schema and domain administrators can complete these steps by directing a schema and domain administrator to run the DPMADSchemaExtension tool.
- The DPMADSchemaExtension tool is stored on the DPM server in the folder Microsoft DPM\DPM\End User Recovery. A user who is both a schema and domain administrator can run the tool on any computer running Windows Server 2003 that is a member of the domain in which the DPM server is deployed. The administrator must specify the name of the DPM server when running the tool.
- If you use the DPMADSchemaExtension tool to enable end-user recovery, you must run it once for each DPM server.

Installing the client software

Before end users can begin independently recovering previous versions of their files, the DPM recovery point client software must be installed on their computers. If a client for Shadow Copies of Shared Folders is present on the computer, the client software must be updated to support DPM.

The recovery point client software can be installed on computers supported for DPM protection. For more information, see Support Matrix for DPM Protection.

Plan recovery goals

You define recovery goals for data in each protection group. Recovery goal settings include a retention range, synchronization frequency, and a recovery point schedule.

You should set realistic recovery goals for each data source that you will protect. Not all information or data maintained on your company's computers requires equal protection, nor does all of it merit the same investment in protection. Your deployment plan should establish recovery goals for each data source according to your business needs for protection of that data.

In DPM, you set your recovery goals in terms of *synchronization frequency*, *recovery point schedule*, and *retention range*, as follows:

- Synchronization frequency should be selected based on your data loss tolerance, or how much data you can lose. You can specify the synchronization for a protection group to occur as frequently as every 15 minutes. You can also specify less frequent synchronizations. At a minimum, DPM must synchronize the replicas for a protection group at least once between recovery points.
- The recovery point schedule establishes how many recovery points of this data should be created and when. A recovery point is the date and time of a version of a data source that is available for recovery from media that is managed by DPM.

- The retention range is how long you need the backed-up data available. To determine your retention range needs, consider the pattern of recovery requests you experience in your enterprise. If requests are concentrated within two weeks of data loss, 10 days might be an appropriate retention range for you. If requests are concentrated at a later time, you might need a longer retention range.

For example, your recovery goals for a specific Exchange Server database could be that the most recent data is never more than 30 minutes old, that you can select from versions created at 30-minute intervals, that it will be available for recovery from disk for 14 days, and that it will be available for recovery from tape for 3 years.

For more information, see Recovery Goals for Disk-Based Protection, and Recovery Goals for Tape-Based Protection.

Recovery goal options for storage methods

The following table lists the recovery goal options for each DPM protection method.

Recovery Goal Options for Protection Methods

Protection method	Retention range	Synchronization frequency or backup schedule	Recovery points
Short-term on disk	1–448 days For file members in a protection group, DPM can store a maximum of 64 recovery points (this is a VSS limit for client accessible shadow copies). If you schedule one recovery point per day (7 per week), you can retain 64 recovery points for a maximum of 448 days (7 * 64 = 448 days). For applications, there is a maximum of 512 available recovery points. However, DPM reserves 64 recovery	Select a frequency between 15 minutes and 24 hours, or select **Just before a recovery point**.	When a specific synchronization frequency is selected: • Recovery points for files are created according to the schedule you configure. • Recovery points for application data are created after each synchronization. When **Just before a recovery point** is selected, recovery points for all protection group members are created according to the schedule you configure.

Protection method	Retention range	Synchronization frequency or backup schedule	Recovery points
	points, so you can only select up to 448 recovery points for applications. This is because DPM assumes that file protection could use the same volume as the applications you are protection, so the VSS shadow copies apply to the same volume. Therefore, 448 + 64 = 512 (which is the VSS shadow copy maximum per volume).		
Short-term on tape	1–12 weeks	Select to back up: • Every day • Every week • Every two weeks	Instead of recovery points, you configure one of the following backup types: • Full and incremental backups • Only full backup When you select weekly or every two weeks, only full backup is available. You specify the day and time. When you select daily full backups, you specify the time. When you select daily full and incremental, you specify the day and time for the full backup and for the incremental

Protection method	Retention range	Synchronization frequency or backup schedule	Recovery points
			backup.
Long-term on tape	Minimum: 1 week Maximum: 99 years	Select to back up: • Daily • Weekly • Biweekly • Monthly • Quarterly • Half-yearly • Yearly	See Recovery Point Schedules for Long-Term Protection and Customizing Recovery Goals for Long-Term Protection.

Recovery point options for long-term protection

Recovery point schedules for long-term protection

The following table lists the DPM recovery point schedule for the different long-term protection combinations.

Recovery Point Schedules for Long-Term Protection

Backup frequency and retention range	Recovery point schedule
Daily, 1–4 weeks	Full backup daily
Daily, 1–11 months	1 full backup each day for 4 weeks 1 full backup each month after the initial 4 weeks
Daily, 1–99 years	1 full backup each day for 4 weeks 1 full backup each month after the initial 4 weeks, until the 12th month 1 full backup each year after the initial 11 months
Weekly, 1–4 weeks	Full backup weekly
Weekly, 1–11 months	1 full backup each week for 4 weeks 1 full backup each month after the initial 4 weeks

Backup frequency and retention range	Recovery point schedule
Weekly, 1–99 years	1 full backup each week for 4 weeks 1 full backup each month after the initial 4 weeks, until the 12th month 1 full backup each year after the initial 11 months
Bi-weekly, 1–11 months	1 full backup every 2 weeks for 4 weeks 1 full backup each month after the initial 4 weeks
Bi-weekly, 1–99 years	1 full backup every 2 weeks for 4 weeks 1 full backup each month after the initial 4 weeks, until the 12th month 1 full backup each year after the initial 11 months
Monthly, 1–11 months	Full backup monthly
Monthly, 1–99 years	1 full backup each month, until the 12th month 1 full backup each year after the initial 11 months
Quarterly, 1–99 years	1 full backup every 3 months until the 12th month 1 full backup each year after the initial 11 months
Half-yearly, 1–99 years	1 full backup every 6 months until the 12th month 1 full backup each year after the initial 11 months
Yearly, 1–99 years	Full backup yearly

Scheduling options for long-term protection

The following table lists the scheduling options you can modify for long-term protection with DPM.

Scheduling Options for Long-Term Protection

For this backup frequency	Depending on retention range, you can configure
Daily	• Time for daily backup • Specific day or day of week and time for

For this backup frequency	Depending on retention range, you can configure
	monthly backup • Specific day or date and time for yearly backup
Weekly	• Time and day of week for weekly backup • Specific day or day of week and time for monthly backup • Specific day or date and time for yearly backup
Biweekly	• Time and day of week for biweekly backup • Specific day or day of week and time for monthly backup • Specific day or date and time for yearly backup
Monthly	• Specific day or day of week and time for monthly backup • Specific day or date and time for yearly backup
Quarterly	• Time and date for quarterly backup (Quarterly backups are performed in January, April, July, and October on the specified day of the month.) • Specific day or date and time for yearly backup
Half-yearly	• Time, specific day or date, and months for half-yearly backup • Specific day or date and time for yearly backup
Yearly	• Specific day or date and time for yearly backup

Recovery Goals for Disk-Based Protection

Although all members of a protection group share the same synchronization frequency, the synchronization process and the resulting recovery point schedule differ based on the type of data being protected. For more information, see **How DPM Works**.

Synchronization and Recovery Points for Files

For a file volume or share, the protection agent on the protected computer tracks changed blocks in the change journal that is part of the operating system. During synchronization, these changes

are transferred to the DPM server and then applied to the replica to synchronize the replica with the data source.

You can select a synchronization frequency interval of anywhere from 15 minutes to 24 hours. The default is 15 minutes. You can also select to synchronize only before a recovery point is created.

Recovery points, which are shadow copies of the replica for file data, are created from the synchronized replica on a configurable schedule. Each file synchronization does not result in a recovery point unless you synchronize only before each recovery point; however, you can manually create a recovery point from the most recent file synchronization.

For example, a volume is synchronized hourly and a recovery point for the volume is created at 8:00 A.M., 12:00 P.M., and 6 P.M. A user makes changes to a file on the volume at 1:30 P.M.; however, when another user makes changes an hour later, the file is inadvertently corrupted, and you are asked to recover the file with the first user's changes. Because the changes at 1:30 P.M. were made after the most recent recovery point was created at 12:00 P.M., you cannot recover the file from the most recent recovery point. However, you can manually create a recovery point from the appropriate synchronization of that replica and then recover the file from that new recovery point.

The default schedule creates recovery points at 8:00 A.M., 12:00 P.M., and 6:00 P.M. daily. You can modify both the times and the specific days. You cannot specify different times for different days. For example, you can schedule recovery points for 2:00 A.M. and 2:00 P.M. on weekdays only; however, you cannot schedule recovery points for 2:00 A.M. on weekdays and at 12:00 P.M. on weekends.

Retention Range for Files

Retention range is the duration of time for which the data should be available for recovery. When the retention range for a recovery point expires, the recovery point is deleted.

You can select a retention range between 1 and 448 days for short-term disk-based protection, up to 12 weeks for short-term tape-based protection, and up to 99 years for long-term tape-based protection. DPM can store a maximum of 64 recovery points for each file member of a protection group.

For example, if you select to synchronize before each recovery point and you schedule 6 recovery points daily, and you set a retention range of 10 days, recovery points for the files in that protection group never exceed 64. However, if you choose a combination of settings that exceeds the limit of 64 recovery points, DPM warns you during the configuration process so that you can modify your selections; you cannot configure a protection configuration for files that exceeds the limit of 64 recovery points.

Synchronization and Recovery Points for Application Data

For application data, changes to volume blocks belonging to application files are tracked by the volume filter. Synchronization of application data is analogous to an incremental backup and creates an accurate reflection of the application data when combined with the replica.

You can select a synchronization frequency interval of anywhere from 15 minutes to 24 hours. The default is 15 minutes. You can also select to synchronize only before a recovery point is created. If you select to synchronize only before a recovery point is created, DPM performs express full backup to synchronize the replica according to the recovery point schedule.

For applications that support incremental backups, the default schedule results in recovery points for each synchronization (every 15 minutes) and for the express full backup at 8:00 P.M. daily. For applications that do not support incremental backups, the default schedule results in a recovery point for the express full backup at 8:00 P.M. daily.

You can modify both the times and the specific days. You cannot specify different times for different days. For example, you can schedule recovery points for 2 A.M. and 2 P.M. on weekdays only; however, you cannot schedule recovery points for 2 A.M. on weekdays and at 12:00 P.M. on weekends.

Exception for Some SQL Server Databases

Transaction log backups, which DPM uses for incremental synchronization of application data, cannot be performed for a SQL Server database that is read-only, configured for log shipping, or configured to use the Simple Recovery Model. For those SQL Server databases, recovery points correspond to each express full backup.

Comparing Synchronization and Express Full Backup

To enable faster recovery time, DPM will regularly perform an express full backup in place of incremental synchronization. An express full backup is a type of synchronization that updates the replica to include the changed blocks.

Note
You can modify the express full backup schedule for any protection group that contains application data by using the **Optimize performance** action in the **Protection** task area or by using the Modify Group Wizard.

Retention Range for Application Data

You can select a retention range between 1 and 448 days for short-term disk-based protection, up to 12 weeks for short-term tape-based protection, and up to 99 years for long-term tape-based protection.

For example, if you select to synchronize every 15 minutes and you set a retention range of 10 days, those recovery goals result in a protection plan that maintains 960 recovery points for application data in that protection group after the initial 10 days of data protection.

See Also

Recovery Goals for Tape-Based Protection

Recovery Goals for Tape-Based Protection

DPM protects data on tape through a combination of full and incremental backups from either the protected data source (for short-term protection on tape or for long-term protection on tape when

DPM does not protect the data on disk) or from the DPM replica (for long-term protection on tape when short-term protection is on disk).

The choices for retention range, frequency of backups, and recovery options are different for short-term and long-term protection.

Note

You can select disk or tape for short-term protection, but not both.

Short-Term Protection on Tape

For short-term data protection on tape, you can select a retention range of 1–12 weeks. DPM provides management support of your tapes through alerts and reports, and it uses the specified retention range to establish the expiration date for each tape.

Your options for backup frequency are daily, weekly, or biweekly, depending on the retention range.

If you select short-term protection on tape using both incremental and full backups, the retention range will be longer than the one you specified (up to a maximum of 1 week longer) because of a dependency between full and incremental backups. Tapes containing full backup are recycled only after all dependent incremental tapes are recycled. Because full backup happen once a week and the incrementals daily, the weekly full backup tape must wait for the six daily incremental backup tapes to be recycled before the full backup tape is recycled. If an incremental backup fails and there is no incremental tape to recycle, the full backup tape will be recycled earlier.

Long-Term Protection on Tape

For long-term data protection, also known as tape archive, you can select a retention range between 1 week and 99 years. DPM provides management support of your tape archives through alerts and reports, and it uses the specified retention range to establish the expiration date for each tape.

The frequency of backup is based on the specified retention range, as shown in the following list:

- When the retention range is 1–99 years, you can select backups to occur daily, weekly, biweekly, monthly, quarterly, half-yearly, or yearly.
- When the retention range is 1–11 months, you can select backups to occur daily, weekly, biweekly, or monthly.
- When the retention range is 1–4 weeks, you can select backups to occur daily or weekly.

See Also

Recovery Goals for Disk-Based Protection

Plan protection policy

DPM configures the *protection policy*, or schedule of jobs, for each protection group based on the recovery goals that you specify for that protection group. Examples of recovery goals are as follows:

- “Lose no more than 1 hour of production data”
- “Provide me with a retention range of 30 days”
- “Make data available for recovery for 7 years”

Your *recovery goals* quantify your organization's data protection requirements. In DPM, the recovery goals are defined by retention range, data loss tolerance, recovery point schedule, and, for database applications, the express full backup schedule.

The *retention range* is how long you need the backed-up data available. For example, do you need data from today to be available a week from now? Two weeks from now? A year from now?

Data loss tolerance is the maximum amount of data loss, measured in time, that is acceptable to business requirements, and it will determine how often DPM should synchronize with the protected server by collecting data changes from the protected server. You can change the synchronization frequency to any interval between 15 minutes and 24 hours. You can also select to synchronize just before a recovery point is created, rather than on a specified time schedule.

The *recovery point schedule* establishes how many recovery points of this protection group should be created. For file protection, you select the days and times for which you want recovery points created. For data protection of applications that support incremental backups, the synchronization frequency determines the recovery point schedule. For data protection of applications that do not support incremental backups, the express full backup schedule determines the recovery point schedule.

Note
When you create a protection group, DPM identifies the type of data being protected and offers only the protection options available for the data.

Plan for DPM deployment with Operations Manager

As you consider the number of servers running System Center 2012 – Operations Manager that your organization requires, this section will give you broad guidelines to help you make better decisions.

Single or multiple Operations Manager servers

A single Operations Manager server with SQL Server and Management Server can host up to 10,000 data sources from up to 50 DPM servers. The recommended hardware for this computer is 12 GB with good efficient storage configured in RAID.

A multi-server Operations Manager setup with two computers, with SQL Server and Management Server on different servers can host up to 50,000 data sources from up to 100 dpm2012long severs. The recommended hardware is 12 GB on the Operations Manager server and 8 GB on the SQL Server with good efficient storage configured in RAID.

Memory usage on Operations Manager server

Typically, the memory usage on the Operations Manager server is:

- Operations Manager Console - approximately 300 MB
- Scoped Administrator Console – 50 to 120 MB
- Windows Presentation Foundation (WPF) - 30 to 50 MB
- On a typical computer with 2 GB memory, you can use 1 GB for monitoring, which allows you to have five scoped Administrator Consoles, an Operations Manager Console, and up to seven WPF dialogs.

Working with more than 2,000 data sources

If you are working with over 2,000 data sources on the DPM server, you need to make the following registry changes on the DPM server on which the Operations Manager agent is installed:

- Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\HealthService\Parameters\Persistence Version Store Maximum to 80 MB (5120). Default = 60 MB
- Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\HealthService\Parameters\Management Groups\<MG Name>\maximumQueueSizeKb to 100 MB. Default = 15 MB
- Set HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Modules\Global\PowerShell\ScriptLimit\QueueMinutes to 120 mins

Planning the Operations Manager data warehouse database size

For every 100000 entries (backups), you will need about 6.5 GB.

The things to consider when you are deciding on how much disk space you will needs are:

- Number of backups in the environment per day = Average number of backups per data source per day * Average number of data sources per DPM * Number of DPM servers.
- Retention period (in days)

Working over Wide Area Networks

The DPM scoped Administrator Console will not work over WAN that have a latency over 15 ms. Although the functionality will be available, the console will be unresponsive.

Plan the DPM Directory Structure

When you begin protecting data with DPM, you will notice that the installation path of DPM contains three folders in the Volumes directory:

- <Install Drive>\Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\DiffArea
- <Install Drive>\Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\Replica

- <Install Drive>\Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\ShadowCopy

The DiffArea folder contains mounted shadow copy volumes that store the recovery points for a data source.

The Replica folder contains mounted replica volumes.

The ShadowCopy folder contains local backup copies of the DPM database. In addition, when you use DPMBackup.exe to create backup shadow copies of the replicas for archive by third-party backup software, the backup shadow copies are stored in the ShadowCopy folder.

Plan for DPM security

DPM operates as a high-privileged server on the network. To help ensure the security of the DPM server, the DPM security architecture relies on the security features of Windows Server 2008 and Active Directory Domain Services, SQL Server 2008, and SQL Server Reporting Services.

To maintain the DPM security architecture:

- Accept all default security settings.
- Do not install unnecessary software on the DPM server.
- Do not change security settings after DPM is deployed. In particular, do not change SQL Server 2008 settings, Internet Information Services (IIS) settings, DCOM settings, or settings for the local users and groups that DPM creates during product installation.
- A remote instance of SQL Server should not run as Local System.

Caution

If you are using one SQL Server to host multiple DPM databases, the administrators of each of the DPM servers has access to the databases of the other DPM servers.

Installing unnecessary software and changing default security settings can seriously compromise DPM security.

In This Section

Configuring Antivirus Software

Configuring firewalls

Security considerations for end-user recovery

Granting Appropriate User Privileges

See Also

Plan for end-user recovery

Plan for DPM server deployment

Configuring Antivirus Software

DPM is compatible with most popular antivirus software products. However, antivirus products can affect DPM performance, and, if they are not configured properly, they can cause data corruption of replicas and recovery points. This section provides instructions for mitigating such problems.

Configuring Real-Time Monitoring for Viruses

To minimize performance degradation on the DPM server, disable antivirus real-time monitoring of replicas for all protected data sources by disabling real-time monitoring of the DPM process DPMRA.exe, which is located in the folder Microsoft Data Protection Manager\DPM\bin. Real-time monitoring of replicas degrades performance because it causes the antivirus software to scan all affected files each time DPM applies changes to the replicas.

Additionally, if you experience degraded performance while using DPM Administrator Console, disable real-time monitoring of the csc.exe process, which is located in the folder Windows\Microsoft.net\Framework\v2.0.50727. The csc.exe process is the C# compiler. Real-time monitoring of the csc.exe process can degrade performance because it causes the antivirus software to scan files that the csc.exe process emits when generating XML messages.

For instructions for configuring real-time monitoring for individual processes, see your antivirus product documentation.

Setting Options for Infected Files

To prevent data corruption of replicas and recovery points, configure the antivirus software on the DPM server to delete infected files rather than automatically cleaning or quarantining them. Automatic cleaning and quarantining can result in data corruption because these processes cause the antivirus software to modify files with changes that DPM cannot detect. Any time that DPM attempts to synchronize a replica that has been modified by another program, data corruption of the replica and recovery points can result. Configuring the antivirus software to delete infected files avoids this problem. Note, however, that you must run manual synchronization with consistency check each time that the antivirus software deletes files from a replica. For instructions for configuring your antivirus software to delete infected files, see the product documentation.

See Also

Plan for DPM security

Configuring firewalls

If the computers you want to protect reside behind a firewall, you must configure the firewall to allow communication between the DPM server, the computers it protects, and the domain controllers.

Protocols and Ports

Depending on your network configuration, you might need to perform firewall configuration to enable communication between DPM, the protected servers, and the domain controllers. To help with firewall configuration, the following table provides details about the protocols and ports used by DPM.

Protocols and Ports Used by DPM

Protocol	Port	Details
DCOM	135/TCP Dynamic	The DPM control protocol uses DCOM. DPM issues commands to the protection agent by invoking DCOM calls on the agent. The protection agent responds by invoking DCOM calls on the DPM server. TCP port 135 is the DCE endpoint resolution point used by DCOM. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through 65535. However, you can configure this range by using Component Services. Note that for DPM-Agent communication you must open the upper ports 1024-65535. To open the ports, perform the following steps: 1. In IIS 7.0 Manager, in the **Connections** pane, click the server-level node in the tree. 2. Double-click the **FTP Firewall Support** icon in the list of features. 3. Enter a range of values for the **Data Channel Port Range**. 4. After you enter the port range for your FTP service, in the **Actions** pane, click

Protocol	Port	Details
		Apply to save your configuration settings.
TCP	5718/TCP 5719/TCP	The DPM data channel is based on TCP. Both DPM and the protected computer initiate connections to enable DPM operations such as synchronization and recovery. DPM communicates with the agent coordinator on port 5718 and with the protection agent on port 5719.
DNS	53/UDP	Used between DPM and the domain controller, and between the protected computer and the domain controller, for host name resolution.
Kerberos	88/UDP 88/TCP	Used between DPM and the domain controller, and between the protected computer and the domain controller, for authentication of the connection endpoint.
LDAP	389/TCP 389/UDP	Used between DPM and the domain controller for queries.
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	Used between DPM and the protected computer, between DPM and the domain controller, and between the protected computer and the domain controller, for miscellaneous operations. Used for SMB directly hosted on TCP/IP for DPM functions.

Windows Firewall

Windows Firewall is included with Windows Server 2008 and Windows Server 2008 R2. If you enable Windows Firewall on the DPM server before you install DPM, DPM Setup properly configures the firewall for DPM.

If you enable Windows Firewall on the DPM server after you install DPM, you must configure the firewall manually to permit communication between the DPM server and protected computers. Configure Windows Firewall on a DPM server by opening port 135 to incoming TCP traffic and specifying the DPM service (Microsoft DPM/bin/MsDPM.exe) and the protection agent (Microsoft DPM/bin/Dpmra.exe) as exceptions to the Windows Firewall policy.

For instructions for configuring Windows Firewall, search on "Windows Firewall" in Windows Help and Support for Windows Server 2008 or Windows Server 2008 R2.

See Also

Plan for DPM security

Security considerations for end-user recovery

You can enable end-user recovery for file data, but not for application data. Use only domain-based security groups for permissions to files and folders on which you plan to enable end-user recovery. DPM cannot guarantee consistency between end-user access to data on protected computers and end-user access to recovery points of that data on the DPM server if you rely on local security groups.

For example, if the set of users included in the protected computer's local Users group differs from the set of users included in the DPM server’s local users group, different sets of users will have access to the data on the protected computer and to the recovery points of that data.

See Also

Plan for DPM security

Granting Appropriate User Privileges

Before you begin a DPM deployment, verify that appropriate users have been granted required privileges for performing the various tasks. The following table shows the user privileges that are required to perform the major tasks associated with DPM.

User Privileges Required to Perform DPM Tasks

Task	Required Privileges
Adding a DPM server to an Active Directory domain	Domain administrator account, or user right to add a workstation to a domain
Installing DPM	Administrator account on the DPM server

Task	Required Privileges
Installing the DPM protection agent on a computer	Domain account that is a member of the local administrators group on the computer
Opening DPM Administrator Console	Administrator account on the DPM server
Extending the Active Directory Domain Services schema to enable end-user recovery	Schema administrator privileges in the domain
Creating an Active Directory Domain Services container to enable end-user recovery	Domain administrator privileges in the domain
Granting a DPM server permissions to change the contents of the container	Domain administrator privileges in the domain
Enabling end-user recovery feature on a DPM server	Administrator account on the DPM server
Installing recovery point client software on a client computer	Administrator account on the client computer
Accessing previous versions of protected data from a client computer	User account with access to the protected share
Recovering Windows SharePoint Services data	Windows SharePoint Services farm administrator account that is also an administrator account on the front-end Web server that the protection agent is installed on

Caution
If you are using one SQL Server to host multiple DPM databases, the administrators of each of the DPM servers has access to the databases of the other DPM servers.

See Also

Plan for DPM security

Installing and Upgrading System Center 2012 - DPM

This content provides instructions for installing, repairing, configuring, and troubleshooting System Center 2012 – Data Protection Manager (DPM).

In This Section

Installing DPM

The deployment of System Center 2012 – Data Protection Manager (DPM) will depend on which features of DPM you want to use. A complete installation of DPM requires a DPM server, an Operations Manager server, a SQL Server and computers you want to protect. You can use the DPM Setup screen to install the various features.

DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:

- A computer on which the Application Server role is installed
- A computer that is an Operations Manager management server
- A computer on which Exchange Server is running
- A computer that is a node of a cluster

You must have administrative privileges to install DPM.

Before you install DPM, you must run the Prerequisite Checker from the Setup splash screen. The checker will check whether your computer meets the minimum requirements to run DPM. Setup installs the prerequisite software automatically. However, if it fails, you can install the prerequisite software manually. For more information, see Installing Prerequisite Software Manually.

DPM requires a SQL Server instance for the DPM database. You can use SQL Server 2008 R2 or SQL Server 2012. For more information on setting up the database, see Setting up the DPM database.

You can install DPM and its prerequisite software either from the product DVD or from a network share to which you have copied the contents of the product DVD. If you want to install from a network share, the share must duplicate the exact directory structure of the product DVD. Install DPM from a shared folder only if the share is hosted on a trusted site.

You may need to restart the computer after setup is complete.

Before installing DPM, note the following:

- All computers that you use for your DPM installation must meet at least the minimum hardware and software requirements. For more information, see System Requirements for DPM in System Center 2012.
- Setup stops the Removable Storage service before installing DPM.

- After you install DPM, you must perform a series of required configuration tasks before you can start protecting your data. For more information, see Deploying DPM.
- The installation logs are placed in C:\Program Files\ Microsoft System Center 2012\DPM\DPMLogs.
- DPM installs its own file filter (DPMFilter.SYS). It is Windows Hardware Quality Labs (WHQL) certified and is installed as part of DPM installation. This file is not removed during DPM uninstallation.

Important
DPM does not support clustered or mirrored SQL Server for hosting the DPM database.

After you install DPM, you must wait until the next scheduled discovery before you can use scoped DPM Administrator Console from Central Console.

In This Section

System Requirements for DPM in System Center 2012

DPM Setup Wizard Help Pages

Setting up the DPM database

Installing DPM on a Domain Controller

Installing Prerequisite Software Manually

Upgrading the DPM Database

System Requirements for DPM in System Center 2012

Before you install System Center 2012 – Data Protection Manager (DPM), ensure that the computer you will use for your DPM server and all the computers and applications you want to protect meet or exceed the minimum hardware, software, and network requirements.

In This Section

System requirements for System Center 2012 R2 - DPM

System requirements for System Center 2012 SP1 - DPM

System requirements for System Center 2012 - DPM

System requirements for System Center 2012 - DPM

This topic summarizes system requirements for System Center 2012 – Data Protection Manager (DPM) in System Center 2012.

DPM server hardware requirements

The following table lists the hardware requirements for the DPM server.

Component	Minimum requirement	Recommended requirement
Processor	1 GHz, dual-core CPU or faster	2.33 GHz quad-core CPU
RAM	4 GB	8 GB
Pagefile	1.5 times the amount of RAM on the computer.	0.2 percent of the combined size of all recovery point volumes, in addition to the minimum requirement size (1.5 times the amount of RAM on the computer).
Disk space for DPM installation	• DPM installation location: 3 GB • Database files drive: 900 MB • System drive: 1 GB **Note** The system drive disk space requirement is necessary if you choose to install the dedicated instance of SQL Server from DPM Setup. If you use a remote instance of SQL Server, this disk space requirement is considerably less.	**Note** DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a DPM temporary installation location; therefore, we recommend that the volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool **Note** The storage pool does not support Universal Serial Bus (USB)/1394 disks.	1.5 times the size of the protected data	2.5–3 times the size of the protected data
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot

Component	Minimum requirement	Recommended requirement
		record (MBR) disks **Note** These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

DPM server operating system requirements

Supported operating systems

Supported operating system	Details	Required updates
Windows Server 2008 R2 SP1, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	
Windows Server 2008 R2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	Before you install DPM on a computer that is running Windows Server 2008 R2, you must install the following updates and hotfixes: • KB983633 • KB2223201 **Important** If you are upgrading to Windows Server 2008 R2, you must remove any pre-release version of Windows PowerShell 2.0 before you upgrade.
Windows Server 2008 SP2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	

Supported operating system	Details	Required updates
Windows Server 2008, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	• KB971254 • KB962975 • KB975759 • KB2279769 **Important** After installing all updates, restart the computer before you install DPM. For more information about Windows Server 2008 system requirements, see Windows Server 2008 System Requirements.

Disk requirements

DPM requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files
- DPM prerequisite software
- DPM database files

Note the following:

- DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, disk is defined as any disk device manifested as a disk in Disk Management. For more information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool.
- If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that DPM will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.
- The DPM storage pool disks cannot be .VHD – they must be either iSCSI attached disks or pass-through disks. The following types of disk configuration are supported as DPM storage pool:

    - Pass-through disk with host direct attached storage (DAS)
    - Pass-through iSCSI LUN which is attached to host.
    - Pass-through FC LUN which is attached to host.
    - iSCSI target LUN which is connected to DPM virtual machine directly.
- Short-term or long-term backup to tape will be limited to using iSCSI attached tape libraries, and we recommend a separate NIC for that connection.
- you cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

Installation requirements and limitations

This section summarizes installation requirements, prerequisites, and limitations.

DPM server requirements

- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system.
- DPM server DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:
    - A computer on which the Application Server role is installed.
    - A computer that is an Operations Manager management server
    - A computer on which Exchange Server is running.
    - A computer that is a cluster node.
- DPM is not supported on the Turkish language version of any of the listed Windows Server versions.
- The following prerequisites are required for installation:
    - Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)
    - Microsoft Visual C++ 2008 Redistributable
    - Windows PowerShell 2.0
    - Windows Installer 4.5 or later versions
    - Windows Single Instance Store (SIS)
    - Microsoft Application Error Reporting

    Setup automatically installs these if they are not already installed or enabled. If any pre-requisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.
- After you have installed DPM, we recommend that you run Windows Update on the DPM server and, if you use a remote database, on the remote computer where the DPM database is located, and install all important updates or hotfixes.

SQL Server requirements

For the DPM database, DPM requires a dedicated instance of the 64-bit version of SQL Server 2012 or SQL Server 2008 R2 or SQL Server 2008 R2 SP1, Enterprise or Standard

Edition. During setup, you can select either to have DPM Setup install SQL Server 2008 R2 on the DPM server, or you can specify that DPM use a remote instance of SQL Server.

If you do not have a licensed version of SQL Server 2008 R2, you can install an evaluation version from the setup DVD. To install the evaluation version, do not provide the product key when you are prompted. However, you must buy a license for SQL Server if you want to continue to use it after the evaluation period.

When you use a remote instance of SQL Server with the DPM installation, note the following requirements:

- You must install the remote instance of SQL Server before you install DPM.

  Important
  A remote instance of SQL Server on a domain controller is not supported.
- The computer that is running a remote instance of SQL Server must be located in the same domain and time zone as the DPM server.
- Setup creates the **DPMDBReaders$<DPM server name>** and **DPMDBAdministrators$<DPM server name>** local groups on the computer that is running the remote instance of SQL Server. You must add DPM administrators to these groups for DPM to use the remote instance of SQL Server.
- For the DPM server to access a remote instance of SQL Server through Windows Firewall, you must configure an exception on the computer that is running SQL Server to use port 80.
- You must install the DPM support files on the computer that is running the remote instance of SQL Server. For more information, see Setting up the DPM database.
- You cannot user a clustered instance of SQL Server 2012 to host a remote DPM database.
- You cannot host the DPM database on a SQL Server AlwaysOn deployment.

In addition to installing programs that are required for DPM, SQL Server Setup installs the following programs, which are not required for DPM:

- Microsoft SQL Server Compact 3.5 SP1
- Microsoft SQL Server Compact 3.5 SP1 Query Tools
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft Visual Studio Tools for Applications 2.0
- Microsoft Office 2003 Web Components

Note
These programs are not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall these programs manually.

Data source limits for DPM server

The following table lists the data source limits that a DPM server can protect (if it meets the minimum hardware requirements) and the recommended disk space required for the DPM server.

Platform	Data source limit	Recommended disk space
64-bit computers	600 volumes, of which 300 are replica volumes and 300 are recovery point volumes Data sources are typically spread across approximately 75 servers and 150 client computers.	120 TB per DPM server, with 80 TB replica size with a maximum recovery point size of 40 TB

Requirements for protected computers

For a complete list of DPM protection support for computers and workloads, see the Support Matrix for DPM Protection. Prerequisites for computers running the DPM protection agent are summarized in the following table. If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Protected workload	Prerequisites
Computer volumes	• Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB. • Computers must have the Microsoft .NET Framework 3.5 with Service Pack 1 (SP1) installed.
File Servers	Before you can protect a file server running Windows Server 2008 R2, you must apply the hotfix KB977381
Exchange	Note the following when protecting Exchange: • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006. • The eseutil.exe and ese.dll versions that are installed on the most recent release of Exchange Server must be the same versions

Protected workload	Prerequisites
	that are installed on the DPM server. So if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see **Eseutil.exe and Ese.dll**. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll: a. Install the Microsoft Exchange Server 2007 management tools on the DPM server. b. When you install the management tools, ensure that you install the management tools for the latest version of Microsoft Exchange that you are protecting. For example, if one of your mail servers is running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2007 SP1, you must install the management tools for Microsoft Exchange 2007 SP1. c. At the command prompt, in the **<DPM installation folder>\Bin** directory, use the following syntax with the **fsutil** command to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>** On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"**
Hyper-V	To protect Hyper-V, note the following: • For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB975354 • For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in KB975921

Protected workload	Prerequisites

	• Before you can protect a computer running Windows Server 2008 with Hyper-V, you must apply the following updates:
	  • KB948465
	  • KB971394

SharePoint	When protecting SharePoint, note the following:
	• Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422
	• If you use the **Office SharePoint Server Search** service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply the following updates:
	  • KB951695
	  • KB941422

Administration options

In addition to managing DPM directly from the DPM server, you can use the following options:

- Use DPM Remote Administration
- Use DPM Central Console

DPM Remote Administration

DPM Remote Administration allows you to work on your DPM servers from any computer. It also supports task-based scripting. You can install it on the following operating systems:

- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2008 R2
- Windows Server 2008

Computers from which you want to remotely administer DPM require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

DPM Central Console

With DPM Central Console you can monitor and manage multiple DPM servers from one location. You can monitor and troubleshoot servers running both DPM 2010 QFE2 with feature pack and

DPM. DPM Central Console must be installed on Operations Manager server or a computer running Operations Manager Console. You can install it on the following operating systems:

- Windows 7
- Windows Vista

Computers from which you want to run DPM Central Console require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Network requirements

The following are the network requirements for System Center 2012 – Data Protection Manager (DPM):

- DPM must be installed on a 64-bit computer that is located in a Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 Active Directory domain.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you can protect the computers using DPM's support for computers in workgroups or untrusted domains. For more information, see Managing Protected Computers in Workgroups and Untrusted Domains.

  DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 forest mode.
- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM does not support disjointed namespaces.

System requirements for System Center 2012 SP1 - DPM

This topic summarizes system requirements for System Center 2012 – Data Protection Manager (DPM) in System Center 2012 Service Pack 1 (SP1).

DPM server hardware requirements

The following table lists the minimum and recommended hardware requirements for the DPM server.

Component	Minimum requirement	Recommended requirement
Processor	1 GHz, dual-core CPU or faster	2.33 GHz quad-core CPU

Component	Minimum requirement	Recommended requirement
RAM	4 GB	8 GB
Pagefile	1.5 times the amount of RAM on the computer	0.2 percent of the combined size of all recovery point volumes, in addition to the minimum required size (1.5 times the amount of RAM on the computer).
Disk space for DPM installation	• DPM installation location: 3 GB • Database files drive: 900 MB • System drive: 1 GB **Note** The system drive disk space requirement is necessary if you choose to install the dedicated instance of SQL Server from DPM Setup. If you use a remote instance of SQL Server, this disk space requirement is considerably less.	**Note** DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a DPM temporary installation location; therefore, we recommend that the volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool **Note** The storage pool does not support Universal Serial Bus (USB)/1394 disks.	1.5 times the size of the protected data	2.5–3 times the size of the protected data
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot record (MBR) disks **Note**

Component	Minimum requirement	Recommended requirement
		These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

DPM server operating system requirements

Supported operating systems

Supported operating system	Details	Required updates
Windows Server 2012, Datacenter and Standard editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	
Windows Server 2008 R2 SP1, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	
Windows Server 2008 R2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	Before you install DPM on a computer that is running Windows Server 2008 R2, you must install the following updates and hotfixes: • KB983633 • KB2223201 **Important** If you are upgrading to Windows Server 2008 R2, you must remove any pre-release version of Windows PowerShell 2.0 before you upgrade.
Windows Server 2008 SP2, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not	

Supported operating system	Details	Required updates
	supported.	
Windows Server 2008, Standard and Enterprise editions	64-bit only. 32-bit or Itanium architecture–based operating systems are not supported.	• KB971254 • KB962975 • KB975759 • KB2279769 **Important** After installing all updates, restart the computer before you install DPM. For more information about Windows Server 2008 system requirements, see Windows Server 2008 System Requirements.

Disk requirements

DPM requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files
- DPM prerequisite software
- DPM database files

Note the following:

- DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, disk is defined as any disk device manifested as a disk in Disk Management. For more information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool.
- If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that DPM will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.

- The DPM storage pool disks cannot be .VHD – they must be either iSCSI attached disks or pass-through disks. The following types of disk configuration are supported as DPM storage pool:
  - Pass-through disk with host direct attached storage (DAS)
  - Pass-through iSCSI LUN which is attached to host.
  - Pass-through FC LUN which is attached to host.
  - iSCSI target LUN which is connected to DPM virtual machine directly.
- Short-term or long-term backup to tape will be limited to using iSCSI attached tape libraries, and we recommend a separate NIC for that connection.
- you cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

Installation requirements and limitations

This section summarizes installation requirements, prerequisites, and limitations.

DPM server requirements

- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system.
- DPM server DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:
  - A computer on which the Application Server role is installed.
  - A computer that is an Operations Manager management server
  - A computer on which Exchange Server is running.
  - A computer that is a cluster node.
- DPM is not supported on the Turkish language version of any of the listed Windows Server versions.
- The following prerequisites are required for installation:
  - Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)
  - Microsoft Visual C++ 2008 Redistributable
  - Windows PowerShell 2.0
  - Windows Installer 4.5 or later versions
  - Windows Single Instance Store (SIS)
  - Microsoft Application Error Reporting

  Setup automatically installs these if they are not already installed or enabled. If any pre-requisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.
- After you have installed DPM, we recommend that you run Windows Update on the DPM server and, if you use a remote database, on the remote computer where the DPM database is located, and install all important updates or hotfixes.

SQL Server requirements

For the DPM database, DPM requires a dedicated instance of the 64-bit version of SQL Server 2012 or SQL Server 2008 R2 or SQL Server 2008 R2 SP1, Enterprise or Standard Edition. During setup, you can select either to have DPM Setup install SQL Server 2008 R2 on the DPM server, or you can specify that DPM use a remote instance of SQL Server.

If you do not have a licensed version of SQL Server 2008 R2, you can install an evaluation version from the setup DVD. To install the evaluation version, do not provide the product key when you are prompted. However, you must buy a license for SQL Server if you want to continue to use it after the evaluation period.

When you use a remote instance of SQL Server with the DPM installation, note the following requirements:

- You must install the remote instance of SQL Server before you install DPM.

  Important
  A remote instance of SQL Server on a domain controller is not supported.
- The computer that is running a remote instance of SQL Server must be located in the same domain and time zone as the DPM server.
- Setup creates the **DPMDBReaders$<DPM server name>** and **DPMDBAdministrators$<DPM server name>** local groups on the computer that is running the remote instance of SQL Server. You must add DPM administrators to these groups for DPM to use the remote instance of SQL Server.
- For the DPM server to access a remote instance of SQL Server through Windows Firewall, you must configure an exception on the computer that is running SQL Server to use port 80.
- You must install the DPM support files on the computer that is running the remote instance of SQL Server. For more information, see Setting up the DPM database.
- You cannot user a clustered instance of SQL Server 2012 to host a remote DPM database.
- You cannot host the DPM database on a SQL Server AlwaysOn deployment.

In addition to installing programs that are required for DPM, SQL Server Setup installs the following programs, which are not required for DPM:

- Microsoft SQL Server Compact 3.5 SP1
- Microsoft SQL Server Compact 3.5 SP1 Query Tools
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft Visual Studio Tools for Applications 2.0
- Microsoft Office 2003 Web Components

Note
These programs are not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall these programs manually.

Data source limits for DPM server

The following table lists the data source limits that a DPM server can protect (if it meets the minimum hardware requirements) and the recommended disk space required for the DPM server.

Platform	Data source limit	Recommended disk space
64-bit computers	600 volumes, of which 300 are replica volumes and 300 are recovery point volumes Data sources are typically spread across approximately 75 servers and 150 client computers.	120 TB per DPM server, with 80 TB replica size with a maximum recovery point size of 40 TB

Requirements for protected computers

For a complete list of DPM protection support for computers and workloads, see the Support Matrix for DPM Protection. Prerequisites for computers running the DPM protection agent are summarized in the following table. If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Protected workload	Prerequisites
Computer volumes	• Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB. • Computers must have the Microsoft .NET Framework 3.5 with Service Pack 1 (SP1) installed.
File Servers	Before you can protect a file server running Windows Server 2008 R2, you must apply the hotfix KB977381 Before you can protect a file server running Windows Server 2008, you must apply the following updates: • KB977381

Protected workload	Prerequisites
	• KB975759
Exchange	Note the following when protecting Exchange: • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006. • The eseutil.exe and ese.dll versions that are installed on the most recent release of Exchange Server must be the same versions that are installed on the DPM server. So if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see **Eseutil.exe and Ese.dll**. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll: a. Install the Microsoft Exchange Server 2007 management tools on the DPM server. b. When you install the management tools, ensure that you install the management tools for the latest version of Microsoft Exchange that you are protecting. For example, if one of your mail servers is running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2007 SP1, you must install the management tools for Microsoft Exchange 2007 SP1. c. At the command prompt, in the **<DPM installation folder>\Bin** directory, use the following syntax with the **fsutil** command to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>** On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe"**

Protected workload	Prerequisites
	"c:\program files\microsoft\Exchange\bin\eseutil.exe"

Hyper-V	To protect Hyper-V, note the following:
	• For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB975354
	• For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in KB975921
	• Before you can protect a computer running Windows Server 2008 with Hyper-V, you must apply the following updates:
	  • KB948465
	  • KB971394

SharePoint	When protecting SharePoint, note the following:
	• Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422
	• If you use the **Office SharePoint Server Search** service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply the following updates:
	  • KB951695
	  • KB941422
	• Before you can protect a computer running Windows SharePoint Services 3.0, you must apply the update in KB941422.
	• Before you can protect Windows SharePoint Services 3.0 data, you must do the following:
	  • Start the Windows SharePoint Services VSS Writer service on the Windows SharePoint Services server and then provide the protection agent with credentials for the Windows SharePoint Services farm.
	  • Install the SQL Server Client components on the front-end Web server of the Windows SharePoint Services farm that DPM is going to protect. For information about installing SQL Server 2008

Protected workload	Prerequisites
	components, see How to: Install SQL Server 2008. If you use the **Office SharePoint Server Search** service, before you can protect Windows SharePoint Services 3.0 data, you must apply the following updates: • KB951695 • KB941422

Administration options

In addition to managing DPM directly from the DPM server, you can use the following options:

- Use DPM Remote Administration
- Use DPM Central Console

DPM Remote Administration

DPM Remote Administration allows you to work on your DPM servers from any computer. It also supports task-based scripting. You can install it on the following operating systems:

- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2008 R2
- Windows Server 2008

Computers from which you want to remotely administer DPM require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

DPM Central Console

With DPM Central Console you can monitor and manage multiple DPM servers from one location. You can monitor and troubleshoot servers running both DPM 2010 QFE2 with feature pack and DPM. DPM Central Console must be installed on Operations Manager server or a computer running Operations Manager Console. You can install it on the following operating systems:

- Windows 7
- Windows Vista

Computers from which you want to run DPM Central Console require the following prerequisites:

Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)

If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Network requirements

The following are the network requirements for System Center 2012 – Data Protection Manager (DPM):

- DPM must be installed on a 64-bit computer that is located in a Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 Active Directory domain.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you can protect the computers using DPM's support for computers in workgroups or untrusted domains. For more information, see Managing Protected Computers in Workgroups and Untrusted Domains.

  DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 forest mode.
- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM does not support disjointed namespaces.

System requirements for System Center 2012 R2 - DPM

This topic summarizes system requirements for System Center 2012 R2- Data Protection Manager (DPM) in Windows Server® 2012 R2.

DPM server hardware requirements

The following table lists the minimum and recommended hardware requirements for the DPM server.

Component	Minimum requirement	Recommended requirement
Processor	1 GHz, dual-core CPU or faster	2.33 GHz quad-core CPU
RAM	4 GB	8 GB
Pagefile	1.5 times the amount of RAM on the computer.	0.2 percent of the combined size of all recovery point volumes, in addition to the minimum required size (1.5 times the amount of RAM

Component	Minimum requirement	Recommended requirement
		on the computer).
Disk space for DPM installation	• DPM installation location: 3 GB • Database files drive: 900 MB • System drive: 1 GB The system drive disk space requirement is necessary if you choose to install the dedicated instance of SQL Server from DPM Setup. If you use a remote instance of SQL Server, this disk space requirement is considerably less.	DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a temporary DPM installation location; therefore, we recommend that the volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool The storage pool does not support Universal Serial Bus (USB)/1394 disks.	1.5 times the size of the protected data	2.5–3 times the size of the protected data
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot record (MBR) disks These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

DPM server operating system requirements

The table below summarizes supported operating systems for the DPM server. Note that only 64-bit operating systems are supported. 32-bit and Itanium architecture–based operating systems are not supported.

Supported operating system
Windows Server 2012 R2, Datacenter and Standard editions
Windows Server 2012, Datacenter and Standard editions
Windows Server 2008 R2 with SP1, Standard and Enterprise editions

DPM server installation requirements and limitations

- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system.
- DPM is designed to run on a dedicated, single-purpose server. The DPM server should not be installed on any of the following:
  - A computer on which the Application Server role is installed.
  - A computer that is an Operations Manager management server
  - A computer on which Exchange Server is running.
  - A computer that is a cluster node.
- DPM is not supported on the Turkish language version of any of the listed Windows Server versions.
- The following prerequisites are required for installation:
  - Microsoft .NET Framework 4.0
  - Microsoft Visual C++ 2008 Redistributable Microsoft Visual C++ 2008 Redistributable
  - Windows PowerShell 3.0
  - Windows Installer 4.5 or later versions
  - Windows Single Instance Store (SIS)
  - Microsoft Application Error Reporting

  Setup automatically installs these if they are not already installed or enabled. If any pre-requisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.
- After you have installed DPM, we recommend that you run Windows Update on the DPM server and, if you use a remote database, on the remote computer where the DPM database is located, and install all important updates or hotfixes.

Disk requirements

DPM requires the following:

- A disk that is dedicated to the storage pool
- A disk that is dedicated to:

- System files
- DPM installation files
- DPM prerequisite software
- DPM database files

Note that:

- DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, disk is defined as any disk device manifested as a disk in Disk Management. For more information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool.
- If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that DPM will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.
- DPM in System Center 2012 R2 Preview can use the following types of storage:
  - .VHD disks that are managed in the VMM library (for virtualized deployments).
  - Pass-through disk with host direct attached storage (DAS)
  - Pass-through iSCSI LUN which is attached to host.
  - Pass-through FC LUN which is attached to host.
  - iSCSI target LUN which is connected to DPM virtual machine directly.
- Short-term or long-term backup to tape will be limited to using iSCSI attached tape libraries, and we recommend a separate NIC for that connection.
- You cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

SQL Server requirements

For the DPM database, DPM requires a dedicated instance of 64-bit SQL Server as follows:

- SQL Server 2012 with SP1 (11.0.3000)—Standard or Enterprise edition.
- SQL Server 2008 R2 with SP2 (10.50.4000)—Standard or Enterprise edition.

When you use a remote instance of SQL Server with the DPM installation, note the following requirements:

- You must install the remote instance of SQL Server before you install DPM.
- A remote instance of SQL Server on a domain controller is not supported.
- The computer that is running a remote instance of SQL Server must be located in the same domain and time zone as the DPM server.
- Setup creates the **DPMDBReaders$<DPM server name>** and **DPMDBAdministrators$<DPM server name>** local groups on the computer that is running

the remote instance of SQL Server. You must add DPM administrators to these groups for DPM to use the remote instance of SQL Server.

- For the DPM server to access a remote instance of SQL Server through Windows Firewall, you must configure an exception on the computer that is running SQL Server to use port 80.
- You must install the DPM support files on the computer that is running the remote instance of SQL Server. For more information, see Setting up the DPM database.
- DPM in System Center 2012 R2 preview supports the use of a clustered instance of SQL Server 2012 to host a remote DPM database, or a reporting server.
- You cannot host the DPM database on a SQL Server AlwaysOn deployment.

In addition to installing programs that are required for DPM, SQL Server Setup installs the following programs, which are not required for DPM:

- Microsoft SQL Server Compact 3.5 SP1
- Microsoft SQL Server Compact 3.5 SP1 Query Tools
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft Visual Studio Tools for Applications 2.0
- Microsoft Office 2003 Web Components

These programs are not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall these programs manually.

Data source limits for the DPM server

The following table lists the data source limits that a DPM server can protect (if it meets the minimum hardware requirements) and the recommended disk space required for the DPM server.

Platform	Data source limit	Recommended disk space
64-bit computers	600 volumes, of which 300 are replica volumes and 300 are recovery point volumes Data sources are typically spread across approximately 75 servers and 150 client computers.	120 TB per DPM server, with 80 TB replica size with a maximum recovery point size of 40 TB

Protected computer requirements

For a complete list of DPM protection support for computers and workloads, see the Support Matrix for DPM Protection. Prerequisites for computers running the DPM protection agent are summarized in the following table. If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Protected workload	Prerequisites
Computer volumes	• Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB. • Computers must have the Microsoft .NET Framework 3.5 with Service Pack 1 (SP1) installed.
File Servers	Before you can protect a file server running Windows Server 2008 R2, you must apply the hotfix KB977381
Exchange	Note the following when protecting Exchange: • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must apply KB940006. • The eseutil.exe and ese.dll versions that are installed on the most recent release of Exchange Server must be the same versions that are installed on the DPM server. So if you're using the 64-bit version of DPM, you must have the 64-bit version of eseutil.exe and ese.dll. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see **Eseutil.exe and Ese.dll**. Do the following to maintain up-to-date copies of eseutil.exe and ese.dll: a. Install the Microsoft Exchange Server 2007 management tools on the DPM server. b. When you install the management tools, ensure that you install the management tools for the latest version of Microsoft Exchange that you are protecting. For example, if one of your mail servers is

Protected workload	Prerequisites
	running Microsoft Exchange 2007 and another mail server is running Microsoft Exchange 2007 SP1, you must install the management tools for Microsoft Exchange 2007 SP1. c. At the command prompt, in the **<DPM installation folder>\Bin** directory, use the following syntax with the **fsutil** command to create a hard link for eseutil.exe: **fsutil hardlink create <link> <target>** On a typical installation, the command would look like the following: **fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"**

Hyper-V	To protect Hyper-V, note the following:
	• For a clustered or non-clustered computer running Windows Server 2008 R2 with Hyper-V, apply the hotfix described in KB975354
	• For a clustered computer running Windows Server 2008 R2 with Hyper-V, also apply the hotfix described in KB975921
	• Before you can protect a computer running Windows Server 2008 with Hyper-V, you must apply the following updates:
	  • KB948465
	  • KB971394

SharePoint	When protecting SharePoint, note the following:
	• Before you can protect a computer running Office SharePoint Server 2007, you must apply the update in KB941422
	• If you use the **Office SharePoint Server Search** service, before you can protect Office SharePoint Server 2007 SP1 data, you must apply the following updates:
	  • KB951695
	  • KB941422

Remote administration requirements

In addition to managing DPM directly from the DPM server, you can use DPM Remote Administration or the Central Console.

DPM Remote Administration allows you to work on your DPM servers from any computer. It also supports task-based scripting.

With DPM Central Console you can monitor and manage multiple DPM servers from one location.

Operating system requirements are summarized in the following table.

Remote Administration Option	Supported Operating System
Remote Administration	• Windows 8.1 preview • Windows 8 • Windows 7 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2
Central Console	

In addition, computers from which you want to remotely administer DPM require the following prerequisites::

- DPM Central Console must be installed on Operations Manager server or a computer running Operations Manager Console. You can install it on the following operating systems:
- Microsoft .NET Framework 4.0 or 4.5
- If any prerequisites cannot be installed during setup, or if you want to install them before you install DPM, you can install them manually. For more information, see Installing Prerequisite Software Manually.

Network requirements

The following are the network requirements for System Center 2012 – Data Protection Manager (DPM):

- DPM must be installed on a 64-bit computer that is located in a Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 Active Directory domain.
- DPM can protect servers and workstations across domains within a forest that has a two-way trust relationship with the domain that the DPM server is located in. If there is not a two-way trust across domains, you can protect the computers using DPM's support for computers in workgroups or untrusted domains. For more information, see Managing Protected Computers in Workgroups and Untrusted Domains.

  DPM supports data protection across forests as long as you establish a forest-level, two-way trust between the separate forests. To set up a forest-level trust relationship, both domains must be in Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 forest mode.

- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).
- DPM does not support disjointed namespaces.

Setting up the DPM database

Data Protection Manager (DPM) requires an instance of SQL Server to host the DPM database. You can use SQL Server 2012, SQL Server 2008 R2 (available on the System Center 2012 SP1 DVD) or SQL Server 2008 R2 with SP1. The setup wizard allows you to setup and configure an instance of SQL Server for use by DPM or you can use an existing instance to host the DPM database. In either case, DPM allows you to either have a local instance of the database for each installation of DPM or a shared instance which is used by multiple DPM servers.

On the prerequisites page of the DPM setup wizards you can choose how you want to setup your database.

Use the dedicated instance of SQL Server: Use this option to install or connect to a local instance of SQL Server to host the DPM database. If you want to use a new instance of SQL Server, DPM allows you to install SQL Server 2008 R2 from the System Center 2012 SP1 DVD and host the DPM database on this instance. On the other hand, if you want to use an existing local instance of SQL Server on the computer that you are installing DPM, you can use that instance to host the DPM database.

Use an existing instance of SQL Server: Use this option to connect to a remote instance of SQL Server that is being shared across multiple DPM servers.

Important

When using a remote instance of SQL Server, you must make sure of the following:

- Enable remote procedure calls (RPC) on the computer on which SQL Server is installed.
- The remote instance of SQL Server is not on a domain controller.
- The computer running SQL Server is in the same domain as the DPM server.
- When you install DPM and specify the remote instance of SQL Server, Setup creates the DPMDBReaders$<DPM server name> and DPMDBAdministrators$<DPM server name> local groups on the computer where the remote instance of SQL Server is installed.
- For the DPM server to access a remote instance of SQL Server through Windows Firewall, on the remote computer, you must configure an incoming exception for sqlservr.exe for the specific instance that you use for the DPM database to allow use of the TCP protocol on port 80.
- After the installation of SQL Server is complete, enable the TCP/IP protocol for the specific instance that you use for the DPM database.
- Use the following SQL Server settings - default failure audit setting and enable password policy checking.

To install DPM using a local SQL Server instance

1. Log on to the computer that will be your DPM server using a domain user account that is a member of the local Administrators group.
2. Start Setup.
3. In the **SQL server settings** section, click **Use an existing instance of SQL Server**, and then click **Check and Install**.
4. On the **Security Settings** page, specify and confirm a strong password for the restricted MICROSOFTDPMAcct and DPMR$<*computer name*> local user accounts, and then click **Next**.

   To enhance security, setup creates the following low-privileged local user accounts:

   - MICROSOFTDPMAcct to run the **SQL Server** and **SQL Server Agent** services.
   - DPMR$<*computer name*> to generate DPM reports by using SQL Server Reporting Services.

   A strong password is typically defined as a password that is at least six characters long, does not contain all or part of the user's account name, and contains at least three of the following four categories of characters: uppercase characters, lowercase characters, base 10 digits, and symbols (such as !, @, #).

   Note
   The password that you specify for these accounts does not expire.

To install DPM using a remote instance of SQL Server

1. Log on to the DPM server with a domain user account that is a member of all the following:
   - The local Administrators group on the DPM server
   - The SQL Server **Sysadmin** fixed server role on the computer running the remote instance of SQL Server

   Note
   After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.
2. Start setup.
3. On the **System Center 2012 – Data Protection Manager (DPM)** screen, click **Install Data Protection Manager**.
4. On the **Prerequisite Checks** page, in the **Instance of SQL Server** box, type the name of the remote SQL Server instance as **<Computer Name>\<Instance Name>**, and then type the credentials for a domain user account that is a member of both the local Administrators group and the SQL Server **Sysadmin** fixed server role on the computer where the remote instance is installed.

   Note
   After setup is complete, you can remove the user account from the local

Administrators group.

Note
A restart is necessary to start the volume filter that DPM uses to track and transfer block-level changes between DPM and the computers it protects, or between the primary and secondary DPM servers.

After installation, your DPM database will be named **DPMDB_<DPMServername>** or **DPMDB_<DPMServername><GUID>**.

After you install DPM, you must perform some required configuration tasks before you can start protecting your data. For more information, see Required Configuration Tasks

Important
Do not use localized characters in the computer name if you want to install DPM using SQL Server remotely.

Installing DPM on a Domain Controller

Use the procedures in this topic to install System Center 2012 – Data Protection Manager (DPM) on a domain controller.

To install DPM on a read-only domain controller (RODC), on the primary domain controller (PDC), perform procedures 1 and 2 (creating security groups and user accounts required for DPM and SQL Server 2008). Allow time for the groups to replicate to the RODC, and then, on the RODC, perform procedures 3 and 4 (installing SQL Server and DPM).

Caution
For a DPM server that is installed on a domain controller, only protection of data sources local to the DPM server is supported. You cannot install agents on other computers to configure protection.

Procedure 1: To create the security groups and user accounts required for DPM

1. On the primary domain controller, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Create the following security groups under **Domain\Builtin**. For each group, accept the default settings for **Scope**: Global and **Group type**: Security.
   - DPMDBReaders$<*Computer Name*>
   - MSDPMTrustedMachines$<*Computer Name*>
   - DPMRADCOMTrustedMachines$<*Computer Name*>
   - DPMRADmTrustedMachines$<*Computer Name*>

- DPMDBAdministrators$<*Computer Name*>
- MSDPMTrustedUsers$<*Computer Name*>
- DPMSCOM$<*Computer Name*>
- DPMRATrustedDPMRAs$<Computer Name>

Where <*Computer Name*> is the computer name of the domain controller on which DPM will be installed.

3. Add the local machine account for the domain controller (**<Computer Name>**) to the **MSDPMTrustedMachines$<Computer Name>** group.
4. On the primary domain controller, create a domain user account with the lowest possible credentials assign it a strong password that does not expire, and then add it to the local Administrators group.

Important
Make a note of this account because you need to use it in a later procedure to configure the SQL Server services during the installation of SQL Server. You can name this user account anything that you want; however, for the purposes of easily identifying the account's purpose, you might want to give it a significant name, such as DPMSQLSvcsAcct. For the purposes of these procedures, this account is referred as the **DPMSQLSvcsAcct** account.

5. On the primary domain controller, create another domain user account with the lowest possible credentials and name the account **DPMR$MACHINENAME**, assign it a strong password that does not expire, and then add this account to the **DPMDBReaders$<Computer Name>** group.

Procedure 2: To create the security groups and user accounts required for SQL Server 2008

1. On the primary domain controller, create the following security groups for SQL Server 2008. For each group, accept the default values for **Scope**: Global and **Group type**: Security.
   - SQLServerSQL2005BrowserUser$<*Computer Name*>
   - SQLServerMSSQLServerADHelperUser$<*Computer Name*>
   - SQLServerReportServerUser$<*Computer Name*>$<*Instance ID*>.$<*Instance Name*>
   - SQLServerMSASUser$<*Computer Name*>$<*Instance Name*>
   - SQLServerDTSUser$<*Computer Name*>
   - SQLServerFDHostUser$<*Computer Name*>$<*Instance Name*>

   Where:

   - <*Computer Name*> is the computer name of the domain controller on which SQL Server 2008 will be installed.
   - <*Instance Name*> is the name of the instance of SQL Server that you plan to create

on the domain controller. The instance name can be any name other than the default DPM instance name (MSDPM2010).

- *<Instance ID>* by default, this is assigned by SQL Server Setup and indicates that the group applies to Reporting Services (MSRS) for the major version of the instance (10) of SQL Server. For this release, this value is **MSRS10_50**.

2. On the primary domain controller, add the domain user account that you created earlier, which is referred to as the **DPMSQLSvcsAcct** account, to the following groups:
   - **SQLServerReportServerUser$<ComputerName>$MSRS10.<InstanceID>**
   - **SQLServerMSASUser$<ComputerName>$<InstanceID>**

Procedure 3: To install SQL Server 2008 R2

1. To install DPM 2010 on a domain controller, you must install SQL Server SP1, Enterprise or Standard Edition, before you install DPM. Log on to the domain controller on which you want to install DPM using the domain user account that you created earlier in procedure 1. For purposes of these procedures, this account is referred to as the **DPMSQLSvcsAcct** account.
2. For step-by-step instructions for installing SQL Server 2008 SP1, see **Installing SQL Server 2008**.

   Important
   On the Server Configuration page of the SQL Server 2008 Setup Wizard, configure the **SQL Server Agent**, **SQL Server Database Engine**, and **SQL Server Reporting Services** services to run under the first domain user account that you created earlier in procedure 1. For purposes of these procedures, this account is referred to as the **DPMSQLSvcsAcct** account.
3. After SQL Server is installed, open SQL Server Configuration Manager, expand **SQL Server Network Configuration**, click **Protocols**, right-click **Named Pipes**, and then click **Enable**.

   Note
   For this change to take effect, you must stop and restart the SQL Server service.

Procedure 4: To install DPM

1. For step-by-step instructions for installing DPM, see Installing DPM. In the Setup Wizard, use the settings in the following steps to complete the specified wizard pages.
2. On the **Installation Settings** page, in the **SQL server settings** section, click **Use an existing instance of SQL Server 2008**.
3. On the **SQL Server Settings** page, in the **Instance of SQL Server** box, type the name of the instance of SQL Server that you installed in procedure 3, as localhost*<Instance Name>*, and then type the credentials for the first domain user account that you created in procedure 1. For purposes of these procedures, this account is referred to as the **DPMSQLSvcsAcct** account.

Note

The user account must be a member of the local Administrators group on the domain controller where the remote instance is installed. After setup is complete, you can remove the user account from the local Administrators group.

4. On the **Security Settings** page, enter the same password that you used when you created the **DPMR$MACHINENAME** user account in procedure 1.
5. Open SQL Server Management Studio and connect to the instance of SQL Server that DPM is configured to use. Click **New Query**, copy the text below to the right pane, and then press F5 to run the query.

```
use DPMDB
declare @refresh_jobid uniqueidentifier
select @refresh_jobid = ScheduleId from
tbl_SCH_ScheduleDefinition where JobDefinitionId in
(select JobDefinitionId from tbl_JM_TaskDefinition where
TaskDefinitionId in (select distinct TaskDefinitionID from
tbl_TE_TaskTrail
where VerbID = '53603503-C4C8-4D0E-8F1E-D2F3868E51E3')) and
IsDeleted=0
exec msdb.dbo.sp_update_job @job_name =@refresh_jobid,
@enabled=0
update tbl_SCH_ScheduleDefinition
set IsDeleted=1
where ScheduleId = @refresh_jobid
```

See Also

Installing DPM

System Requirements for DPM in System Center 2012

Installing DPM in a virtual environnment

With the release of the new version of System Center 2012 R2 - Data Protection Manager (DPM), you have the option to install DPM on virtual machines. The installation and storage configuration process remains the same as a physical installation, but with following virtual considerations.

- For high availability DPM storage, virtual hard drives should be placed on scaled-out file servers.
- Virtual DPM installation is not advised for scaled up environments. Instead, use direct attach/SAN-based storage.

- There is no size limit for VHDX.
- Both fixed and dynamically expanding VHDX files are supported.
- Both VHD and VHDX files are supported in the DPM storage pool.
- For dynamic and fixed virtual hard drives, VHD and VHDX files are supported on remote SMB shares.
- Performance can suffer in scaled up (Hyper-V on CSV) environments using VHDX files compared to SAN. Therefore, for scaled up environments we don't recommend using VHDX.
- Virtual DPM installations do not support the following:
    - Windows 2012 Storage Spaces.
    - Virtual hard drives built on top of storage spaces.
    - Local or remote hosting of VHDX files on Windows 2012 storage spaces.
    - Enabling Disk Dedupe on volumes hosting virtual hard drives.
    - Using synthetic FC to connect to tape drives.
    - Windows 2012 iSCSI targets (which use virtual hard drives) as a DPM storage pool.
    - NTFS compression for volumes hosting VHD files used in the DPM storage pool.
    - Bitlocker on volumes hosting VHD files used for the storage pool.
    - A native 4K sector size of physical disks for VHDX files in the DPM storage pool.
    - SMB 3.0 shares for hosting the DPM storage pool.
    - Virtual hard drives hosted on Windows 2008 servers.

Installing Prerequisite Software Manually

System Center 2012 – Data Protection Manager (DPM) requires a SQL Server 2008 R2 instance for the DPM database. During setup, you can choose to have Setup install SQL Server on the DPM server, or you can specify a remote SQL Server instance to use with DPM.

For step-by–step instructions on how to manually install and configure a remote instance of SQL Server for DPM, see Setting up the DPM database.

Using a remote SQL Server instance requires that the DPM support files is installed on the remote computer. For step-by-step instructions, see To manually install the support files.

Depending on which supported operating system you use, there are updates that you must apply before installing DPM. For a list of the supported operating systems, the required updates for each, and links that you can use to download and install the updates, see **DPM Server Software Prerequisites**.

Setup automatically installs the prerequisites in the following table. If you need to manually install one or more of the prerequisites, you can use the procedures and links in this topic.

DPM prerequisite	How to install manually
.NET Framework 3.5 with Service	**For a computer that is running Windows**

DPM prerequisite	How to install manually
Pack 1 (SP1) or later	**Server 2008** To install this application from the DVD, navigate to the following path, and start the installation as Administrator **dotNetFx35setup.exe**. **<root directory>\Redist\DotNetFrameworks** To download and install this application, go to Microsoft .NET Framework 3.5 Service Pack 1. **For a computer that is running Windows Server 2008 R2 or later** In Server Manager, use the **Add Features** action to enable .NET Framework 3.5.1 role.
Microsoft Visual C++ 2008 Redistributable	To install this application from the DVD, navigate to the following path, and start the installation as Administrator **vcredist_x64.exe**. **<root directory>\Redist\vcredist** To download and install this application, go to Microsoft Visual C++ 2008 Redistributable Package (x64)
Windows PowerShell 2.0 **Note** Windows PowerShell 1.0 is included in Windows Server 2008. If you install DPM on Windows Server 2008, the Setup Wizard automatically installs Windows PowerShell 2.0. Windows PowerShell 2.0 is included in Windows Server 2008 R2.	To download and install this application as part of the Windows Management Framework Core package, go to Update for Windows Server 2008 x64 Edition (KB968930).
Windows Installer 4.5 or later **Note** Windows Server 2008 includes Windows Installer 4.5 and Windows Server 2008 R2 includes Windows Installer 5.0.	To install this application from the DPM product media, navigate to the following path, and start the installation as Administrator **INSTMSI45.EXE**. **<root directory>DPM2012\setup\redist\WindowsInstaller**

DPM prerequisite	How to install manually
Windows Single Instance Store (SIS)	To install this application, follow the procedure later in this topic.
Microsoft Application Error Reporting	To install this application from the DPM product media, navigate to the following path, and start the installation as Administrator **dw20sharedamd64.msi**. **<root directory>DPM2012\setup\redist**

To manually install Windows Single Instance Store (SIS)

1. On the computer that will be your DPM server, open an elevated command prompt window, and run the following command.

```
start /wait ocsetup.exe SIS-Limited /quiet /norestart
```

   Note
   The service name is case-sensitive so you must type **SIS-Limited**. The installation fails if you type **sis-limited** or **SIS-limited**.

2. After the installation is complete, you must restart the computer.

Note

SIS.sys is a third-party driver and may not have the Windows Hardware Quality Labs (WHQL) signature. It is not removed during DPM uninstallation.

If you use a remote SQL Server instance for DPM, you must manually install the support files on the remote computer. Use the following procedure to install the DPM support files.

To manually install the support files

1. On the remote computer running SQL Server, run the System Center 2012 Service Pack 1 (SP1) DPM installer.
2. On the installation screen, select **DPM Remote SQL Prep**.
3. Follow the steps in the wizard to install the DPM support files.

See Also

Installing DPM

System requirements for System Center 2012 - DPM

Software Requirements

System requirements for System Center 2012 R2 - DPM

Upgrading the DPM Database

An important part of upgrading to System Center 2012 – Data Protection Manager (DPM) is upgrading the DPM database (DPMDB). With the multi-database feature, DPM allows you to consolidate the databases of all your DPM servers to one SQL Server instance. When upgrading, you have to choose one of three scenarios.

- Local SQL Server instance to Local SQL Server instance

  Use this option if you want to continue to have DPMDB on the same computer as DPM.
- Local SQL Server instance to remote SQL Server instance

  Use this option when you want to move from using a local instance of DPMDB to a remote instance. Using this feature, one instance of SQL Server can host the databases of multiple DPM servers.
- Remote SQL Server instance to Remote SQL Server instance

  Use this option when you want to continue to use a remote instance of SQL Server to host the DPMDB. Using this feature, one instance of SQL Server can host the databases of multiple DPM servers.

Important

- Upgrade your DPM servers sequentially. Parallel upgrades may lead to errors.
- If you are using an existing instance of SQL Server, you must run DPM Remote SQL Prep tool from the Setup splash screen on the instance of SQL Server you are going to use.
- You cannot share an instance of SQL Server installed by DPM. We recommend you use it only for DPM databases.
- TCP/IP protocol must be enabled on SQL Server and TCP/IP client protocol on DPM server.
- When setting up tape library sharing, provide the complete name as <servername>\<instancename>\<databasename>.
- The naming conventions for the DPM database have changed with this new feature, and you can find the name of the database from the Information button on the Administrator console.

Local SQL Server instance to Local SQL Server instance

1. Backup DPMDB.
2. Add MicrosoftDPMACCT to the ACL for the DPMDB folder, if it doesn't exist. Add full control to the user.
3. Launch System Center 2012 – Data Protection Manager (DPM) installation. This will start setup in upgrade mode.

Local SQL Server instance to remote SQL Server instance

1. Ensure that the domain user account you will use to install DPM is a member of all the following:
   - The local Administrators group on the DPM server.

- The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

Note

After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.

2. Backup DPMDB.
3. Add MicrosoftDPMACCT to the ACL for the DPMDB folder, if it doesn't exist. Add full control to the user.
4. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 which you plan to use to host databases of multiple DPM servers.

Note

The name of the restored database should be DPMDB.

This instance of SQL Server should be used only for hosting DPM databases only.

5. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
6. Install SQL Prep Tool on the remote computer running SQL Server. You can find this on the Setup page.
7. Launch DPM installation. This will start setup in upgrade mode.

Remote SQL Server instance to Remote SQL Server instance

1. Ensure that the domain user account you will use to install DPM is a member of all the following:
   - The local Administrators group on the DPM server.
   - The local Administrators group on the computer on which you have installed the remote instance of SQL Server 2008 R2.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

Note

After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.

2. Backup DPMDB.
3. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 that you plan to use to host databases of multiple DPM servers.

Note

- The name of the restored database should be the same as the DPM database you backed up.
- This instance of SQL Server should be used only for hosting DPM databases only.

4. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
5. Install SQL Prep Tool on the remote instance of SQL Server.
6. Launch DPM installation. This will start setup in upgrade mode.

See Also

Installing DPM Using a Remote Instance of SQL Server 2008

Installing Central Console

Central Console allows you to monitor and manage multiple DPM servers from one location. In this section, we discuss how you can install Central Console. DPM supports three installation scenarios for Central Console.

Using Central Console, you can monitor and troubleshoot:

- System Center 2012 Service Pack 1 (SP1) Data Protection Manager (DPM)
- System Center 2012 – Data Protection Manager (DPM)
- System Center Data Protection Manager 2010 QFE3 with feature pack

After you install Central Console, there will be four shortcuts on your desktop – one for the Administrator Console and one each for the Management Shells of DPM 2010, System Center 2012 – DPM and System Center 2012 Service Pack 1 (SP1) DPM.

Caution
If you open the Remote Administrator Console from a computer running Windows Server 2012 or Windows 8, you can only manage System Center 2012 Service Pack 1 (SP1) DPM.

Important
System Center 2012 – Data Protection Manager (DPM) only works with System Center 2012 – Operations Manager.

You must install the Operations Manager agent on all the DPM servers that you will be monitoring.

After you install the Operations Manager agent, set the following registry key - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Modules\Global\PowerShell] "ScriptLimit"=dword:0000000f

After you make the preceding change, you must restart the Health Service (Display name: 'System Center Management').

Warning
Central Console will not discover computers running prerelease versions of Data Protection Manager (DPM).

Important
Do not install the Central Console server components on a computer running only Operations Manager Console or which has SQL Prep Tool is installed.

After you have installed the Central Console management pack, in the State view, under DPM (Need upgrade), you will be shown the DPM 2010 servers that need an upgrade.

Important
If you need to uninstall Operations Manager, you must follow the instructions recommended by Operations Manager. For more information, see How to Uninstall Operations Manager.

Supported operating systems

Server operating systems

- Windows Server 2012
- Windows Server 2008 R2 SP1

Client operating systems

- Windows 8
- Windows Vista
- Windows 7

Important
DPM does not support installing Central Console or Remote Administration on Windows XP.

To install client and server features

When you install both the server and client features, you can monitor DPM servers on which the Operations Manager agent is present and use the scoped DPM Administrator console.

Note
DPM adds firewall exceptions for port 6075 to enable scoped Administrator console. Open ports for SQL Server.exe and SQL browser.exe.

Procedure to install client and server features

1. Start Operations Manager Console and Importing the management pack
2. On the Setup screen, click **Install Central Console**.
3. Click **Install Central Console Server and Client side Components** option.

To install only server features

When you install only the server features, you can monitor DPM servers on which the Operations Manager agent is present, but you cannot use the scoped DPM Administrator console.

Note
DPM adds firewall exceptions for port 6075 to enable scoped DPM Administrator console. Open ports for SQL Server.exe and SQL browser.exe.

Procedure to install server features

1. Start Operations Manager Console and Importing the management pack.
2. On the Setup screen, click **Install Central Console**.
3. Click **Install Central Console Server side Components** option.

To install only client features

When you install only the client features, you can use the scoped Administrator console but you cannot monitor DPM servers.

Procedure to install client features

1. On the Setup screen, click **Install Central Console**.
2. Click **Install Central Console Client side Components** option.
3. Start Operations Manager Console.

Importing the management pack

1. Remove existing System Center 2012 – Data Protection Manager (DPM) management packs.
2. Import System Center 2012 – Data Protection Manager (DPM) management packs. The Central Console consists of two management packs - Microsoft.SystemCenter.DataProtectionManager.2012.Discovery.mp and Microsoft.SystemCenter.DataProtectionManager.2012.Library.mp - import both management packs. The management packs are located at <CDDrive:>\Management Packs.

   Note
   When you import the management pack, Windows displays a warning about write actions. This is an expected warning, and you can click **OK** to continue.

Upgrading System Center - DPM

System Center 2012 – Data Protection Manager (DPM) supports an upgrade from System Center Data Protection Manager 2010 with QFE4 (KB2615782) installed on a Windows Server 2008 R2 or Windows Server 2008 64-bit operating system.

Before you begin the upgrade of DPM 2010, note the following requirements and recommendations:

- Install the latest hotfixes for DPM 2010. For the latest updates and hotfixes for DPM, see Downloads for System Center Data Protection Manager.
- Ensure that DPM 2010 is installed on a Windows Server 2008 R2 or Windows Server 2008 64-bit operating system.
- Ensure that the hard disk on which DPM 2010 is installed has at least 4.5 gigabytes (GB) of free disk space.
- We strongly recommend that you back up the DPM 2010 database and save the backup file in a secure location.
- If you are sharing a tape library, you must stop sharing it. You can enable tape library sharing after installing DPM successfully. For more information, see Removing library sharing
- If you are using a remote instance of SQL Server, we recommend install a new instance of SQL Server 2008 R2, Standard or Enterprise Edition. For step-by-step instructions for installing a remote instance of SQL Server, see **Installing a Remote Instance of SQL Server 2008**.

Before you begin the upgrade of DPM 2010, note the following additional considerations:

- After you upgrade DPM 2010, you must upgrade agents on protected computers for protection to continue. For more information, see Post-upgrade steps.
- The protected computer should be running Windows Server 2003 SP2 or later.
- If a protected computer is running Windows Server 2003 SP2, Windows Server 2008 or Windows Vista, you should download and install the following hotfix, An application or service that uses a file system filter driver may experience function failure on a computer that is running Windows Vista, Windows Server 2003, or Windows Server 2008.

In This Section

Upgrading to System Center 2012 R2 - DPM

Data Protection Manager (DPM) running on System Center 2012 Service Pack 1 (SP1) can be upgraded to Data Protection Manager (DPM) running on System Center 2012 R2. This topic describes prerequisites and deployment steps for the upgrade.

- Prerequisites for upgrading to DPM in System Center 2012 R2
- Upgrading DPM
- Upgrading the DPM Database
- Upgrading a DPM server backing up DPM
- Post-upgrade steps
- Retrying a failed upgrade
- Rolling back an upgrade

Warning

If you are upgrading two or more System Center components, you must follow the procedures that are documented in the Upgrade Sequencing for System Center 2012 R2 topic.

The order in which you perform component upgrades is very important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

- Orchestrator
- Service Manager
- Data Protection Manager (DPM)
- Operations Manager
- Configuration Manager
- Virtual Machine Manager (VMM)
- App Controller

Prerequisites for upgrading to DPM in System Center 2012 R2

This topic summarizes prerequisites for upgrading to DPM in System Center 2012 R2 Preview:

- If you are planning to upgrade two or more System Center components, it is imperative that you first consult the guide Upgrade Sequencing for System Center 2012 SP1. The order in which you perform component upgrades is important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are Orchestrator; Service Manager; Data Protection Manager (DPM); Operations Manager; Configuration Manager; Virtual Machine Manager; and App Controller.

- Ensure that the hard disk on which DPM is installed has at least 4.5 gigabytes (GB) of free disk space.
- Install the latest DPM updates on the DPM server and protected computers.
- You must back up the DPM database and save the backup file in a secure location.
- If you are upgrading your instance of SQL Server to SQL Server 2012, we recommend installing a new instance of SQL Server 2012 before proceeding with the upgrade. For step-by-step instructions for installing a remote instance of SQL Server, see Setting up the DPM database. Then migrate your database using the steps outlined in Remote SQL Server instance to Remote SQL Server instance.
- Upgrade will require upgrading the DPM protection agents, which might force a restart of your protected computer.
- After upgrade, DPM will mark all replicas as inconsistent. You must run a manual consistency check after upgrade.
- If a protected computer is running Windows Server 2003 SP2, Windows Server 2008 or Windows Vista, you should download and install the following update, KB 975759.
- If you are sharing a tape library across multiple servers running System Center 2012 – Data Protection Manager (DPM), you must remove library sharing before you upgrade to System Center 2012 SP1 DPM.
- If you have library sharing enabled, disable it and then backup your DPM dataset. You can enable tape library sharing after installing DPM successfully. Remove library sharing as follows:

To remove library sharing

1. On each library client computer, open an elevated command prompt, and then run the following commands:

   cd <system drive> :\Program Files\Microsoft DPM\DPM\Setup

   SetSharedDPMDatabase.exe –RemoveDatabaseSharing

   AddLibraryServerForDPM.exe –DPMServerWithLibrary <*FQDN of the library server*> **-remove**

   where <*FQDN of library server*> is the fully qualified domain name of the library server.
2. Upgrade DPM on the library client computers.
3. Repeat steps 1 and 2 for all library client computers.
4. After you have removed library sharing and upgraded DPM on all library clients, on the library server, open an elevated command prompt, and then run the following commands one time for each library client:

   cd <system drive> :\Program Files\Microsoft DPM\DPM\Setup

   For each library client, run:

   AddLibraryServerForDpm.exe – ShareLibraryWithDpm <FQDN of library client> -remove

where *<FQDN of library client>* is the fully qualified domain name of the library client.

Then run the following command one time:

SetSharedDPMDatabase.exe -RemoveDatabaseSharing

5. Upgrade DPM on the library server.
6. After you have upgraded DPM on the library server, reconfigure tape library sharing. For step-by-step instructions about how to configure library sharing, see Setting up Tape Library Sharing.

Upgrading DPM

This topic describes the steps required to upgrade from DPM in System Center 2012 SP1 to DPM in System Center 2012 R2 Preview.

Before you start

- Do not start any of the setup modules by running the exe files. You must start the setup components from the main setup screen.
- If you want to use a remote SQL instance, run Setup.exe on the SQL Server and select DPM Remote SQL Prep tool from the Setup page.

Upgrading from DPM System Center 2012 in SP1

1. Run Setup.exe on the DPM server and select **Data Protection Manager** from the **Install** list.
2. On the Use the Microsoft Software License Terms page, click I **accept the license terms and condition**s to start Setup. Then click **OK**. If you don't want to accept the terms, click **Cancel** to exit Setup.
3. On the Welcome page, click **Next**.
4. On the Prerequisites Check page, click **Check and Install** to verify that the computer meets the Setup requirements. Note the following:
   - Before you begin the prerequisites check, you must specify whether the DPM database will be on a dedicated instance or an existing instance of SQL Server. If you chose to use an existing instance, the wizard will prompt for details of the instance. In DPM in System Center 2012 R2 Preview, the remote SQL Server can be a standalone server, or a member of a SQL Server cluster.
   - If the "check item failed" symbol appears for one or more required or recommended components, Setup displays one of the following:
     - **Warning**. Indicates that a recommended component is missing or noncompliant. Review the alert and determine whether to resolve the issue now or continue with the installation. If any recommended component is missing, you can click **Next**, and DPM will install the required prerequisite software.

       Note

The installer does not install Windows updates. You must download and install them yourself.

- **Error**. Indicates that a required component is missing or noncompliant. Resolve the error, and then click **Check** to verify all components are installed before you continue with the installation.
- When the prerequisite check is complete and all required components are present, Setup displays a confirmation, and the **Next** button becomes available.

5. On the Product Registration page, specify the identification information that is used to register your copy of DPM, as follows:
   - In **User name**, Type your name. When you install DPM, provide the name of a user responsible for administering the DPM server. A user name is required to continue Setup.
   - In **Company**, optionally specify the name of your organization.
   - In **Product key**, specify the key that came with your DVD.
   - In **Client licenses**, specify the number of licenses that you have purchased to authorize protection of client computers (laptops and desktops).
   - In **Standard licenses**, specify the number of licenses that you have purchased to authorize protection of file resources and system state.
   - In **Enterprise licenses**, specify the number of licenses that you have purchased to authorize protection of both file and application resources.
6. After you enter your identification information, click **Next**.
7. On the Installation Settings page, specify where you want to install the the DPM program and database files. Note the following:
   a. The files can be installed only on a local drive. They cannot be installed on read-only folders, hidden folders, or directly on local Microsoft Windows folders, such as Documents and Settings, Windows NT, or Program Files. (However, the files can be installed on a subfolder in the Program Files folder.)
   b. The installation partition must be formatted with the NTFS file system. To ease recovery if a boot partition failure occurs, install DPM on a partition that is separate from the boot partition.
   c. In **Program Files**, click **Change** to modify the default DPM program files installation location.
   d. In **Database files**, click **Change** to modify the default installation location for the DPM database.
   e. The **Space Requirements**, verify that the selected drives have enough space for the installation.
8. After you enter your installation settings information, click **Next**.
9. On the Security Settings page, specify security settings as follows:
   - In **Password**, type a strong password for the restricted MICROSOFTDPMAcct and DPMR$<computer name> accounts. For security purposes, DPM runs the instance of Microsoft SQL Server and the SQL Server Agent service under the MICROSOFTDPMAcct account, which DPM Setup creates during the installation.

To securely generate reports, DPM creates the DPMR$<computer name> account. Note the following:

- Setting strong passwords is essential to the security of your system. A strong password is a password that is at least six characters long, does not contain all or part of the user's account name, and contains at least three of the following four categories of characters: uppercase characters, lowercase characters, base 10 digits, and symbols (such as !, @, #).
- The password that you provide does not expire.
- DPM sets the system administrator (SA) password for the instance of SQL Server to the same password that you specify for the MICROSOFTDPMAcct account.

10. After you reconfirm the password, click **Next**.
11. On the Microsoft Update Opt-In page, optionally sign up for the Microsoft Update server. To sign up, select **Use Microsoft Update when I check for updates**. Note that signing up for this service delivers not only DPM updates, but all critical and required updates from the Microsoft Update Catalog.
12. After you select the Microsoft Update service option, click **Next**.
13. On the Customer Experience Improvement Program page, select whether you want to participate in the Microsoft Customer Experience Improvement Program (CEIP). The CEIP collects data about your use of Microsoft applications to identify possible improvements. To participate, click **Yes, I want to participate anonymously in this program**. Alternatively, click **No, remind me later** to decline enrolment. You can change your CEIP enrollment choice at any time in DPM Administrator Console options.

    After you choose your CEIP option, click **Next** to continue.
14. On the Summary page, confirm the installations settings, and click **Install** to continue.
15. On the Installation page you can monitor Setup progress. Click **Cancel** at any time to exit Setup. When the installation is complete, **Finish** to exit the DPM Setup Wizard.

Important

After Setup is complete the following is configured:

- Setup upgrades the local SQL instance hosting the DPM database to SQL Server 2008 R2 SP2.
- Setup adds firewall exceptions for port 6075 to enable a scoped DPM Administrator console.
- Setup adds the DPMSCOM group to Windows groups.
- Setup adds the MSDPM Trusted Users group to Windows groups.
- Setup adds the following new event logs: DPM Backup event and DPM alert.

For post-upgrade steps, see Post-upgrade steps.

Upgrading the DPM Database

An important part of upgrading to System Center 2012 R2 Data Protection Manager is upgrading the Data Protection Manager database (DPMDB). With the multi-database feature, Data Protection Manager allows you to consolidate the databases of all your Data Protection Manager servers to one SQL Server instance. When upgrading, you have to choose one of three scenarios.

- Local SQL Server instance to Local SQL Server instance

  Use this option if you want to continue to have DPMDB on the same computer as Data Protection Manager.
- Local SQL Server instance to remote SQL Server instance

  Use this option when you want to move from using a local instance of DPMDB to a remote instance. Using this feature, one instance of SQL Server can host the databases of multiple Data Protection Manager servers.
- Remote SQL Server instance to Remote SQL Server instance

  Use this option when you want to continue to use a remote instance of SQL Server to host the DPMDB. Using this feature, one instance of SQL Server can host the databases of multiple Data Protection Manager servers.

Note

From DPM in System Center 2012 R2, the remote SQL Server can be a standalone server, or part of a SQL Server cluster.

Important

- Upgrade your Data Protection Manager servers sequentially. Parallel upgrades may lead to errors.
- If you are using an existing instance of SQL Server, you must run Data Protection Manager Remote SQL Prep tool from the Setup splash screen on the instance of SQL Server you are going to use. All the Data Protection Manager databases on this instance must be upgraded.

  The remote SQL Server can have only one version of SQL Prep tool on it. You cannot upgrade the tool for only selected databases.
- You cannot share an instance of SQL Server installed by Data Protection Manager. We recommend you use it only for Data Protection Manager databases.
- TCP/IP protocol must be enabled on SQL Server and TCP/IP client protocol on Data Protection Manager server.
- When setting up tape library sharing, provide the complete name as <servername>\<instancename>\<databasename>.
- The naming conventions for the Data Protection Manager database have changed with this new feature, and you can find the name of the database from the Information button on the Administrator console.

Local SQL Server instance to Local SQL Server instance

1. Backup DPMDB.
2.

   Important
   Setup will upgrade the SQL Server instance to SQL Server 2008 R2 SP2.

   Launch Data Protection Manager installation. This will start setup in upgrade mode.

Local SQL Server instance to remote SQL Server instance

1. Ensure that the domain user account you will use to install Data Protection Manager is a member of all the following:
   - The local Administrators group on the Data Protection Manager server.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2 or SQL Server 2012.

   Note
   After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.
2. Backup DPMDB.
3. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 or SQL Server 2012 where you plan to use to host databases of multiple Data Protection Manager servers.

   Note
   The name of the restored database should be DPMDB.

   This instance of SQL Server should be used only for hosting Data Protection Manager databases only.
4. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
5. Install SQL Prep Tool on the remote computer running SQL Server. You can find this on the Setup page.
6. Launch Data Protection Manager installation. This will start setup in upgrade mode.

   Select **Existing instance of SQL Server** as your database.

Remote SQL Server instance to Remote SQL Server instance

1. Ensure that the domain user account you will use to install Data Protection Manager is a member of all the following:
   - The local Administrators group on the DPM server.
   - The local Administrators group on the computer on which you have installed the remote instance of SQL Server 2008 R2.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

Note

After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.

2. Backup the Data Protection Manager database.
3. Restore the Data Protection Manager database backup to a remote instance of SQL Server that you plan to use to host databases of multiple Data Protection Manager servers.

Note

- The name of the restored database should be the same as the Data Protection Manager database you backed up.
- This instance of SQL Server should be used only for hosting Data Protection Manager databases only.

4. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
5. Install SQL Prep Tool on the remote instance of SQL Server.
6. Launch Data Protection Manager installation. This will start setup in upgrade mode.

Use the above steps in case you are moving from one remote SQL Server instance to another. If you are going to use an existing remote instance then simply provide that instance's credentials.

Important

Remember to back up the Data Protection Manager database before you perform this action.

Upgrading a backup DPM server

This topic provides guidance for upgrading a secondary System Center 2012 R2 Data Protection Manager server that is being used as a backup for a primary server.

Caution

When upgrading to System Center 2012 R2 Data Protection Manager, if you are protecting system state and you have customized the location of the backup that is staged, this customization will be lost in the **PSdataSourceConfig.xml** file during the upgrade. The staging location will be set to the drive with the largest available disk space.

To upgrade a DPM server that is being protected by another DPM server

1. Upgrade the secondary server. For step-by-step instructions for upgrading a Data Protection Manager server, see Upgrading System Center - DPM.
2. On the primary server, close Administrator Console and Management Shell.

3. On the primary server, start the Setup Wizard, complete the upgrade, and then restart the computer.
4. Upgrade protection agents on all protected servers.
5. Run a consistency check on all protected data sources.

To upgrade a DPM server that is protecting another DPM server

1. Upgrade the secondary server. For step-by-step instructions for upgrading a Data Protection Manager server, see Upgrading System Center - DPM.
2. On the secondary server, close Administrator Console and Management Shell.
3. On the secondary server, start the Setup Wizard, complete the upgrade, and then restart the computer.
4. Upgrade each primary server that is being protected, and then reinstall the protection agent of each.
5. Upgrade protection agents on all protected servers.
6. Run a consistency check on all protected data sources.

Post-upgrade steps

After upgrading to System Center 2012 R2 Data Protection Manager, note the following:

- You must upgrade all of the protection agents. This might require a restart of the protected computer.
- After upgrading the Data Protection Manager server and the protection agents, all of your data sources will be marked as inconsistent. Upgrade the respective protection agents, and then perform a consistency check.
- Reconfigure tape library sharing.
- If you had Hyper-V Live Migration configured before doing the upgrade, you must run `Set-DpmGlobalProperty -KnownVmmServers <VmmServerName>` to continue protection.

To perform an agent upgrade by running the DPMAgentInstaller.exe

1. In the SCDPM folder of the setup DVD, open the **Agents** folder, and then copy **DPMAgentInstaller_x64.exe** and **DPMAgentInstaller_x86.exe** to a network share.
2. Log on to the protected computers, navigate to the network share, and then run the appropriate **DPMAgentInstaller.exe** command.

   ```
   DpmAgentInstaller.exe [/q] [<DPM server name>] [/IAcceptEula]
   ```

   Note
   Only agents that are running version System Center 2012 SP1 DPM can be upgraded. For agents that are running any other version, you must uninstall the agent, and then install the System Center 2012 R2 Data Protection Manager

agent.

To configure secondary protection

1. On the secondary DPM server, launch the Data Protection Manager Agent Installation Wizard.
2. Select **Install Agents**.
3. Select the primary Data Protection Manager servers that the secondary Data Protection Manager protects.
4. Complete the protection agent installation.

Retrying a failed upgrade

This topic guides you through the process of retrying your System Center 2012 R2 Data Protection Manager upgrade if your previous attempt failed.

Before you retry the upgrade, check the logs at C:\Program Files\Microsoft System Center 2012\DPM\DPMLogs to see why the upgrade failed. After you have taken corrective action, follow the steps outlined here.

To retry the DPM upgrade

1. Back up the Data Protection Manager database.
2. Uninstall the failed Data Protection Manager upgrade while retaining your data by clicking **Retain disk-based recovery points** on the **Uninstallation Options** page. For step-by-step instructions for uninstalling Data Protection Manager, see Uninstalling DPM.
3. Delete the Data Protection Manager database.
4. Reinstall System Center 2012 SP1 Data Protection Manager and all updates in the same sequence as they were installed to the return to the same state as the original installation.

   Tip
   Run the following query on the System Center 2012 SP1 Data Protection Manager database in Administrator mode to find the sequence in which the updates were originally applied.

   select * from tbl_DPM_InstalledUpdates
5. Restore the saved System Center 2012 SP1 Data Protection Manager database files.
6. Retry the upgrade.

To back up the DPM database

1. On the computer where the Data Protection Manager database is installed, open

Microsoft SQL Server Management Studio for SQL Server 2008 R2 and then connect to the instance of SQL Server that System Center 2012 – Data Protection Manager (DPM) was using.

2. Take a backup of the Data Protection Manager database. To back up a database, right-click the database, click **Tasks**, and then click **Backup**.
3. Store this backup file to a safe location.

Rolling back an upgrade

If your upgrade to System Center 2012 R2 Data Protection Manager does not complete successfully, or if you need to go back to System Center 2012 SP1, you can roll back the upgrade without losing the benefit of protection that you previously had.

To roll back a DPM upgrade

1. Backup your Data Protection Manager database.
2. If Data Protection Manager is installed, uninstall it while retaining your data by clicking **Retain disk-based recovery points** on the **Uninstallation Options** page. For step-by-step instructions for uninstalling DPM, see Uninstalling DPM.
3. Install System Center 2012 R2 Data Protection Manager. If you had any updates installed, reinstall them in the same sequence that you had installed them the first time.

   Tip
   Run the following query on the System Center 2012 SP1 DPM database in Administrator mode to find the sequence in which the updates were originally applied.

   select * from tbl_DPM_InstalledUpdates
4. Before you began the upgrade, you should have backed up your DPM database and stored it in a safe location.

   To restore the System Center 2012 SP1 DPM database to the SQL Server instance that DPM was using previously, open DPM Management Shell and run the command `dpmsync -restoredb`..
5. To synchronize the databases, in DPM Management Shell, run the command `dpmsync -sync`.
6. Open DPM Administrator Console and ensure that all agents are the same version as the DPM server.
7. Perform a consistency check on all the data sources.

Caution
If DPM was functional after installation, any recovery points created will be lost. Recovery points created prior to upgrading will still be available.

Upgrading to System Center 2012 SP1 - DPM

System Center 2012 Service Pack 1 (SP1) Data Protection Manager (DPM) supports an upgrade from System Center 2012 – Data Protection Manager (DPM) with Update Rollup 3 (KB2751230) installed on a Windows Server 2008 R2 SP1 operating system.

Warning

If you are planning to upgrade two or more System Center components, it is imperative that you first consult the guide Upgrade Sequencing for System Center 2012 SP1. The order in which you perform component upgrades is important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator
2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

Caution

- Upgrade will require upgrading the DPM protection agents, which might force a restart of your protected computer.
- After upgrade, DPM will mark all replicas as inconsistent. You must run a manual consistency check after upgrade.
- If a protected computer is running Windows Server 2003 SP2, Windows Server 2008 or Windows Vista, you should download and install the following update, KB 975759.
- Upgrade from System Center 2012 SP1 DPM Beta is not supported.

Upgrading DPM

You can do an in-place upgrade from System Center 2012 Data Protection Manager (DPM) to System Center 2012 Service Pack 1 (SP1) Data Protection Manager (DPM).

Before you begin the upgrade, note the following requirements and recommendations:

- Do not start any of the setup modules by running the exe files. You must start the setup components from the main setup screen.
- Install the latest DPM updates on the DPM server and protected computers. For the latest updates and updates for DPM, see Downloads for System Center Data Protection Manager.

- Ensure that the hard disk on which DPM is installed has at least 4.5 gigabytes (GB) of free disk space.
- You **must** back up the DPM database and save the backup file in a secure location.
- If you have library sharing enabled, disable it and then backup your DPM dataset. You can enable tape library sharing after installing DPM successfully. For more information, see Removing library sharing
- If you are upgrading you instance of SQL Server to SQL Server 2012, we recommend installing a new instance of SQL Server 2012 before proceeding with the upgrade. For step-by-step instructions for installing a remote instance of SQL Server, see Setting up the DPM database.

  Then migrate your database using the steps outlined in Remote SQL Server instance to Remote SQL Server instance.
- If you are also upgrading your operating system to Windows Server 2012, you must enable the Deduplication role.

Procedure to upgrade from System Center 2012 DPM

1. If you want to use a remote SQL instance, run Setup.exe on the SQL Server and select DPM Remote SQL Prep tool from the Setup page. For more information on upgrading DPM database, see Upgrading the DPM Database.
2. Run Setup.exe on the DPM server and select Data Protection Manager from the Setup page and follow the wizard.

Important

- Setup upgrades the local SQL instance hosting the DPM database to SQL Server 2008 R2 SP2.
- Setup adds firewall exceptions for port 6075 to enable a scoped DPM Administrator console.
- Setup adds the DPMSCOM group to Windows groups.
- Setup adds the MSDPM Trusted Users group to Windows groups.
- Setup adds the following new event logs: DPM Backup event and DPM alert.

For post-upgrade steps, see Post-upgrade steps.

Upgrading the DPM Database

An important part of upgrading to System Center 2012 – Data Protection Manager (DPM) is upgrading the DPM database (DPMDB). With the multi-database feature, DPM allows you to consolidate the databases of all your DPM servers to one SQL Server instance. When upgrading, you have to choose one of three scenarios.

- Local SQL Server instance to Local SQL Server instance

Use this option if you want to continue to have DPMDB on the same computer as DPM.

- Local SQL Server instance to remote SQL Server instance

  Use this option when you want to move from using a local instance of DPMDB to a remote instance. Using this feature, one instance of SQL Server can host the databases of multiple DPM servers.

- Remote SQL Server instance to Remote SQL Server instance

  Use this option when you want to continue to use a remote instance of SQL Server to host the DPMDB. Using this feature, one instance of SQL Server can host the databases of multiple DPM servers.

Important

- Upgrade your DPM servers sequentially. Parallel upgrades may lead to errors.
- If you are using an existing instance of SQL Server, you must run DPM Remote SQL Prep tool from the Setup splash screen on the instance of SQL Server you are going to use.
- You cannot share an instance of SQL Server installed by DPM. We recommend you use it only for DPM databases.
- TCP/IP protocol must be enabled on SQL Server and TCP/IP client protocol on DPM server.
- When setting up tape library sharing, provide the complete name as <servername>\<instancename>\<databasename>.
- The naming conventions for the DPM database have changed with this new feature, and you can find the name of the database from the Information button on the Administrator console.

Local SQL Server instance to Local SQL Server instance

1. Backup DPMDB.
2. Add MicrosoftDPMACCT to the ACL for the DPMDB folder, if it doesn't exist. Add full control to the user.
3. Launch System Center 2012 – Data Protection Manager (DPM) installation. This will start setup in upgrade mode.

Local SQL Server instance to remote SQL Server instance

1. Ensure that the domain user account you will use to install DPM is a member of all the following:
   - The local Administrators group on the DPM server.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

   Note
   After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.
2. Backup DPMDB.

3. Add MicrosoftDPMACCT to the ACL for the DPMDB folder, if it doesn't exist. Add full control to the user.
4. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 which you plan to use to host databases of multiple DPM servers.

   Note

   The name of the restored database should be DPMDB.

   This instance of SQL Server should be used only for hosting DPM databases only.
5. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
6. Install SQL Prep Tool on the remote computer running SQL Server. You can find this on the Setup page.
7. Launch DPM installation. This will start setup in upgrade mode.

Remote SQL Server instance to Remote SQL Server instance

1. Ensure that the domain user account you will use to install DPM is a member of all the following:
   - The local Administrators group on the DPM server.
   - The local Administrators group on the computer on which you have installed the remote instance of SQL Server 2008 R2.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

   Note

   After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.
2. Backup DPMDB.
3. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 that you plan to use to host databases of multiple DPM servers.

   Note
   - The name of the restored database should be the same as the DPM database you backed up.
   - This instance of SQL Server should be used only for hosting DPM databases only.
4. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
5. Install SQL Prep Tool on the remote instance of SQL Server.
6. Launch DPM installation. This will start setup in upgrade mode.

See Also

Installing DPM Using a Remote Instance of SQL Server 2008

Removing library sharing

If you are sharing a tape library across multiple servers running System Center 2012 – Data Protection Manager (DPM), you must remove library sharing before you upgrade to System Center 2012 SP1 DPM.

- The *library server* is a computer on which DPM is installed, the library-sharing command has been run, and the medium changer is enabled.
- A *library client* is a computer on which DPM is installed, the library-sharing command has been run, and the medium changer is not enabled.

To remove library sharing

1. On each library client computer, open an elevated command prompt, and then run the following commands:

   cd <system drive> :\Program Files\Microsoft DPM\DPM\Setup

   SetSharedDPMDatabase.exe –RemoveDatabaseSharing

   AddLibraryServerForDPM.exe –DPMServerWithLibrary <*FQDN of the library server*> **-remove**

   where <*FQDN of library server*> is the fully qualified domain name of the library server.
2. Upgrade DPM on the library client computers.
3. Repeat steps 1 and 2 for all library client computers.
4. After you have removed library sharing and upgraded DPM on all library clients, on the library server, open an elevated command prompt, and then run the following commands one time for each library client:

   cd <system drive> :\Program Files\Microsoft DPM\DPM\Setup

   For each library client, run:

   AddLibraryServerForDpm.exe – ShareLibraryWithDpm <FQDN of library client> -remove

   where <*FQDN of library client*> is the fully qualified domain name of the library client.

   Then run the following command one time:

   SetSharedDPMDatabase.exe -RemoveDatabaseSharing
5. Upgrade DPM on the library server.
6. After you have upgraded DPM on the library server, reconfigure tape library sharing. For step-by-step instructions about how to configure library sharing, see Setting up Tape Library Sharing.

Upgrading a DPM server backing up DPM

This topic provides guidance for upgrading a secondary System Center 2012 – Data Protection Manager (DPM) server that is being used as a backup for a primary server.

Caution

When upgrading to System Center 2012 SP1 DPM, if you are protecting system state and you have customized the location of the backup that is staged, this customization will be lost in the **PSdataSourceConfig.xml** file during the upgrade. The staging location will be set to the drive with the largest available disk space.

To upgrade a DPM server that is being protected by another DPM server

1. Upgrade the secondary server. For step-by-step instructions for upgrading a DPM server, see Upgrading System Center - DPM.
2. On the primary server, close Administrator Console and Management Shell.
3. On the primary server, start the Setup Wizard, complete the upgrade, and then restart the computer.
4. Upgrade protection agents on all protected servers.
5. Run a consistency check on all protected data sources.

To upgrade a DPM server that is protecting another DPM server

1. Upgrade the secondary server. For step-by-step instructions for upgrading a DPM server, see Upgrading System Center - DPM.
2. On the secondary server, close Administrator Console and Management Shell.
3. On the secondary server, start the Setup Wizard, complete the upgrade, and then restart the computer.
4. Upgrade each primary server that is being protected, and then reinstall the protection agent of each.
5. Upgrade protection agents on all protected servers.
6. Run a consistency check on all protected data sources.

Post-upgrade steps

After upgrading to System Center 2012 SP1 DPM, note the following:

- You must upgrade all of the protection agents. This might require a restart of the protected computer.

- After upgrading the DPM server and the protection agents, all of your data sources will be marked as inconsistent. Upgrade the respective protection agents, and then perform a consistency check.
- Reconfigure tape library sharing.
- If you had Hyper-V Live Migration configured before doing the upgrade, you must run `Set-DpmGlobalProperty -KnownVmmServers <VmmServerName>` to continue protection.

To perform an agent upgrade by running the DPMAgentInstaller.exe

1. In the SCDPM folder of the setup DVD, open the **Agents** folder, and then copy **DPMAgentInstaller_x64.exe** and **DPMAgentInstaller_x86.exe** to a network share.
2. Log on to the protected computers, navigate to the network share, and then run the appropriate **DPMAgentInstaller.exe** command.

   ```
   DpmAgentInstaller.exe [/q] [<DPM server name>] [/IAcceptEula]
   ```

   Note
   Only agents that are running version System Center 2012 – Data Protection Manager (DPM) can be upgraded. For agents that are running any other version, you must uninstall the agent, and then install the DPM Beta agent.

To configure secondary protection

1. On the secondary DPM server, launch the DPM Agent Installation Wizard.
2. Select **Install Agents**.
3. Select the primary DPM servers that the secondary DPM protects.
4. Complete the protection agent installation.

Retrying a failed upgrade

This topic guides you through the process of retrying your System Center 2012 SP1 DPM upgrade if your previous attempt failed.

Before you retry the upgrade, check the logs at C:\Program Files\Microsoft System Center 2012\DPM\DPMLogs to see why the upgrade failed. After you have taken corrective action, follow the steps outlined here.

To retry the DPM upgrade

1. Back up the DPM database.
2. Uninstall the failed DPM upgrade while retaining your data by clicking **Retain disk-based recovery points** on the **Uninstallation Options** page. For step-by-step instructions for

uninstalling DPM, see Uninstalling DPM.

3. Delete the DPM database.
4. Reinstall System Center 2012 – Data Protection Manager (DPM) and all updates in the same sequence as they were installed to the return to the same state as the original installation.

   Tip

   Run the following query on the System Center 2012 – Data Protection Manager (DPM) database in Administrator mode to find the sequence in which the updates were originally applied.

   select * from tbl_DPM_InstalledUpdates
5. Restore the saved System Center 2012 – Data Protection Manager (DPM) database files.
6. Retry the upgrade.

To back up the DPM database

1. On the computer where the DPM database is installed, open Microsoft SQL Server Management Studio for SQL Server 2008 R2 and then connect to the instance of SQL Server that System Center 2012 – Data Protection Manager (DPM) was using.
2. Take a backup of the DPM database. To back up a database, right-click the database, click **Tasks**, and then click **Backup**.
3. Store this backup file to a safe location.

Rolling back an upgrade

If your upgrade to System Center 2012 – Data Protection Manager (DPM) does not complete successfully, or if you need to go back to DPM 2010, you can roll back the upgrade without losing the benefit of protection that you previously had.

To roll back a DPM upgrade

1. Backup your DPM database.
2. If DPM is installed, uninstall it while retaining your data by clicking **Retain disk-based recovery points** on the **Uninstallation Options** page. For step-by-step instructions for uninstalling DPM, see Uninstalling DPM.
3. Install System Center 2012 – Data Protection Manager (DPM). If you had any updates installed, reinstall them in the same sequence that you had installed them the first time.

   Tip

   Run the following query on the DPM 2010 database in Administrator mode to find

the sequence in which the updates were originally applied.

select * from tbl_DPM_InstalledUpdates

4. Before you began the upgrade, you should have backed up your DPM database and stored it in a safe location.

   To restore the DPM 2010 database to the SQL Server instance that DPM was using previously, open DPM Management Shell and run the command `dpmsync -restoredb`..
5. To synchronize the databases, in DPM Management Shell, run the command `dpmsync -sync`.
6. Open DPM Administrator Console and ensure that all agents are the same version as the DPM server.
7. Perform a consistency check on all the data sources.

Caution

If DPM was functional after installation, any recovery points created will be lost. Recovery points created prior to upgrading will still be available.

Upgrading to System Center 2012 - DPM

To upgrade to System Center 2012 – Data Protection Manager (DPM), DPM 2010 with QFE4 (KB2615782) must be installed on a 64-bit version of Windows Server 2008 R2 or Windows Server 2008. DPM does not support 32-bit or Itanium architecture–based operating systems.

Before you begin the upgrade, ensure that System Center Data Protection Manager 2010 has the latest hotfixes installed. For the latest updates and hotfixes for DPM, see Downloads for System Center Data Protection Manager.

Important

Before you upgrade DPM 2010, we strongly recommend that you back up your DPM database and store the backup file in a secure location. If your upgrade does not complete successfully, or if you need to go back to DPM 2010, you can roll back the upgrade.

Procedure to upgrade from DPM 2010

1. If you want to use a remote SQL instance, run Setup.exe on the SQL Server and select DPM Remote SQL Prep tool from the Setup page. For more information on upgrading DPMDB, see Upgrading the DPM Database.
2. Run Setup.exe on the DPM server and select Data Protection Manager from the Setup page and follow the wizard.

Important

- Setup adds firewall exceptions for port 6075 to enable a scoped DPM Administrator console.
- Setup adds the DPMSCOM group to Windows groups.
- Setup adds the MSDPM Trusted Users group to Windows groups.
- Setup adds the following new event logs: DPM Backup event and DPM alert.

See Also

Upgrading System Center - DPM

Upgrading the DPM Database

An important part of upgrading to System Center 2012 – Data Protection Manager (DPM) is upgrading the DPM database (DPMDB). With the multi-database feature, DPM allows you to consolidate the databases of all your DPM servers to one SQL Server instance. When upgrading, you have to choose one of three scenarios.

- Local SQL Server instance to Local SQL Server instance

  Use this option if you want to continue to have DPMDB on the same computer as DPM.
- Local SQL Server instance to remote SQL Server instance

  Use this option when you want to move from using a local instance of DPMDB to a remote instance. Using this feature, one instance of SQL Server can host the databases of multiple DPM servers.
- Remote SQL Server instance to Remote SQL Server instance

  Use this option when you want to continue to use a remote instance of SQL Server to host the DPMDB. Using this feature, one instance of SQL Server can host the databases of multiple DPM servers.

Important

- Upgrade your DPM servers sequentially. Parallel upgrades may lead to errors.
- If you are using an existing instance of SQL Server, you must run DPM Remote SQL Prep tool from the Setup splash screen on the instance of SQL Server you are going to use.
- You cannot share an instance of SQL Server installed by DPM. We recommend you use it only for DPM databases.
- TCP/IP protocol must be enabled on SQL Server and TCP/IP client protocol on DPM server.
- When setting up tape library sharing, provide the complete name as <servername>\<instancename>\<databasename>.
- The naming conventions for the DPM database have changed with this new feature, and you can find the name of the database from the Information button on the Administrator console.

Local SQL Server instance to Local SQL Server instance

1. Backup DPMDB.

2. Add MicrosoftDPMACCT to the ACL for the DPMDB folder, if it doesn't exist. Add full control to the user.
3. Launch System Center 2012 – Data Protection Manager (DPM) installation. This will start setup in upgrade mode.

Local SQL Server instance to remote SQL Server instance

1. Ensure that the domain user account you will use to install DPM is a member of all the following:
   - The local Administrators group on the DPM server.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

   Note
   After setup is complete, you can remove the user account from the local Administrators group on the computer running the remote instance of SQL Server.
2. Backup DPMDB.
3. Add MicrosoftDPMACCT to the ACL for the DPMDB folder, if it doesn't exist. Add full control to the user.
4. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 which you plan to use to host databases of multiple DPM servers.

   Note
   The name of the restored database should be DPMDB.

   This instance of SQL Server should be used only for hosting DPM databases only.
5. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
6. Install SQL Prep Tool on the remote computer running SQL Server. You can find this on the Setup page.
7. Launch DPM installation. This will start setup in upgrade mode.

Remote SQL Server instance to Remote SQL Server instance

1. Ensure that the domain user account you will use to install DPM is a member of all the following:
   - The local Administrators group on the DPM server.
   - The local Administrators group on the computer on which you have installed the remote instance of SQL Server 2008 R2.
   - The SQL Server Sysadmin fixed server role on the computer on which you have installed the remote instance of SQL Server 2008 R2.

   Note
   After setup is complete, you can remove the user account from the local

Administrators group on the computer running the remote instance of SQL Server.

2. Backup DPMDB.
3. Restore the DPMDB backup to a remote instance of SQL Server 2008 R2 that you plan to use to host databases of multiple DPM servers.

   Note
   - The name of the restored database should be the same as the DPM database you backed up.
   - This instance of SQL Server should be used only for hosting DPM databases only.
4. Ensure that TCP/IP protocol is enabled for this instance of SQL Server.
5. Install SQL Prep Tool on the remote instance of SQL Server.
6. Launch DPM installation. This will start setup in upgrade mode.

See Also

Installing DPM Using a Remote Instance of SQL Server 2008

Removing library sharing

If you are sharing a tape library across multiple servers running System Center Data Protection Manager (DPM) 2010, you must remove library sharing before you upgrade to System Center 2012 – Data Protection Manager (DPM).

- The *library server* is a computer on which DPM is installed, the library-sharing command has been run, and the medium changer is enabled.
- A *library client* is a computer on which DPM is installed, the library-sharing command has been run, and the medium changer is not enabled.

To remove library sharing

1. On each library client computer, open an elevated command prompt, and then run the following commands:

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

   SetSharedDPMDatabase.exe -RemoveDatabaseSharing

   AddLibraryServerForDPM.exe –DPMServerWithLibrary <*FQDN of the library server*> **-remove**

   where <*FQDN of library server*> is the fully qualified domain name of the library server.

2. Upgrade DPM on the library client computers.
3. Repeat steps 1 and 2 for all library client computers.
4. After you have removed library sharing and upgraded DPM on all library clients, on the library server, open an elevated command prompt, and then run the following commands one time for each library client:

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

   For each library client, run:
   AddLibraryServerForDpm.exe – ShareLibraryWithDpm <FQDN of library client> -remove

   where <*FQDN of library client*> is the fully qualified domain name of the library client.

   Then run the following command one time:

   SetSharedDPMDatabase.exe -RemoveDatabaseSharing
5. Upgrade DPM on the library server.
6. After you have upgraded DPM on the library server, reconfigure tape library sharing. For step-by-step instructions about how to configure library sharing, see Setting up Tape Library Sharing.

Upgrading the Disaster Recovery Configuration

This topic provides guidance for upgrading your disaster recovery configuration to System Center 2012 – Data Protection Manager (DPM).

Caution
When upgrading to System Center 2012 – Data Protection Manager (DPM), if you are protecting system state and you have customized the location of the backup that is staged, this customization will be lost in the **PSdataSourceConfig.xml** file during the upgrade. The staging location will be set to the drive with the largest available disk space.

Upgrading a DPM server that is being protected by or is protecting another DPM server

To upgrade a DPM that is being protected by another DPM server

1. Upgrade the secondary server. For step-by-step instructions for upgrading a DPM server, see Upgrading System Center - DPM.

2. On the primary server, close Administrator Console and Management Shell.
3. On the primary server, start the Setup Wizard, complete the upgrade, and then restart the computer.
4. Upgrade protection agents on all protected servers.
5. Run a consistency check on all protected data sources.

To upgrade a DPM server that is protecting another DPM server

1. Upgrade the secondary server. For step-by-step instructions for upgrading a DPM server, see Upgrading System Center - DPM.
2. On the secondary server, close Administrator Console and Management Shell.
3. On the secondary server, start the Setup Wizard, complete the upgrade, and then restart the computer.
4. Upgrade each primary server that is being protected, and then reinstall the protection agent of each.
5. Upgrade protection agents on all protected servers.
6. Run a consistency check on all protected data sources.

Post-upgrade steps

After upgrading to System Center 2012 – Data Protection Manager (DPM), note the following:

- You must upgrade all of the protection agents. This operation does not require a restart of the protected computer.
- After upgrading the DPM server and the protection agents, all of your data sources will be marked as inconsistent. Upgrade the respective protection agents, and then perform a consistency check.
- Reconfigure tape library sharing.

To perform an agent upgrade by running the DPMAgentInstaller.exe

1. In the SCDPM folder of the setup DVD, open the **Agents** folder, and then copy **DPMAgentInstaller_x64.exe** and **DPMAgentInstaller_x86.exe** to a network share.
2. Log on to the protected computers, navigate to the network share, and then run the appropriate **DPMAgentInstaller.exe** command.

   Note
   Only agents that are running version DPM 2010 can be upgraded to System Center 2012 – Data Protection Manager (DPM). For agents that are running any other version, you must uninstall the agent, and then install the System Center 2012 – Data Protection Manager (DPM) agent.

To configure secondary protection

1. On the secondary DPM server, launch the DPM Agent Installation Wizard.
2. Select **Install Agents**.
3. Select the primary DPM servers that the secondary DPM protects.
4. Complete the protection agent installation.

See Also

Updating Protection Agents

How to Set Up Tape Library Sharing

Retrying a failed DPM upgrade

This topic guides you through the process of retrying your System Center 2012 – Data Protection Manager (DPM) upgrade if your previous attempt failed.

Before you retry the upgrade, check the logs at C:\Program Files\Microsoft System Center 2012\DPM\DPMLogs to see why the upgrade failed. After you have taken corrective action, follow the steps outlined here.

To retry the DPM 2012 upgrade

1. Uninstall the failed DPM upgrade while retaining your data by clicking **Retain disk-based recovery points** on the **Uninstallation Options** page. For step-by-step instructions for uninstalling DPM, see Uninstalling DPM.
2. Back up the DPM 2010 database. For more information, see To back up the DPM 2010 database.
3. Delete the DPM database.
4. Reinstall DPM 2010 and all updates in the same sequence as they were installed to the return to the same state as the original installation.

   Tip

   Run the following query on the DPM 2010 database in Administrator mode to find the sequence in which the updates were originally applied.

   select * from tbl_DPM_InstalledUpdates
5. Restore the saved DPM 2010 database files.
6. Retry the upgrade.

To back up the DPM 2010 database

1. On the computer where the DPM database is installed, open Microsoft SQL Server Management Studio for SQL Server 2008 and then connect to the instance of SQL Server that DPM 2010 was using.
2. Take a backup of the DPMDB database. To back up a database, right-click the database, click **Tasks**, and then click **Backup**.
3. Store this backup file to a safe location.
4. Delete the DPMDB database by using SQL Server Management Studio.

See Also

Upgrading System Center - DPM

Upgrading to System Center 2012 - DPM

Rolling back a DPM upgrade

Rolling back a DPM upgrade

If your upgrade to System Center 2012 – Data Protection Manager (DPM) does not complete successfully, or if you need to go back to DPM 2010, you can roll back the upgrade without losing the benefit of protection that you previously had.

To roll back a DPM 2010 upgrade

1. If DPM is installed, uninstall it while retaining your data by clicking **Retain disk-based recovery points** on the **Uninstallation Options** page. For step-by-step instructions for uninstalling DPM, see Uninstalling DPM.
2. Install DPM 2010. If you had any updates installed, reinstall them in the same sequence that you had installed them the first time.

   Tip
   Run the following query on the DPM 2010 database in Administrator mode to find the sequence in which the updates were originally applied.

   select * from tbl_DPM_InstalledUpdates
3. Before you began the upgrade, you should have backed up your DPM 2010 database and stored it in a safe location according to the upgrade instructions provided at Upgrading from DPM 2010.

   To restore the DPM 2010 database to the SQL Server instance that DPM was using previously, open DPM Management Shell and run the command `dpmsync -restoredb`..
4. To synchronize the databases, in DPM Management Shell, run the command `dpmsync -sync`.
5. Open DPM Administrator Console and ensure that all agents are the same version as the DPM server.

6. Perform a consistency check on all the data sources.

Caution
If DPM was functional after installation, any recovery points created will be lost. Recovery points created prior to upgrading will still be available.

Repairing DPM

In the unlikely event of corruption of the Microsoft Windows registry, system files, or the System Center 2012 – Data Protection Manager (DPM) binaries, you can repair DPM by reinstalling it. Repairing DPM involves uninstalling DPM while retaining your data protection configuration, and then reinstalling DPM.

This topic provides step-by-step instructions for repairing DPM, including the following information:

- What you need to do before you reinstall DPM.
- What you need to do if you do not plan to reinstall DPM immediately.
- What happens to protection jobs during the repair process.
- What procedures you need to use to successfully repair DPM.
- What you need to do after the uninstallation of DPM is complete and before you reinstall DPM.

Important
Before starting a reinstallation of DPM, we strongly recommend that you back up the DPM database, the Report database, and replicas to tape or other removable storage medium. For more information, see Disaster Recovery.

In most cases, you do not need to uninstall the DPM prerequisite software before you reinstall DPM. However, if the SQL Server 2008 SP1 binaries become corrupted, you might have to uninstall and reinstall SQL Server 2008 SP1 also.

You do not have to uninstall the protection agents from the protected computers to reinstall DPM.

Protection jobs cannot run successfully during a repair operation. Any jobs scheduled to run while a repair operation is in progress will be unsuccessful. Any jobs that are in progress when the uninstallation part of a repair operation starts are canceled. Upon completing the repair operation, DPM automatically attempts to perform any canceled replica creation, synchronization, or consistency-check jobs, but it does not attempt to perform canceled recovery point creation jobs.

Important
If you do not plan to reinstall DPM immediately, before uninstalling DPM, you should do the following:

1. Disable end-user recovery on the DPM server. For more information, see How to Disable End-User Recovery in DPM Help.

2. Run synchronization for each volume in your protection groups. For more information, see How to Synchronize a Replica in DPM Help.

   Following these steps helps to ensure that users for whom you have denied access to files on protected computers cannot access replicas of those files on the DPM server.

To successfully repair DPMM, you must perform the following procedures in sequence:

1. Back up the DPM database.
2. Uninstall DPM.
3. Delete the DPM database.
4. Reinstall DPM.
5. Restore the DPM database.
6. Run `DPMSync -sync`.

To back up the DPM database

1. On the computer where your DPM database is located, do one of the following:
   - **If the DPM database is on the DPM server**

     On the DPM server, open an elevated command prompt window, go to cd <system drive>:\Program Files\Microsoft DPM\DPM\bin, and run **DPMBackup.exe -db**.
   - **If the DPM database is on a remote computer**

     On the computer where the DPM database is installed, open an elevated command prompt window, go to cd <system drive>:\Program Files\Microsoft Data Protection Manager\DPM\SQLPrep, and run **DPMBackup.exe -db**.
2. On the computer where your DPM database is located, do one of the following:
   - **If the DPM database is on the DPM server**

     Go to <system drive>:\Program Files\Microsoft DPM\DPM\Volumes\ShadowCopy\Database Backups. The file name of the DPM database backup is **DPMDB.bak**.
   - **If the DPM database is on a remote computer**

     Go to <system drive>:\DPMBackup\dpmserver. The file name of the DPM database backup is DPMDB.bak.
3. Copy the database backup file to a secure location that you can access when you are ready to restore your DPM database.

To uninstall DPM

1. In Control Panel, click **Programs**, and then click **Programs and Features**.
2. In the **Uninstall or change a program** list, right-click **System Center 2012 – Data Protection Manager (DPM)**, and then click **Uninstall/Change**.

   The Setup Wizard opens.
3. On the **Uninstallation Options** page, select the **Retain data** option, and then click **Next**.
4. On the **Summary of Options** page, click **Uninstall**.

5. When uninstallation is complete, click **Close**.

To delete the DPM database

1. On the computer where your DPM database is located, click **Start**, point to **All Programs**, click **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Server name** box, type **<computer name>\<instance name>**, and then click **Connect**.

   Note
   The default instance name for a local DPM database installation on the DPM server is **MSDPM2012**.
3. Expand **Databases**, right-click the **DPMDB** database, and then click **Delete**.
4. Click **Yes** to confirm the deletion.

To install DPM

- For information about how to install DPM, see Installing DPM.

To restore the DPM database using the DpmSync tool

1. On the computer where your DPM database will be restored, open an elevated command prompt window, go to cd <system drive>:\Program Files\Microsoft DPM\DPM\bin, and run **DpmSync –restoredb –dbloc <DPMDB file location>**.

   DpmSync restores the DPM database and the DPM Report database, and synchronizes the restored DPM database with the previous state of the DPM system. In the command, <*DPMDB file location*> is the location where you stored the DPM database backup file (DPMDB.bak). For more information about using DpmSync, run **DpmSync /?**.

   Note
   The default location of DPMDB is C:\Program Files\Microsoft DPM\DPM\DPMDB. When you use a remote instance of SQL Server for DPM, the default location of the DPM database is the path where the SQL database files for the instance are located.
2. From the command prompt, run **DpmSync -sync**.
3. After the new installation is complete and the database is restored, in DPM Administrator Console, in the **Monitoring** workspace, check for protection jobs that failed during the repair operation. Manually restart any failed jobs.
4. After you restart the failed jobs, you must perform a consistency check for all data sources. For more information about how to perform a manual consistency check, see How to Synchronize a Replica in DPM Help.

See Also

Installing and Upgrading System Center 2012 - DPM

Installing DPM

Uninstalling DPM

This article provides step-by-step instructions for uninstalling System Center 2012 – Data Protection Manager (DPM). When you uninstall DPM, you can choose whether to remove or retain your data protection configuration, which contains your recovery points, replicas, and protection schedule. If you plan to reinstall DPM and resume the protection schedule or access current recovery points, you must choose to retain your data protection configuration when you uninstall DPM.

Important

If you do not plan to reinstall DPM immediately, before you uninstall DPM, you should disable end-user recovery on the DPM server and run synchronization jobs for each data source in your protection. Following these steps helps to ensure that end users for whom you have denied access to files on protected computers cannot access the replicas of those files on the DPM server.

Uninstall DPM

When you uninstall DPM, Setup uninstalls only the DPM application. Setup does not remove the prerequisite software, protection agents, user settings, or DPM reports deployed by using SQL Server Reporting Services. If you are not reinstalling DPM, the reports will be removed when you uninstall SQL Server.

Caution

If you plan to reinstall DPM, uninstall only the DPM application. Do not uninstall protection agents, prerequisites, or SQL Server. If you uninstall SQL Server, you will lose your DPM reports.

To permanently uninstall DPM, the prerequisite software, DPM reports, and protection agents, complete all steps in the following order:

Step 1: Uninstalling the DPM application

If you want to permanently uninstall DPM, use DPM Administrator Console to uninstall protection agents deployed on protected servers before you uninstall DPM. Alternatively, you can use **Add or Remove Programs** to uninstall protection agents from the protected computers locally after you uninstall DPM.

To uninstall the DPM application

1. In Control Panel, click **Programs**, and then click **Programs and Features**.
2. In the **Uninstall or change a program** list, right-click **System Center 2012 – Data Protection Manager (DPM)**, and then click **Uninstall/Change**.

   The Setup Wizard opens.
3. On the **Uninstallation Options** page, click either **Retain disk-based recovery points** or **Remove data**, and then click **Next**.
4. On the **Summary of Options** page, click **Uninstall**.
5. When DPM has been uninstalled, click **Close**.

Step 2: Uninstalling DPM prerequisites

Following are the prerequisites that you might want to uninstall, unless you are using them with other programs.

Caution

Uninstalling SQL Server 2008 also uninstalls SQL Server Reporting Services. If you plan to reinstall DPM and have DPM reports, do not uninstall SQL Server 2008.

SQL Server 2008

To uninstall SQL Server 2008

1. In Control Panel, click **Programs**, and then click **Programs and Features**.
2. In the **Uninstall or change a program** list, right-click **Microsoft SQL Server 2008 (64-bit)**, click **Uninstall/Change**, and then click **Remove**.
3. Follow the steps in the wizard to remove SQL Server 2008.

   Note

   In addition to installing software required for DPM, SQL Server Setup installs the following software, which is not a requirement for DPM:

   - Microsoft SQL Server Compact 3.5 SP1
   - Microsoft SQL Server Compact 3.5 SP1 Query Tools
   - Microsoft SQL Server 2008 Native Client
   - Microsoft Visual Studio Tools for Applications 2.0
   - Microsoft Office 2003 Web Components

   This software is not removed when you uninstall DPM or when you uninstall the last instance of SQL Server. You must uninstall this software manually.

Windows PowerShell 2.0

The following procedure applies to only Windows Server 2008.

To uninstall Windows PowerShell 2.0

1. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, expand **Features**, and then click **Remove Features**.
3. On the **Select Feature** page of the Remove Features Wizard, in the **Features** pane, click **Remove Features**.
4. Clear the **Windows PowerShell** check box and complete the uninstallation process.

Single Instance Storage (SIS)

To uninstall Windows Single Instance Storage (SIS)

1. In an elevated command prompt window, run **start /w ocsetup.exe SIS-Limited /uninstall /quiet /norestart**.
2. After SIS is uninstalled, you must restart the computer.

See Also

Installing DPM

DPM Server Software Prerequisites

Deploying DPM

After you install System Center 2012 – Data Protection Manager (DPM), you must perform a series of required configuration tasks before you can start protecting your data. You can also configure optional DPM features at this time, or you can wait and configure optional features at any time after you deploy DPM. The topics in this section provide instructions for opening DPM for the first time, and then performing each of the required and optional configuration tasks.

In This Section

Deployment checklist

Opening the DPM Administrator Console

Opening the DPM Administrator Console

Required Configuration Tasks

Optional Configuration Tasks

Opening the DPM Administrator Console

Use the procedure in this topic to open DPM Administrator Console so that you can configure and manage System Center 2012 – Data Protection Manager (DPM).

For an introduction to DPM Administrator Console, see Administrator Console for DPM.

To open DPM Administrator Console

1. Log on to the DPM server using a domain user account that is a member of the local Administrators group.
2. On the **Start** menu, point to **All Programs**, point to **System Center 2012**, and then click **System Center 2012 – Data Protection Manager (DPM)**.

   –Or–

   If it is available, double-click the **System Center 2012 – Data Protection Manager (DPM)** icon on the desktop.

Deployment checklist

This checklist includes the planning tasks necessary to prepare to deploy System Center 2012 – Data Protection Manager (DPM).

Task	Reference
Identify each data source to be protected, including the following information: • Data source type (file server, Microsoft Exchange, Microsoft SQL Server, Microsoft Windows SharePoint Services, Microsoft Virtual Server, system state) • Data source size • Any folders or file name extensions to be excluded from protection • Fully qualified domain name (FQDN) of computer • Cluster name (if applicable)	Plan for file data protection on computers and servers
Identify one of the following methods for each protection group: • Short-term disk-based protection • Short-term tape-based protection	Selecting a Data Protection Method

Task	Reference
• Long-term tape-based protection • Short-term disk-based protection and long-term tape-based protection • Short-term tape-based protection and long-term tape-based protection	
For each data source, determine the recovery goals for each data protection method that you will use. For short-term disk-based protection, identify the following information: • Retention range • Synchronization frequency • Number of recovery points For short-term tape-based protection, identify the following information: • Retention range • Backup schedule • Type of backup • Number of backup copies • Tape labeling scheme For long-term tape-based protection, identify the following information: • Retention range • Backup schedule and scheduling options • Number of backup copies • Tape labeling scheme	Plan recovery goals Defining Recovery Goals
Organize the data sources into protection groups.	Selecting Protection Group Members
Determine your storage needs, based on your information about the protected data sources and recovery goals.	Allocating Space for Protection Groups
If you are using tape-based protection, decide if you want to compress or encrypt the data on tapes.	Specifying Tape and Library Details
Decide which method of replica creation you will use for each protection group.	Choosing a Replica Creation Method

Task	Reference
Identify the DPM server configurations necessary, including the following information: • The number of DPM servers • Where to locate each DPM server • Which instance of SQL Server each DPM server will use	Plan for DPM server deployment
Determine the disk configurations each DPM server will require to meet the storage needs of the protection groups. Include any custom volumes that specific data sources will use.	Plan for DPM storage
Identify the DPM servers that require tape libraries and the capacity of each library.	Planning the Tape Libraries Configuration
Identify the DPM servers for which end-user recovery will be enabled and which clients will require installation of the recovery point client software.	Plan for end-user recovery

See Also

Planning for DPM Deployment

Plan for workload protection

Required Configuration Tasks

Before you can start protecting data by using System Center 2012 – Data Protection Manager (DPM), you must verify that each computer that DPM will protect meets the protected computer software requirements. For information about the protected computer software requirements, see **Protected Computer Software Requirements**.

You must also perform the following list of tasks if applicable to your protection configuration.

- Add one or more disks to the storage pool.

  Note
  Adding a disk to the storage pool is not a requirement if you are going to use custom volumes to protect your data sources, or if you are only going to use disk-to-tape protection.
- If you are protecting data on tape, configure tape libraries and stand-alone tape drives.
- Install and configure a protection agent on each computer that you want to protect.

- If you are protecting server farms for servers running Windows SharePoint Services 3.0 or Microsoft Office SharePoint 2007 Server, start and configure the Windows SharePoint Services VSS Writer service (WSS Writer service), and provide farm administration credentials for the protection agent.
- Create one or more protection groups.

In This Section

Adding Disks to the Storage Pool

The *storage pool* is a set of disks on which the System Center 2012 – Data Protection Manager (DPM) server stores replicas and recovery points for protected data. Before you can start protecting data, you must add at least one disk to the storage pool. After configuration, you can add more disks to the storage pool.

Note
DPM does not support USB/1394 disks.

Adding a disk to the storage pool is not a requirement if you are going to use custom volumes to protect your data sources, or if you are only going to use disk-to-tape protection.

For more information and guidelines for choosing disk types and calculating capacity requirements for your storage pool, see Planning the Storage Pool.

To help you estimate your storage space needs, download the Storage Calculators for System Center Data Protection Manager.

DPM requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files
- DPM prerequisite software
- DPM database files

You can install DPM on the same volume that the operating system is installed on or on a different volume that does not include the operating system. However, a disk on which you install DPM cannot be added to the storage pool.

Note

When you add a disk to the storage pool, DPM uses the available free space on the disk and does not delete any data that is already on the disk. If there are existing volumes on the disk that have free space, DPM cannot use that space for the storage pool. DPM can use only space in the volumes that it creates. If you want to make the entire disk space available to the storage pool, you must delete any existing volumes on the disk before adding it to the storage pool.

To add disks to the storage pool

1. In DPM Administrator Console, click **Management**, and then click the **Disks**.
2. Click **Add** on the tool ribbon.

   The **Add Disks to Storage Pool** dialog box appears. The **Available disks** section lists the disks that you can add to the storage pool.
3. Select one or more disks, click **Add**, and then click **OK**.

Configuring Tape Libraries

You can add tape libraries and stand-alone tape drives to System Center 2012 – Data Protection Manager (DPM) to enable short-term and long-term data protection on tape. The tape libraries and stand-alone tape drives must be physically attached to the DPM server.

Before DPM can recognize the tape library, you must add the following firewall exceptions:

- C:\Program Files\Microsoft System Center 2012\DPM\SQL\MSSQL10_50.MSDPMV4RC\MSSQL\Binn\sqlservr.exe
- C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe
- C:\Program Files\Microsoft System Center 2012\DPM\DPM\bin\DPMLA.exe

Important

If you are sharing the tape library across multiple DPM servers, add the exceptions on all of them.

After you attach a new tape library or stand-alone tape drive to your DPM server, you must perform a **Rescan** operation before the DPM server can identify them. When you perform a **Rescan** operation, DPM examines the tape libraries or stand-alone tape drives that are attached to the DPM server and updates the information that is displayed on the **Libraries** area of the **Management** workspace in DPM Administrator Console. The **Libraries** area displays each stand-alone tape drive, and each tape library and its drives.

You use the **Rescan** operation on the **Libraries** area to check for and refresh the state of all new tape libraries and stand-alone tape drives when you make changes to your hardware.

Note

If the stand-alone tape drives listed on the **Libraries** area in DPM Administrator Console do not match the physical state of your stand-alone tape drives, see Managing Tapes in DPM Help. For example, if drives from a tape library are listed as stand-alone tape drives, or if a stand-alone tape drive displays incorrectly as a drive in a tape library, you need to remap the tape drive information.

To configure tape libraries

1. In DPM Administrator Console, click **Management**, and then click **Libraries**.
2. Click **Rescan** on the tool ribbon.

   The **Rescan** operation might take several minutes to complete. DPM will add any library jobs to the queue that began during the **Rescan** operation. If a library job is already in progress when the **Rescan** operation begins, the **Rescan** operation will fail.

See Also

How to Set Up Tape Library Sharing

How to Enable and Disable a Library

Installing and Configuring Protection Agents

A *protection agent* is software that you install on a computer you want to protect with System Center 2012 – Data Protection Manager (DPM). The protection agent identifies data on a computer that DPM can protect and recover, and tracks changes to protected data and transfers the changes from the protected computer to the DPM server.

Before you can start protecting data, you must install a protection agent on each computer that contains data that you want to protect. After the protection agent is installed on a computer, the computer is listed as an unprotected computer in the **Management** task area of DPM Administrator Console. The data sources on the computer are not protected until you add them to a protection group. Each computer that you want to protect must meet the protected computer prerequisites. For more information, see **Protected Computer Software Requirements**.

If Windows Firewall or another firewall is enabled on the DPM server, you must configure the firewall to open port 135 to TCP traffic, and enable the DPM service (Msdpm.exe) and the protection agent (Dpmra.exe) to communicate through the firewall. For more information about configuring the firewall on the DPM server, see Configuring Windows Firewall on the DPM Server. For more information about how to update protection agents on computers that reside behind a firewall, see Updating Protection Agents.

In This Section

Configuring Windows Firewall on the DPM Server

Installing Protection Agents
Attaching Protection Agents
Updating Protection Agents

Configuring Windows Firewall on the DPM Server

For a protection agent to communicate with the System Center 2012 – Data Protection Manager (DPM) server through a firewall, you must configure exceptions for the firewall. The following procedure applies to configuring Windows Firewall. If Windows Firewall is enabled on the DPM server when you install DPM, Setup configures the firewall automatically. For more information about configuring other software or hardware firewalls, consult the vendor documentation.

To configure Windows Firewall on a DPM server

1. In Server Manager, expand **Configuration** and then expand **Windows Firewall with Advanced Security**.
2. In the **Overview** area, verify that Windows Firewall is on for all profiles, and then click **Inbound Rules**.
3. To create a new exception, do the following:
   a. In the **Actions** pane, click **New Rule** to open the New Inbound Rule Wizard.
   b. On the **Rule Type** page, verify that **Program** is selected, and then click **Next**.
   c. On the **Program** page, click **Browse** for the **This program path** box, navigate to **<system drive letter>:\Program Files\Microsoft DPM\DPM\bin**, click **Msdpm.exe**, click **Open**, and then click **Next**.
   d. On the **Action** page, leave the default setting of **Allow the connection**, or modify the settings according to your organization's guidelines, and then click **Next**.
   e. On the **Profile** page, leave the default settings of **Domain**, **Private**, and **Public**, or modify the settings according to your organization's guidelines, and then click **Next**.
   f. On the **Name** page, type a name for the rule and optionally a description, and then click **Finish**.

      Note
      The DPM default name for this exception is **System Center 2012 – Data Protection Manager (DPM)**.
4. To create a new exception, do the following:
   a. In the **Actions** pane, click **New Rule** to open the New Inbound Rule Wizard.
   b. On the **Rule Type** page, verify that **Program** is selected, and then click **Next**.
   c. On the **Program** page, click **Browse** for the **This program path** box, navigate to **<system drive letter>:\Program Files\Microsoft DPM\DPM\bin**, click **Dpmra.exe**, click **Open**, and then click **Next**.

d. On the **Action** page, leave the default setting of **Allow the connection**, or modify the settings according to your organization's guidelines, and then click **Next**.

e. On the **Profile** page, leave the default settings of **Domain**, **Private**, and **Public**, or modify the settings according to your organization's guidelines, and then click **Next**.

f. On the **Name** page, type a name for the rule and optionally a description, and then click **Finish**.

Note
The DPM default name for this exception is **System Center 2012 – Data Protection Manager (DPM) Replication Agent**.

5. To create a new exception, do the following:

a. In the **Actions** pane, click **New Rule** to open the New Inbound Rule Wizard.

b. On the **Rule Type** page, click **Port**, and then click **Next**.

c. On the **Protocols and Ports** page, verify that **TCP** and **Specific local ports** options are selected, in the **Specific local ports** box, type **135**, and then click **Next**.

d. On the **Action** page, leave the default setting of **Allow the connection**, or modify the settings according to your organization's guidelines, and then click **Next**.

e. On the **Profile** page, leave the default settings of **Domain**, **Private**, and **Public**, or modify the settings according to your organization's guidelines, and then click **Next**.

f. On the **Name** page, type a name for the rule and optionally a description, and then click **Finish**.

Note
The DPM default name for this exception is **DPMRA_DCOM_135**.

Installing Protection Agents

You can use the Protection Agent Installation Wizard to install protection agents that are located outside of a firewall, and you can manually install protection agents on computers that are located behind a firewall, or that are located in a workgroup or a domain that does not have a two-way trust relationship with the domain that the System Center 2012 – Data Protection Manager (DPM) server is located in. After you install a protection agent manually, you then need to attach the agent in DPM Administrator Console to enable protection. To install protection agents on computers that are located behind a firewall, see Installing Protection Agents on Computers Behind a Firewall. To install protection agents on computers that are in a workgroup or a domain that does not have a two-way trust relationship with the domain that the DPM server is located in, see Installing Protection Agents on Computers in a Workgroup or Untrusted Domain.

If you are installing a protection agent and encounter network-related or permissions-related issues because of domain policies, we recommend that you install the protection agent manually.

For information about manually installing a protection agent, see Installing Protection Agents Manually.

For information about installing a protection agent by using a server image on the computer without specifying the DPM server, see Installing Protection Agents Using a Server Image.

In This Section

Installing Protection Agents on Computers Outside of a Firewall

Before you install protection agents on the computers that you want to protect, note the following:

- If a firewall is enabled on a protected computer, you must install the protection agent manually. For information about installing protection agents on a computer that is behind a firewall, see Installing Protection Agents on Computers Behind a Firewall.
- If the firewall is not enabled on a protected computer, or if there are exceptions in Windows Firewall that allow the protection agent to communicate with the DPM server, use the following procedure to install a protection agent. For more information about configuring Windows Firewall for DPM, see Configuring Windows Firewall on the DPM Server.

To install a protection agent on a computer outside of a firewall

1. In DPM Administrator Console, click **Management**, and then click **Agents**.
2. Click **Install** on the tool ribbon.

   The Protection Agent Installation Wizard opens.
3. On the **Select Agent Deployment Method** page, click **Install agents**, and then click **Next**.
4. On the **Select Computers** page, DPM displays a list of available computers that are in the same domain as the DPM server. If this is the first time you have used the wizard, DPM queries Active Directory to get a list of available computers. After the first installation, DPM stores the list of computers in its database, which is updated once each day by the auto-discovery process.

   If you know the name of a specific computer on which you want to install a protection agent, you can quickly locate the computer by typing all or part of its name in the

Computer name box, and then clicking **Add**.

To find a computer in another domain that has a two-way trust relationship with the domain that the DPM server is located in, you must type the fully qualified domain name of the computer that you want to protect (for example, <*Computer1*>**.Domain1.contoso.com**, where *Computer1* is the name of the computer that you want to protect, and *Domain1.contosa.com* is the domain to which the target computer belongs.

In the **Computer name** list, select one or more computers (up to a maximum of 50), click **Add**, and then click **Next**.

Note

The **Advanced** button on the **Select Computers** page is enabled only when there is more than one version of a protection agent available for installation on the computers. If it is enabled, you can use this option to install a previous version of the protection agent that was installed before you upgraded DPM server to a more recent version.

5. On the **Enter Credentials** page, type the user name and password for a domain account that is a member of the local Administrators group on all selected computers.
6. In the **Domain** box, accept or type the domain name of the user account that you are using to install the protection agent on the target computer. This account may belong to the domain that the DPM server is located in or to a domain that has a two-way trust relationship with the domain that the DPM server is located in.

   If you are installing a protection agent on a computer across a trusted domain, enter your current domain user credentials. You can be a member of any domain that has a two-way trust relationship with the domain that the DPM server and you must be member of the local Administrators group on all selected computers on which you want to install an agent.

   If you select a node in a cluster, DPM detects all additional nodes in the cluster and displays the **Select Cluster Nodes** page.
7. On the **Select Cluster Nodes** page, in the **Cluster node selection** section, select an option that you want DPM to use for installing agents on additional nodes in the cluster, and then click **Next**.
8. On the **Choose Restart Method** page, select the method to use to restart the selected computers after the protection agent is installed. The computer must be restarted before you can start protecting data. A restart is necessary to load the volume filter that DPM uses to track and transfer block-level changes between DPM server and the protected computers.

   If you select **No. I will restart the selected computers later**, after the computers restart, the protection agent installation status is not automatically refreshed on the **Agents** tab in the **Management** task area. To refresh the protection agent installation status, click one or more computers in the details pane, and then click **Refresh Information**.

Note

You do not need to restart the computer if you are installing a protection agent on another DPM server.

If any of the computers that you selected are nodes in a cluster, an additional **Choose Restart Method** page appears that you can use to select the method to restart the clustered computers.

You must install a protection agent on all nodes in a cluster to successfully protect the clustered data. The computers must be restarted before you can start protecting data. Because of the time required to start services, it might take a few minutes after a restart before DPM can contact the agent on the cluster.

Note
DPM will not automatically restart a computer that belongs to a Microsoft Cluster Server (MSCS) cluster. You must manually restart computers in an MSCS cluster.

9. On the **Summary** page, click **Install** to begin the installation.
10. On the **Installation** page, the results appear on the **Task** tab to indicate whether the installation is successful. You can click **Close** before the wizard is finished performing the tasks, and then monitor the installation progress in DPM Administrator Console on the **Agents** tab in the **Management** task area.

If the installation is unsuccessful, you can view the alerts in the **Monitoring** task area on the **Alerts** tab.

Note

After you install a protection agent on a computer that is part of a Windows SharePoint Services farm, each of the computers in the farm will not appear as protected computers on the **Agents** tab in the **Management** task area, only the computer that you selected. However, if the Windows SharePoint Services farm has data on the selected computer, DPM protects the data on all of the computers in the farm, provided all of them have the protection agent installed.

Installing Protection Agents on Computers Behind a Firewall

If you are installing a protection agent on a computer in an Active Directory domain and that is behind a firewall, you must manually install the protection agent on the computer that you want to protect, and then use the procedure in this topic to attach the agent. For more information about manually installing an agent, see Installing Protection Agents Manually.

To install an agent on a computer behind a firewall

1. Run the following command on the protected computer before you begin the protection

agent installation to make sure that the agent can be pushed out through the firewall.

```
netsh advfirewall firewall add rule name="Allow DPM Remote Agent Push" dir=in
action=allow service=any enable=yes profile=any remoteip=<IPAddress>
```

Where IPAddress is the address of the DPM server.

2. In DPM Administrator Console, on the navigation bar, click **Management**, and then click the **Agents** tab.
3. In the **Actions** pane, click **Install**.

   The Protection Agent Installation Wizard opens.
4. On the **Select Agent Deployment Method** page, select **Attach agents**, select **Computer on a trusted domain**, and then click **Next**.
5. On the **Select Computers** page, DPM displays a list of available computers in the same domain as the DPM server. If this is the first time you have used the wizard, DPM queries Active Directory to get a list of potential computers. After the first installation, DPM displays the list of computers in its database, which is updated once each day by the auto-discovery process.

   On the **Select Computers** page, select one or more computers (50 maximum), from the **Computer name** list, click **Add**, and then click **Next**.

   If you know the name of a specific computer on which you want to install the protection agent, you can quickly find and select the computer by typing the name of the computer in the **Computer name** box, and then clicking **Add**. DPM will query Active Directory for the computer, and then add it to the **Selected computers** list. If you do not know the name of the computer, browse the list to find the computer.

   To add multiple computers by using a text file, click the **Add From File** button, and in the **Add From File** dialog box, type the location of the text file or click **Browse** to navigate to its location.
6. On the **Enter Credentials** page, type the user name and password for a domain account that is a member of the local Administrators group on all selected computers.
7. In the **Domain** box, accept or type the domain name of the user account that you are using to install the protection agent on the target computer. This account may belong to the domain that the DPM server is located in or to a trusted domain.

   If you are installing a protection agent on a computer across a trusted domain, enter your current domain user credentials. You can be a member of any trusted domain, and you must be a member of the local Administrators group on all selected computers that you want to protect.
8. On the **Summary** page, click **Attach**.
9. On the **Installation** page, view the results on the **Task** tab to determine whether the installation is successful. You can click **Close** before the wizard is finished installing the agent, and then monitor the installation progress in DPM Administrator Console on the **Agents** tab in the **Management** task area.

If the installation is unsuccessful, you can view the alerts on the **Alerts** tab in the **Monitoring** task area.

Installing Protection Agents on Computers in a Workgroup or Untrusted Domain

If you are installing a protection agent on a computer that is not in an Active Directory domain, you must manually install the protection agent first, and then attach it in DPM Administrator Console. This topic describes how to attach a protection agent on a computer in a workgroup or a domain that does not have a two-trust relationship with the domain that the DPM server is located in.

Note
Before performing the following procedures, you must first manually install the protection agent on the target computer. For step-by-step instructions for manually installing a protection agent, see Installing Protection Agents Manually.

Using non-Active Directory authentication

1. In DPM Administrator Console, on the navigation bar, click **Management**, and then click the **Agents** tab.
2. In the **Actions** pane, click **Install**.

   The Protection Agent Installation Wizard opens.
3. On the **Select Agent Deployment Method** page, select **Attach agents**, select **Computer in workgroup or untrusted domain**, and then click **Next**.
4. On the **Select Computers** page, in the **Computer name** box, type the name of the computer that you want to add to the DPM server. Enter the user credentials for the user account that you created on the computer when you manually installed the protection agent, click **Add**, and then click **Next**.

   Note
   You can add one or more computers at one time up to a maximum of 50 computers.
5. On the **Summary** page, click **Attach**.

After installing the agent, you need to run SetDpmServer and specify the local user credentials which would be used for authentication. A local user account will be created and the DPM protection agent would be configured to use this account for authentication.

Syntax: `SetDpmServer.exe -dpmServerName <serverName> -isNonDomainServer -userName <userName> [-productionServerDnsSuffix <DnsSuffix>]`

Parameter	Description
-IsNonDomainServer	Specifies that this server is in a workgroup or an untrusted domain.
-UserName	Creates an NT user account with the specified username for this server to communicate with DPM server. This option should be used along with -IsNonDomainServer.
-ProductionServerDnsSuffix	In case there are multiple DNS suffixes configured for this server, ProductionServerDnsSuffix represents the DNS suffix which DPM server will use to communicate with this server.
-DpmServerName	Name of the DPM server. FQDN if DPM server and protected computer are accessible to each other using FQDNs. NETBIOS if DPM server and protected computer are accessible to each other using NETBIOS names.

Using certificate-based authentication

1. Install the protection agent on the computer you want to protect.
2. Generate a certificate from the certification authority for the computer you want to protect.
3. Import the certificate to the personal certificate store of Local Computer.
4. Run Using SetDPMServer to complete the setup.

   The program saves a file locally with the certificate metadata. Later, this file is used to attach this agent to the DPM server.

   Tip

   If this file is lost or deleted, you can recreate it by running SetDPMServer.exe.
5. Copy the generated Cert.xml file to the DPM server.
6. Run Using Attach-ProductionServerWithCertificate to attach an untrusted computer to the DPM server.

Repeat these steps on every untrusted computer you want to protect.

Installing Protection Agents on a Read-Only Domain Controller

This topic describes how to install a protection agent on a read-only domain controller (RODC). Note that if a firewall is enabled on the RODC, you must either turn the firewall off or run the following commands before installing the protection agent:

```
netsh advfirewall firewall set rule group="@FirewallAPI.dll,-29502" new enable=yes
netsh advfirewall firewall set rule group="@FirewallAPI.dll,-34251" new enable=yes
netsh advfirewall firewall add rule name=dpmra dir=in program="%PROGRAMFILES%\Microsoft Data Protection Manager\DPM\bin\DPMRA.exe" profile=Any action=allow
netsh advfirewall firewall add rule name=DPMRA_DCOM_135 dir=in action=allow  protocol=TCP localport=135 profile=Any
```

To install a protection agent on a read-only domain controller

1. On the primary domain controller, create and then populate the following security groups, where the protected server name is the name of the RODC on which you plan to install the protection agent:
   - Create a security group named **DPMRADCOMTRUSTEDMACHINES$PSNAME**, and then add the DPM server machine account as a member.
   - Create a security group named **DPMRADMTRUSTEDMACHINES$PSNAME**, and then add the DPM server machine account as a member.
   - Add the DPM server machine account as a member of the **Builtin\Distributed Com Users** security group.
2. Ensure that the security groups that you created earlier have replicated on the RODC.
3. Install the protection agent on the RODC.
4. On the DPM server, perform the following steps to grant launch and activation permissions for the DPMRA service:
   a. Open DPM Management Shell, and then run the command **dcomcnfg.exe**.

      The **Component Services** window opens.
   b. In the **Component Services** window, expand **Computers**, expand **My Computer**, right-click the **DPMRA** service, and then click **Properties**.
   c. Click **General**, and then set the **Authentication Level** to **Default**.
   d. Click **Location**, and then ensure that only **Run application on this computer** is selected.
   e. Under **Launch and Activation Permissions**, select **Customize**, and then click **Edit** to open the **Launch Permission** dialog box.
   f. In the **Launch Permission** dialog box, assign permissions for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** for the DPM server

machine account.

g. Click **OK** to close the dialog box.

h. Navigate to **<drive letter>:\Program Files\Microsoft DPM\DPM\setup**, copy the following files to the RODC at **<drive letter>:\Program Files\Microsoft DPM\DPM\setup**.

- setagentcfg.exe
- traceprovider.dll
- LKRhDPM.dll

5. On the RODC, from an elevated command prompt, run the command **setagentcfg.exe a DPMRA domain\DPMserver** from the location that you specified in the previous step (**<drive letter>:\Program Files\Microsoft DPM\DPM\setup**).
6. Attach the protection agent to the DPM server. For more information about attaching protection agents, see Attaching Protection Agents.

Installing Protection Agents Manually

You can install protection agents manually and, in some circumstances, you must install the protection agent manually, for example, when the computer that you want to protect is behind a firewall, in a workgroup, or in a domain that does not have a two-way trust relationship with the domain that the DPM server is located in.

You can manually install an agent on targeted computers first, and then attach the computers in DPM Administrator Console, or you can attach the targeted computers in DPM Administrator Console first, and then install protection agents on the targeted computers.

Note

If you attach a computer before you install an agent, the agent status for the computer on the **Agents** tab of the **Management** task area of DPM Administrator Console displays an error until you have installed the agent and then refreshed the computer in DPM Administrator Console.

You can also use this procedure if you installing the agent directly from the product DVD.

Use the following procedure to manually install a protection agent.

To install the protection agent manually

1. On the computer that you want to protect, open an elevated Command Prompt window, and then run the following commands:

   net use Z: \\<DPMServerName>\c$

   where *Z* is the local drive letter that you want to assign and *<DPMServerName>* is the name of the DPM server that you want to use to protect the computer.
2. To change the directory, at the command prompt on the targeted computer, run one of

the following commands:

- For a 64-bit computer, type the following command:

  cd /d <assigned drive letter>:\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\3.0.<build number>.0\amd64
  where <*assigned drive letter*> is the drive letter that you assigned in the previous step and <*build number*> is the latest DPM build number.

  For example: **cd /d X:\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\3.0.7696.0\amd64**

  Important
  Ensure that the latest DPM build number is the latest one.

- For a 32-bit computer, type the following command:

  cd /d <assigned drive letter>:\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\3.0.<build number>.0\i386
  where <*assigned drive letter*> is the drive that you mapped in the previous step and <*build number*> is the latest DPM build number.

3. To install the protection agent on the targeted computer, open an elevated Command Prompt window, and then run one of the following commands:

   Important
   If you specify a DPM server name in the command line, it installs the protection agent, and automatically configures the security accounts, permissions, and firewall exceptions necessary for the agent to communicate with the specified DPM server. If you do not specify a DPM server name, you must complete an additional step.

   - For a 64-bit computer, run the following command:

     DpmAgentInstaller_x64.exe <DPMServerName>
     where <*DPMServerName*> is the fully qualified domain name (FQDN) of the DPM server.

     For example: **DPMAgentInstaller_x64.exe DPMserver1.contoso.com**

   - For a 32-bit computer, run the following command:

     DpmAgentInstaller_x86.exe <DPMServerName>
     where <*DPMServerName*> is the fully qualified domain name of the DPM server.

   Note
   To perform a silent installation, you can use the **/q** option after the **DpmAgentInstaller_x64.exe** command.

   For example: **DpmAgentInstaller_x64.exe /q <DPMServerName>**

4. If you specified a DPM server name in the command line in the previous step, this step is not required.

If you did not specify a DPM server name in the command line in the previous step, open an elevated Command Prompt on the targeted computer, and then run the following commands:

a. To change the directory on the targeted computer, run the following command:

   cd /d <system drive>:\Program Files\Microsoft Data Protection Manager\DPM\bin

b. To configure the security accounts, permissions, and firewall exceptions necessary for the agent to communicate with a DPM server, run the following command:

   SetDpmServer.exe –dpmServerName <DPMServerName>

5. If you added the targeted computer to the DPM server before you installed the agent, the DPM server begins to create backups for the protected computer. If you installed the agent before you added the computer to the DPM server, you must attach the computer before the DPM server begins to create backups. For step-by-step instructions about how to add the computer to the DPM server by attaching the protection agent, see Attaching Protection Agents.

Installing Protection Agents Using a Server Image

You can use a server image to install a protection agent without specifying the DPM server by using **DPMAgentInstaller.exe**. After the image is applied to the computer and the computer is brought online, you run **SetDpmServer.exe** to complete the configuration and create the firewall exceptions.

To install a protection agent by using a server image

1. On the computer on which you want to install the protection agent, at a command prompt, type **DpmAgentInstaller.exe**.
2. Apply the server image to a physical computer, and then bring the computer online.
3. Join the computer to a domain, and then log on with a domain user account that is a member of the local Administrators group.
4. At a command prompt, go to **cd <system drive letter>:\Program Files\Microsoft Data Protection Manager\bin**, and run **SetDpmServer.exe <dpm server name>**.

   Specify the fully qualified domain name (FQDN) for the DPM server. For the protected computer's domain or for unique computer names across domains, specify only the computer name.

   Important

You must run SetDpmServer.exe from <*drive letter*>:\Program Files\Microsoft Data Protection Manager\bin. If you run the program from any other location, the operation will fail.

5. Attach the agent by using DPM Administrator Console. For more information, see Attaching Protection Agents.

Attaching Protection Agents

You can add protected computers to a DPM server. On the protected computer, we recommend attaching protection agents to the DPM server for the following types of computers:

- Computers behind a firewall
- Computers on which protection agents already exist
- Computers in a workgroup
- Computers in a domain that does not have a two-way trust relationship with the domain that the DPM server is in

For detailed information about adding your protected computers to a DPM server, see the following topics:

- Installing Protection Agents on Computers Behind a Firewall
- Installing Protection Agents on Computers in a Workgroup or Untrusted Domain

Updating Protection Agents

If you are upgrading a protection agent that is installed on a computer that is not connected to the network, you cannot perform a connected agent upgrade from within DPM Administrator Console. You must perform the upgrade in a non-active domain environment. The DPM server will show that the protection agent update is pending until the client computer is connected to the network.

This topic describes how to update protection agents for both connected and non-connected client computers.

To update a protection agent for a connected client computer

1. In DPM Administrator Console, click **Management** on the navigation bar, and then click the **Agents** tab.
2. In the display pane, select the client computers on which you want to update the protection agent.

   Note
   The **Agent Updates** column indicates for each protected computer when a protection agent update is available. The **Update** action in the **Actions** pane is

not enabled when a protected computer is selected unless updates are available.

3. To install updated protection agents on selected computers, click **Update** in the **Actions** pane.

To update a protection agent on a disconnected client computer

1. In DPM Administrator Console, click **Management** on the navigation bar, and then click the **Agents** tab.
2. In the display pane, select the client computers on which you want to update the protection agent.

   Note
   The **Agent Updates** column indicates for each protected computer when a protection agent update is available. The **Update** action in the **Actions** pane is not enabled when a protected computer is selected unless updates are available.
3. To install updated protection agents on selected computers, click **Update**.
4. For client computers that are not connected to the network, **Update Pending** appears in the **Agent Status** column until the computer is connected to the network.

   After a client computer is connected to the network, **Updating** appears the **Agent Updates** column for the client computer.

Starting and Configuring the WSS Writer Service

Before you can start protecting server farms on servers running Windows SharePoint Services or Microsoft Office SharePoint Server, you must start and configure the Windows SharePoint Services VSS Writer service (WSS Writer service).

After you install the protection agent on the Windows SharePoint Services Web Front End (WFE) server, you must provide the protection agent with the credentials for the Windows SharePoint Services farm.

Important
You must install the protection agent on all the computers in the farm.

You perform the following procedure for a single WFE server. If your Windows SharePoint Services farm has multiple WFE servers, you must select only one WFE server when you configure protection in the Create New Protection Group Wizard.

To start and configure the WSS Writer service

1. On the WFE server, at a command prompt, go to <*DPM installation location*>\bin\.

2. Run **ConfigureSharePoint -EnableSharePointProtection**.
3. Enter your Windows SharePoint Services farm administrator credentials. This account should be a member of the local Administrator group on the WFE server. If the farm administrator is not a local administrator on the WFE server, you must grant the following permissions on the WFE server:
   - Grant the WSS_Admin_WPG group full control to the DPM folder (%Program Files%\Microsoft Data Protection Manager\DPM).
   - Grant the WSS_Admin_WPG group read access to the DPM Registry key (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager).

   Note
   You must rerun **ConfigureSharePoint -EnableSharePointProtection** whenever the Windows SharePoint Services farm administrator password changes.

For more information about using the ConfigureSharePoint command, see Using ConfigureSharePoint.

Optional Configuration Tasks

You can enable optional System Center 2012 – Data Protection Manager (DPM) features during initial configuration or at any time after you deploy DPM. The topics in this section describe the optional features that you can configure.

In This Section

Subscribing to Alert Notifications

Configuring the SMTP Server

Publishing DPM Alerts

Managing Protection Agents

Subscribing to Alert Notifications

You can configure System Center 2012 – Data Protection Manager (DPM) to notify you by e-mail of critical, warning, or informational alerts, and the status of instantiated recoveries.

Note
Before you can subscribe to notifications, you must configure the Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.

To subscribe to notifications

1. In DPM Administrator Console, click **Options** on the tool ribbon.
2. In the **Options** dialog box, on the **Notifications** tab, do the following:
   - Select which types of alerts you want recipients to be notified of (for example, critical alerts, warning alerts, informational alerts, or any combination of these).
   - Under **Recipients**, type an e-mail address for each recipient to whom you want DPM to send copies of the notifications. Use commas to separate the e-mail addresses.
3. To test the notification settings, click **Send Test Notification**, and then click **OK**.

Configuring the SMTP Server

System Center 2012 – Data Protection Manager (DPM) provides options for subscribing to alert notifications and to reports by e-mail. If you plan to enable either of these features, you must first configure the Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send e-mail. Then specify which e-mail server you want to use.

For added security, the SMTP server can be configured as authenticated. When an SMTP server is authenticated, DPM requires a specified user name and password for the server when sending e-mail notifications and reports.

Note
DPM supports sending e-mail through authenticated SMTP servers. Before configuring DPM to use an SMTP server, the mailbox user must have administrator privileges on the DPM server. You must also have administrator privileges if you are using an Exchange Server 2007 Hub Transport server.

To configure DPM to use an SMTP server that does not require authentication

1. In DPM Administrator Console, click **Options** on the tool ribbon.
2. In the **Options** dialog box, on the **SMTP Server** tab, type the SMTP server name, the SMTP server port, and the e-mail address you want to display in the **From** box of the e-mail messages that DPM sends.

   The e-mail address in the **From** box must be a valid e-mail address on the SMTP server.
3. To test the SMTP server settings, click **Send Test E-mail**, type the e-mail address to where you want DPM to send the test message, and then click **OK**.

To configure DPM to use an SMTP server that requires authentication

1. In DPM Administrator Console, click **Options** to display the **Options** dialog box.
2. On the **SMTP Server** tab, type the SMTP server name, the SMTP server port, and the e-mail address you want to display.

3. In the **Authenticated SMTP server** area, type a user name and password in the appropriate boxes.

   Note
   The **User Name** must be the domain user name (for example, domain\user name). The **From** address must be the SMTP address of the user.

4. To test the SMTP server settings, click **Send Test E-mail**, type the e-mail address where you want DPM to send the test message, and then click **OK**.

Publishing DPM Alerts

You use the **Alert Publishing** option only if you have chosen to centrally monitor your DPM servers in Operations Manager. You use this option to synchronize the DPM alerts that are displayed in the DPM Administrator Console with the Operations Manager console.

When you enable the **Alert Publishing** option, all existing DPM alerts that might require a user action are published to the **DPM Alerts** event log. The Operations Manager agent that is installed on the DPM server then publishes the alerts in the **DPM Alerts** event log to Operations Manager and continues to update the console as new alerts are generated.

To publish existing DPM alerts

1. In DPM Administrator Console, click **Options**.
2. In the **Options** dialog box, on the **Alert Publishing** tab, click **Publish Active Alerts**, and then click **OK**.

Managing Protection Agents

After you install a protection agent on the computers that contain the data you want to protect, you can configure the protection agents in the **Management** task area of DPM Administrator Console. For example, you can configure the throttle settings, manually refresh the protection agents, and disable protection agents if you need to perform maintenance tasks on the server.

In This Section

Configuring Throttle Settings

Network bandwidth usage throttling limits the amount of network bandwidth that System Center 2012 – Data Protection Manager (DPM) can use to create and synchronize replicas. Throttling helps to ensure that network bandwidth is available to applications other than DPM.

Important
You must enable QoS on the DPM server and the protected computer.

DPM does not support throttling for bare metal recovery.

To configure network bandwidth usage throttling

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Agent** tab, and then select the computer for which you want to configure network bandwidth usage throttling.
3. In the **Actions** pane, click **Throttle computer**.
4. In the **Throttle** dialog box, select **Enable network bandwidth usage throttling**.
5. Select **Throttle Settings** and **Work Schedule** for the computer.

   Note
   You can configure network bandwidth usage throttling separately for working hours and nonworking hours, and you can define the working hours for the protected computer.
6. To apply your settings, click **OK**.

Refreshing Protection Agents

System Center 2012 – Data Protection Manager (DPM) automatically refreshes protection agents every 30 minutes on servers that are continuously connected to the network. You can manually refresh the agents in the **Management** task area.

To manually refresh the protection agent status

- In the **Management** workspace, click **Agents**, select the computer, and then click **Refresh information** on the tool ribbon.

For client computers that are not continuously connected to the network, DPM will not automatically refresh the agents every 30 minutes. In the **Management** workspace, click **Agents**, the status will appear as **Unknown** until you manually refresh the agent status.

Enabling and Disabling Protection Agents

You might want to disable a protection agent that protects specific data sources when doing the following:

- Performing maintenance tasks on the server
- Debugging a problem that you want to eliminate the System Center 2012 – Data Protection Manager (DPM) agent as a potential cause

When you disable a protection agent, DPM displays a message that all protection and recovery jobs for the protected computer will fail until the agent is re-enabled.

To disable a protection agent

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click **Agents** in the navigation pane, select the computer with the protection agent that you want to disable.

   Note
   Hold down the SHIFT key to select multiple computes.
3. Click **Disable protection agent** on the tool ribbon.
4. In the dialog box, click **OK** to confirm that you want to proceed.

To enable a protection agent

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click **Agents** in the navigation pane, select the computer with the protection agent that you want to enable.

   Note
   Hold down the SHIFT key to select multiple computers.
3. Click **Enable protection agent** on the tool ribbon to enable the protection agent.

Administering and Managing System Center 2012 - DPM

Operations topics for System Center 2012 – Data Protection Manager (DPM) provide targeted practical guidance for performing the most frequent and critical administrative tasks in DPM, including:

- Managing DPM servers
- Managing protected file servers and workstations

- Managing protected servers running Microsoft Exchange, SQL Server, Windows SharePoint Services, Virtual Server, and Hyper-V
- Managing performance
- Managing tape libraries
- Using DPM for disaster recovery

Administering Protected Computers

The topics in this section provide information about performing common maintenance tasks on protected computers, as well as guidance for making changes to the computer configuration or cluster configuration after the computer or cluster is protected by System Center 2012 – Data Protection Manager (DPM).

In This Section

Using Windows Maintenance Tools on Protected Computers

Applying Operating System Updates on Protected Computers

Running Antivirus Software on Protected Computers

Changing DPM Ports on Protected Computers

Using Windows Maintenance Tools on Protected Computers

In general, you can continue maintenance on file servers and workstations protected by System Center 2012 – Data Protection Manager (DPM) using your regular maintenance schedule and the maintenance tools provided in the operating system. Those tools and any impact on data protection are listed in the following table.

Windows Maintenance Tools and Protected Computers

Windows Tool	Considerations
Disk Cleanup: Use to remove temporary files, Internet cache files, and unnecessary program files.	Running Disk Cleanup should have no adverse affect on performance or data protection.
Disk Defragmenter: Use to analyze volumes for the amount of fragmentation and to defragment volumes.	Before adding a volume to a protection group, check the volume for fragmentation, and if necessary, defragment the volume by using Disk Defragmenter. When protection is applied to extremely fragmented volumes, boot times

Windows Tool	Considerations
	on the protected computer might be slowed down and protection jobs might fail. It is recommended that you run Disk Cleanup before running Disk Defragmenter.
Chkdsk.exe: Use to check the file system and file system metadata for errors and to display a status report of its findings.	Before you run **chkdsk /f** on a protected volume, verify that a consistency check of that volume is not being performed. Running **chkdsk /f** on a protected volume while a consistency check is being performed on that volume can cause 100% CPU utilization. Run synchronization with consistency check after running Chkdsk.exe on the protected computer.

Applying Operating System Updates on Protected Computers

An important part of computer maintenance is ensuring that operating systems and software are up to date. Updates—known as fixes, patches, service packs and security rollup packages—help to protect computers and data.

You can use your preferred method for deploying software updates, such as Automatic Updates or Windows Server Update Services, on System Center 2012 – Data Protection Manager (DPM) protected computers. Because some software updates require a computer restart, you should schedule or perform the updates at times that have the least impact on protection operations.

See Also

Protecting File Servers and Workstations

Running Antivirus Software on Protected Computers

Using Windows Maintenance Tools on Protected Computers

Running Antivirus Software on Protected Computers

To prevent data corruption of replicas and shadow copies, configure the antivirus software to delete infected files rather than automatically cleaning or quarantining them. Automatic cleaning and quarantining can result in data corruption because these processes cause the antivirus software to modify files, making changes that System Center 2012 – Data Protection Manager (DPM) cannot detect. For information about configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

For information about configuring firewalls on computers when installing protection agents, see Installing Protection Agents.

See Also

Applying Operating System Updates on Protected Computers

Protecting File Servers and Workstations

Using Windows Maintenance Tools on Protected Computers

Changing DPM Ports on Protected Computers

System Center 2012 – Data Protection Manager (DPM) requires ports 5718 and 5719. If these ports are already used by another program, the backup jobs will run, but the recoveries will fail. If it is possible, reassign the ports to DPM. Otherwise, complete the following procedure to change the ports for DPM.

To change DPM ports on a protected computer

1. Locate the SetAgentcfg.exe file on the DPM server. By default, the file is located at the following path: **%PROGRAMFILES%\Microsoft DPM\DPM\Setup\SetAgentCfg.exe**.
2. Copy the file to the protected computer that is experiencing the problem. Copy the file to the agent DPM\Bin directory. By default, the file is located at the following path: **%PROGRAMFILES%\Microsoft Data Protection Manager\DPM\bin**.
3. On the protected computer, open an elevated command prompt, change the directory to where the SetAgentCfg.exe file was copied. For example, %PROGRAMFILES%\Microsoft Data Protection Manager\DPM\bin.
4. Run the following command to change the ports that are used by the DPM Agent: **SetAgentCfg e dpmra <port number> <alternate port number>**.
5. Restart the DPM RA service.

Protecting File Servers and Workstations

The topics in this section provide information about performing common maintenance tasks on protected file servers and workstations, as well as guidance for making changes to the computer configuration or cluster configuration after the computer or cluster is protected by System Center 2012 – Data Protection Manager (DPM).

In This Section

Performing File Server and Workstation Management Tasks

Managing Clustered File Servers

Protecting deduplicated volumes

See Also

Administering DPM Servers

Managing Performance

Protecting Exchange Servers

Protecting SQL Servers

Protecting SharePoint Servers

Protecting Virtual Servers

Managing Tapes

Performing File Server and Workstation Management Tasks

When events or business requirements demand it, you might need to make changes to your protected file servers and workstations or to the data sources on the protected computer. The topics in this section discuss the impact certain changes might have on System Center 2012 – Data Protection Manager (DPM) protection.

In This Section

Changing the Path of a Data Source

Moving File Servers and Workstations Between Domains

How to Rename a File Server or Workstation

How to Change the Time Zone of a File Server or Workstation

Using Migrate-Datasource

Using MigrateDatasourceDataFromDPM

See Also

Managing Clustered File Servers

Managing Performance

Changing the Path of a Data Source

Changing the Path of a Shared Data Source

When you protect a shared folder, the path to the shared folder includes the logical path on the volume. If you move the shared folder, protection will fail.

If you must move a protected shared folder, remove it from its protection group and then add it to protection after the move.

Changing the Path of an Encrypted Data Source

If you change the path of a System Center 2012 – Data Protection Manager (DPM) protected data source on a volume that uses the Encrypting File System (EFS) and the new file path exceeds 5120 characters, data protection will fail. You must ensure that the new file path of the protected data source uses fewer than 5120 characters.

See Also

How to Change the Time Zone of a File Server or Workstation

How to Rename a File Server or Workstation

Protecting File Servers and Workstations

Moving File Servers and Workstations Between Domains

Moving File Servers and Workstations Between Domains

You cannot do the following for protected computers:

- Change the domain of a protected computer and continue protection without disruption.
- Change the domain of a protected computer and associate the existing replicas and recovery points with the computer when it is re-protected.

We recommend that you do not change the domain of a protected computer. If you must change the domain of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection while the computer retains its original domain membership.
- Protect the data source on the computer after it becomes a member of another domain.

To change the domain membership of a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the domain membership of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

   For information about performing tasks involving protection agents and protection groups, see DPM Help.

See Also

Changing the Path of a Data Source

How to Change the Time Zone of a File Server or Workstation

How to Rename a File Server or Workstation

Protecting File Servers and Workstations

How to Rename a File Server or Workstation

System Center 2012 – Data Protection Manager (DPM) uses the computer name as a unique identifier for replicas, recovery points, DPM database entries, reporting database entries, and so on.

You cannot do the following:

- Change the name of a protected computer and continue protection without disruption.
- Change the name of a protected computer and associate the existing replicas and recovery points with the new computer name.

We recommend that you do not change the name of a protected computer. If you must change the name of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection (the old computer name).
- Protect the data source on the computer (the new computer name).

To rename a protected computer

1. Stop protection for all data sources on the computer by removing them from the protection group.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the name of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

   For information about tasks that involve protection agents and protection groups, see DPM Help.

See Also

Changing the Path of a Data Source

How to Change the Time Zone of a File Server or Workstation

Protecting File Servers and Workstations

Moving File Servers and Workstations Between Domains

How to Change the Time Zone of a File Server or Workstation

System Center 2012 – Data Protection Manager (DPM) automatically identifies the time zone of a protected computer during installation of the protection agent. If a protected computer is moved to a different time zone after protection is configured, ensure that you do the following:

- Change the computer time in Control Panel by using the **Time Zone** tab in the **Date and Time Properties** dialog box.
- Update the time zone in the DPM database.

For more information about time zones and DPM protection, see Coordinating Protection Across Time Zones.

To update the time zone in the DPM database

1. On the protected computer, in **Add or Remove Programs**, uninstall **Microsoft System Center Data Protection Manager Protection Agent**.
2. On the DPM server, in DPM Administrator Console, in the **Management** task area, click the **Agents** tab, select the computer, and then, in the **Actions** pane, click **Refresh**

information.

The agent status will change to **Error**.

3. In the **Details** pane, click **Remove the record of the computer from this DPM computer**.
4. Reinstall the protection agent on the computer.
5. Run synchronization with consistency check for each protected volume on the protected computer.

See Also

Changing the Path of a Data Source

How to Rename a File Server or Workstation

Protecting File Servers and Workstations

Moving File Servers and Workstations Between Domains

Using Migrate-Datasource

Migrate-Datasource is a command-line script that lets you continue protecting a data source (file, folder, volume, or share) to the same replica volume even after it has been migrated to a different volume on the same protected computer. You have to run the Migrate-Datasource script even if you have not changed the drive letters of the volume because System Center 2012 – Data Protection Manager (DPM) recognizes volumes by the GUID and not the drive letter.

Important

If you have secondary DPM protection configured, you must run the Migrate-Datasource script on the secondary server also.

Note

Migrate-Datasource is used to migrate protected computer volumes while MigrateDatasourceDataFromDPM is used to migrate DPM volumes.

The possible reasons for moving DPM-protected data sources across volumes include the following:

- The disk is corrupt.
- Organization policy demands that disks be replaced at certain time intervals.

Syntax

Migrate-Datasource.ps1 [-DPMServerName] <*string*> [-Option [auto or manual]] [-PSName] <*string*>

Parameter	Description
DPMServerName	Name of the DPM server from which you want to migrate data.
Option	Indicates whether DPM should perform an automatic or manual migration. Automatic: If you specify the automatic option, DPM migrates all the data sources on the protected computer. Use this option if you created a new volume but retained the logical path (for example, if F:\ was reformatted on a new disk but is still called F:\, or the mount point is still the same). DPM automatically updates the mappings for the replica of F:\ to the new volume that is now called F:\. Manual: If you specify the manual option, you have to migrate each data source individually. The script gives you a list of volumes protected by DPM that are not present and a list of unprotected volumes. You can then map the volumes individually. Use this option if the logical path was not preserved (for example, G:\ became H:\).
PSName	Name of the protected computer to which the data source is being migrated.

Things to Remember

- Migrate-Datasource is used only for migration of file system data sources, such as volumes. For other data sources, follow the instructions in the alerts.
- DPM does not support migration from a volume on a drive (for example, D:\) to a mounted volume (for example, E:\<mountpoint>, where mountpoint is a location on which the volume has been mounted).
- For auto-migration of mounted volumes, the volume on the new computer should have the same mount point name as the volume on the previously protected computer. DPM does not allow you to migrate to a drive.
- For migration of mounted volumes (where the old volume is protected by using a mount point):
    - If the protected volume has multiple mount points, at least one mount point of the volume on the new computer should have the same mount point path as before.
      Old volume: C:\mnt
      new volume: C:\mnt (may have drive letter and other mount points)

    - If the volume also has a drive letter, only the drive letter is visible while you select the new volume for migration. This should be selected manually.
- You should migrate volumes only if you have reformatted them or if the volume GUID associated with the volume has changed.

Note
After migration, you cannot perform original location recovery for the recovery points created before the migration. Recovery fails with the message **Couldn't find the selected volume**. You can, however, recover to an alternate location.

Using MigrateDatasourceDataFromDPM

MigrateDatasourceDataFromDPM is a command-line script that lets you migrate System Center 2012 – Data Protection Manager (DPM) data for a data source – replica volumes and recovery point volumes – across disks. Such a migration might be necessary when your disk is full and cannot expand, your disk is due for replacement, or disk errors show up.

Note
MigrateDatasourceDataFromDPM is used to migrate DPM volumes whereas Migrate-Datasource is used to migrate protected computer volumes.

Depending on how you have configured your environment, this could mean one of more of the following scenarios for moving data source data:

- DPM disk to DPM disk
- Data source to DPM disk
- Data source to custom volume

The MigrateDatasourceDataFromDPM script moves all data for a data source or disk to the new disk or volume. After migration is complete, the original disk from where the data was migrated is not chosen for hosting any new backups. You must retain your old disks until all recovery points on them expire. After the recovery points expire, DPM automatically unallocates the replicas and recovery point volumes on these disks.

Migrating does not move recovery point data on the replica, it simply makes new replica and recovery point volumes, then copies the replica data to the new replica. VSS shadow copies are volume specific and cannot be moved or copied. So while all new recovery points are made on the migrated disk, the old replicas and recovery points on the old volume are still required. However, if you want to remove the old disk sooner, then you can reduce the retention range and wait for the old recovery points to expire.

All backup schedules continue to apply and protection of the data source continues as before.

After migrating the replica of a data source that has secondary protection enabled, you must start the Modify Protection Group wizard on the secondary DPM server, select the same data source, and complete the wizard. This reconfigures secondary backups to run from the new replica volume on the primary DPM server.

Syntax

MigrateDatasourceDataFromDPM.ps1 [-DPMServerName] <*string*> [-Source] <*disk[]*> [-Destination] <*disk[]*>

MigrateDatasourceDataFromDPM.ps1 [-DPMServerName] <*string*> [-Source] <*data source*> [-Destination] <*disk[]*>

MigrateDatasourceDataFromDPM.ps1 [-DPMServerName] <*string*> [-Source] <*data source*> [-Destination] <*DPM server volume[]*>

Parameter	Description
DPMServerName	Name of the DPM server for which you want to migrate data.
Source	The location from which the data must be moved. This can be either a DPM disk (use Get-DPMDisk to retrieve the disk) or a DPM data source (use Get-Datasource to retrieve the data source). The source can be a set of disks.
Destination	The location to which the data must be moved. This can be either a DPM disk array (use Get-DPMDisk to retrieve the array of disks) or an array of two DPM volumes (use Get-DPMVolume to retrieve the list of DPM volumes on the server). The first element of the array is the destination replica volume and the second the recovery point volume. The destination disks must be added to the DPM disk pool before migration.

Note
The numbering for the disk array starts with 0.

Examples

The following examples show how the script works.

Example 1: Disk D1 contains the replica and recovery points for the data source DS1.

Disk	Replica	Recovery Point
D1	R1	RP1

To do a disk to disk migration of the volumes on D1 to another disk D2, do the following:

$disk = Get-DPMDisk –DPMServerName DPMTestServer
./MigrateDatasourceDataFromDPM.ps1 –DPMServerName DPMTestServer –Source $disk[0] –Destination $disk[1]

This results in the following:

Disk	Replica	Recovery Point
D1	R1	RP1
D2	R1’	RP1’

You need to retain D1 for the retention range of the latest recovery point on it, usually one month. After the latest recovery point expires, DPM will deallocate the replicas and recovery points on disk D1 automatically.

Example 2: Disk D1 contains the replica of the data source DS1 and the recovery point for data source DS2. Disk 2 contains the replica of DS2 and the recovery point for DS1.

Disk	Replica	Recovery Point
D1	R1	RP2
D2	R2	RP1

If you do a DPM disk to DPM disk migration to a third disk (Disk 3), this disk will have four volumes, replicas and recovery points for DS1 and DS2.

$disk = Get-DPMDisk –DPMServerName DPMTestServer
./MigrateDatasourceDataFromDPM.ps1 –DPMServerName DPMTestServer –Source $disk[0] –Destination $disk[2]

This results in the following:

Disk	Replica	Recovery Point
D1	R1	RP2
D2	R2	RP1
D3	R1’ and R2’	RP1’ and RP2’

This happens because DPM cannot move just a replica or a recovery point, it will always move them in pairs, hence even though the command only moves the volumes from D1, DPM will move also the related replica and recovery point.

Example 3: Disk D1 contains the replica of the data source DS1 and the recovery point for data source DS2. Disk D2 contains the replica of DS2 and the recovery point for DS1.

Disk	Replica	Recovery Point
D1	R1	RP2
D2	R2	RP1

If you choose to migrate only the data for DS1 to a third disk (Disk 3), this disk will have two volumes, the replica and recovery point for DS1.

$pg = Get-ProtectionGroup DPMTestServer
$ds = Get-Datasource $pg[0]
$disk = Get-DPMDisk –DPMServerName DPMTestServer
./MigrateDatasourceDataFromDPM.ps1 –DPMServerName DPMTestServer –Source $ds[0] –Destination $disk[2]

Disk	Replica	Recovery Point
D1	R1	RP2
D2	R2	RP1
D3	R1’	RP1’

Managing Clustered File Servers

On planned failover of a cluster, System Center 2012 – Data Protection Manager (DPM) continues protection. On unplanned failover, DPM issues an alert that a consistency check is required.

For a non-shared disk cluster, planned failover may also require a consistency check.

In This Section

Changing File Server Cluster Members

Changing Resource Groups on Clustered File Servers

See Also

Managing Performance

Performing File Server and Workstation Management Tasks

Changing File Server Cluster Members

When you make changes to a server cluster that is protected by System Center 2012 – Data Protection Manager (DPM), DPM takes the following actions:

- When a new server is added to a cluster, DPM issues an alert to install a protection agent on the new cluster node and protection fails.
- When a server is removed from a cluster, DPM detects that a node has left the cluster and the server now appears separate from the cluster with no data protected on it.

For example, assume you have a server cluster that contains four computers: Node1, Node2, Node3, and Node4. You need to replace computer Node4 with a new computer, named Node5.

You use the administration console for your cluster service to add Node5 to the cluster and configure the resources that can be failed over to Node5.

DPM issues an alert that protection of the server cluster will fail until a protection agent is installed on Node5. You install the protection agent on Node5.

You fail over the resources from Node4 to other nodes in the cluster. When no resources remain on Node4, you remove it from the cluster. DPM detects the failovers and continues protection of the cluster.

DPM detects that Node4 has left the cluster—it appears as a stand-alone node now. If it no longer exists on the network, you can remove the record for this server in DPM Administrator Console.

See Also

Changing Resource Groups on Clustered File Servers

Performing File Server and Workstation Management Tasks

Changing Resource Groups on Clustered File Servers

A cluster node can have any number of resource groups. Moving a DPM protected data source to a resource group, between resource groups, or out of a resource group can cause protection job failures. To successfully make any of those changes to resource group membership, perform the following steps:

1. Stop existing protection of the data source. The data source could belong to a protection group as a single data source on a protected server or as a data source as a member of a resource group.
2. Begin protection of the data source according to its new status, either as a single data source on a protected server or as a data source as a member of a resource group. This will allocate a new replica for the data source.

Changing the name of a resource group will affect the protection of all data sources in the resource group. To change the name of a resource group, perform the following steps:

1. Stop protection of the resource group.
2. Change the name of the resource group.
3. Begin protection of the resource group under its new name.

See Also

Changing File Server Cluster Members

Performing File Server and Workstation Management Tasks

Protecting deduplicated volumes

Data deduplication is a new feature in Windows Server 2012. This feature finds and removes duplication within data on a volume while ensuring that the data remains correct and complete. This makes it possible to store more file data in less space on the volume. Data deduplication is implemented per volume , which means that Windows Server 2012 allows data deduplication to be applied to a whole volume and not to selected files or folders only. Data Protection Manager (DPM) supports protection for Windows Server 2012 volumes that have the deduplication feature enabled.

Warning
You must not enable the data deduplication feature on a DPM disk.

Protect volumes with deduplication

The process to protect a volume with data deduplication is the same as protecting a normal volume. However, you must consider the following actions when you protect a volume that has the deduplication feature enabled.

Important
Protection of volumes with data deduplication enabled is supported only in System Center 2012 SP1 DPM.

- You must enable the Data Deduplication role on the DPM server to protect deduplicated volumes.
- If the entire volume is protected, then DPM provides only optimal protection. If only partial deduplicated volume is protected, then DPM will provide normal backup.
- If you protect data to tape, the data will be stored in unoptimized form.
- End-user recovery for deduplicated volumes will be done in unoptimized form.
- Protection for volumes with data deduplication enabled is not supported for online backup to Windows Azure Online Backup.

When you protect a volume with data deduplication enabled, DPM leverages the benefits of the feature. Specifically, the data from such a volume is stored optimally, and network transfers of the also happen in an optimized form.

Recover volumes with deduplication

The process to recover a volume with data deduplication enabled is the same as recovering a normal volume. However, you must consider the following actions when you perform volume recovery.

- To do full volume (optimal) recovery, you must recover to an empty and formatted volume, and you should not enable the deduplication feature on the target volume.
- If you recover an item by using Item-level recovery, it will be recovered in an unoptimized state.
- If you recover the entire deduplicated volume, the recovery will be optimized. If you recover only selected files and folders, , the recovery will not be optimized.
- You cannot recover a deduplicated volume to a computer that does not have the Windows Server 8 operating system.

See Also

Install and Configure Data Deduplication

Protecting ReFS volumes

The Resilient File System (ReFS) is the new file system in Windows Server 2012. This file system is an improvement on the existing NTFS file system. DPM seamlessly protects and recovers data on ReFS volumes.

Supported scenarios

The procedure to protect and recover ReFS volumes is the same as with the earlier NTFS volumes. All the supported scenarios for NTFS are also supported for ReFS.

Unsupported scenarios

There are a few limitations to DPM protection of ReFS volumes.

- You cannot restore encrypted files that were protected from an NTFS volume to a ReFS volume.
- You cannot protect custom volumes with ReFS.

Protecting Exchange Servers

All information in this section pertains to Microsoft Exchange 2003, Exchange 2007, Exchange 2010 and Exchange 2013 unless otherwise specified.

In This Section

Exchange Server 2010 Prerequisites

The minimum version of Exchange Server that System Center 2012 – Data Protection Manager (DPM) can protect is Exchange Server 2010 with Rollup Update version 1 (RU1).

Installing Protection Agents on Exchange Server 2010 Nodes

To protect an Exchange Server 2010 DAG node, you must install a protection agent on the node. For instructions about installing protection agents, see Installing Protection Agents.

System Center 2012 – Data Protection Manager (DPM) enables you to protect Exchange Server 2010 DAG nodes from different DPM servers. However, one node can be protected by only one DPM server. For example, assume that DAG1 has nodes N1, N2, N3, N4, and N5. One DPM server can protect N1, N2, and N5, and another DPM server can protect nodes N3 and N4.

With DPM, the maximum amount of data that you can protect with a single DPM server is 80 TB. Therefore you can protect DAG's that have up to 20 nodes with a single server or up to 10,000 mailboxes with a DPM server.

Note

When you install a protection agent on a DAG node, DPM displays the following warning: "You cannot protect cluster data in the selected nodes without installing agents on the other nodes." This is a DPM warning when you are protecting clusters. This does not relate to Exchange Server 2010 and you can ignore this message.

Protecting Exchange Server 2010

You can use the **Create New Protection Group Wizard** to protect Microsoft Exchange Server 2010.

System Center 2012 – Data Protection Manager (DPM) will protect the Exchange Server databases for Exchange Server 2010 that are contained in a database availability group (DAG).

Warning

You cannot recover the database if the name of the Exchange Server database starts with a space. Make sure that the database name does not start with a space.

Note

If you try to perform parallel backups on multiple copies of the same Exchange Server database, then the backup procedure will fail.

In addition to the wizard pages that you completed to protect Exchange Server 2007, you must perform the steps on the following wizard pages to protect Exchange Server 2010.

To protect Microsoft Exchange Server 2010:

1. On the **Select Protection Group Type** page, select **Server**, and then click **Next** to continue.
2. On the **Select Group Members** page, expand the domain under which the DAG resides. When you expand the DAG, all the existing databases, together with their respective nodes are displayed. Select the data that you want to protect, and then click **Next** to continue.

   Note

   The **Create New Protection Group** Wizard does not indicate which databases are active or passive. Make sure that you already know which databases are active or passive. For servers that are part of a DAG, the databases will be listed under the <DAG-name> node.
3. On the **Specify Exchange Protection Options** page, specify if you want to run the Eseutil tool on one of the Exchange Server databases. For members on Exchange Server 2010, select if you want to run the Eseutil tool for both the database and the log files, or just for the log files. If you protect the DAG servers, you should run the Eseutil tool for log files only. For standalone servers, you should select both the database and the log files.
4. On the **Specify Exchange DAG Protection** page, select the databases for copy backup and express full backup. To protect multiples copies of the same database, select only one database for express full and incremental backup, and then select the remaining copies for copy backup.

5. On the **Select Data Protection Method** page, select whether you want to use short-term disk-based protection or long-term tape-based protection, and then click **Next** to continue.
6. On the **Select Short-term Goals** page, specify your protection goals, such as retention range and synchronization frequency, and then click **Next** to continue.
7. On the **Summary** page, review your selections, and then click **Create Group** to complete the wizard.

Note

If you change the status of the Exchange Server database from active to passive or vice-versa, you are not required to make any changes on the DPM server. DPM will continue to back up the data from the same node without any failures.

Recovering Exchange Server 2010 Data

You can use System Center 2012 – Data Protection Manager (DPM) to recover Exchange Server 2010 mailboxes and mailbox databases. The procedures to recover Exchange Server 2010 data are the same as those to recover Exchange Server 2007 data.

Recovering Exchange Server 2010 Mailboxes

DPM supports the following types of recovery for Exchange Server 2010 mailboxes:

- **Recover to an Exchange Server database.** Recover only to Exchange Server recovery databases.
- **Recover to a network location.** Copy the database to a network folder.
- **Copy to tape.** Create an on-tape copy of the database.

Recovering Exchange Server 2010 Mailbox Databases

Changing the status of a database from active to passive or vice versa may affect the recovery process. If the database is passive, DPM cannot perform a Volume Shadow Copy Service (VSS) recovery.

Recovering to the active database is the same as recovering to an Exchange Server 2010 stand-alone node. The Exchange Server administrator must synchronize the passive copy from the recovered active copy by running the Resume-MailboxDatabaeCopy cmdlet on the Exchange server. You can recover a database only on the node that was protected.

DPM supports the following five types of recovery for Exchange Server 2010 mailbox databases:

1. **Recover the database to its original location.** Overwrite the existing copy of the database.
2. **Recover the database to an alternate database.** Restore to another database on an Exchange Server.

3. **Recover to an Exchange Recovery database.** Recover to an Exchange Recovery database instead of a standard mailbox database.
4. **Recover to network location.** Copy the database to a network folder.
5. **Copy to tape.** Create an on-tape copy of the database.

Note
DPM does not support recovering mailbox databases to passive databases. While recovering to the original database or to an alternate database, the target database on which the recovery is being performed should not be passive.

Performing General Maintenance on Servers Running Exchange

General maintenance includes tasks such as disk and file maintenance, updating operating systems and applications, and protecting data by using antivirus software and performing regular backups.

For servers running Microsoft Exchange Server, there are also Exchange maintenance tasks that occur regularly, such as database defragmentation and index purging.

When you need to perform maintenance on a protected server and do not want protection jobs to continue for the duration of the maintenance, you can use the following procedure to disable the protection agent.

Note
If you disable a protection agent for a server that is a cluster node, you should disable the protection agent for every node of the cluster.

In This Section

Performing Offline Defragmentation

Most Microsoft Exchange maintenance tasks should have no adverse affect on performance or data protection. However, special considerations apply when you are performing offline database defragmentation on Exchange servers that are protected by System Center 2012 – Data Protection Manager (DPM).

Offline defragmentation involves using the Exchange Server Database Utilities (Eseutil.exe), an Exchange Server utility that you can use to defragment, repair, and check the integrity of Exchange server databases.

If you must perform an offline defragmentation, you should perform a synchronization with consistency check for protected storage groups when defragmentation is complete.

Performing Exchange Server Management Tasks

This section provides instructions and guidelines for managing a protected Exchange server and making changes after the initial System Center 2012 – Data Protection Manager (DPM) configuration.

In This Section

Upgrading Exchange Server 2003 to Exchange Server 2007

You cannot upgrade a computer running Microsoft Exchange Server 2003 to Exchange Server 2007. For instructions on transitioning from Exchange Server 2003 to Exchange Server 2007, see Upgrading to Exchange Server 2007.

In general terms, the transition consists of deploying computers running Exchange Server 2007 and then moving storage groups from the computers running Exchange Server 2003 to the new servers.

How to maintain data protection during a transition to Exchange Server 2007

1. Deploy Exchange Server 2007.
2. Create empty storage groups and databases on the computer running Exchange Server 2007.
3. Install protection agents on the computers running Exchange Server 2007.

4. Create new protection groups, and add the databases and storage groups that you created in step 2.
5. Move the mailboxes to the computers running Exchange Server 2007.
6. Remove all storage groups that will be moved to computers running Exchange Server 2007 from their existing protection groups, selecting the **Retain protected data** option.

   DPM will retain the associated replica, recovery points, and tapes for the retention range specified. You can recover data from the recovery points and tapes to a computer running Exchange Server 2003.

Moving Exchange Servers Between Domains

You cannot do the following for protected computers:

- Change the domain of a protected computer and continue protection without disruption.
- Change the domain of a protected computer and associate the existing replicas and recovery points with the computer when it is re-protected.

We recommend that you do not change the domain of a protected computer. If you must change the domain of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection while the computer retains its original domain membership.
- Protect the data source on the computer after it becomes a member of another domain.

Renaming an Exchange Server

System Center 2012 – Data Protection Manager (DPM) uses the computer name as a unique identifier for replicas, recovery points, DPM database entries, reporting database entries, and so on.

You cannot do the following:

- Change the name of a protected computer and continue protection without disruption.
- Change the name of a protected computer and associate the existing replicas and recovery points with the new computer name.

We recommend that you do not change the name of a protected computer. If you must change the name of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection (the old computer name).
- Protect the data source on the computer (the new computer name).

Adding Storage Groups and Databases

When adding a new storage group to a protected Microsoft Exchange server, you must add it to a protection group manually. When adding a new database to the storage group, a full backup is required, which can be accomplished by an express full backup or a consistency check. Incremental backups will fail until a full backup is completed.

In Exchange Server 2010, databases are grouped under database availability group (DAG). If a database in a DAG on which express full backup is configured goes down temporarily and returns back then you do not have to perform any action.

However if it goes down for a longer duration, then the backups will fail and Exchange Server will be unable to truncate log files for that database. Also the respective DAG node on which the database exists may run out of disk space.

To resolve this issue, you must manually reconfigure an express full backup on another copy of the database so that log truncation happens for that database.

Dismounting Databases

When a database that belongs to a protected storage group is dismounted, protection jobs for that database only will fail. Logs for that storage group will not be truncated. However, the longer that the database remains dismounted, the more likely it is that the log space on the Microsoft Exchange server will overflow, which will result in the dismount of the storage group on the Exchange server. If the database will not be needed, you should delete it.

Changing the Path of a Database or Log File

If a protected database or log files are moved to a volume that contains data that is protected by System Center 2012 – Data Protection Manager (DPM), protection continues. If a protected database or log files are moved to a volume that is not protected by DPM, DPM displays an alert and protection jobs will fail. To resolve the alert, in the alert details, click the **Modify protection job** link and then run a consistency check.

If a recovery point is created after the path changes, you cannot recover the storage group or recovery points from recovery points based on the old path. You can still recover data to a network folder.

If you recover a Microsoft Exchange 2003 storage group after the path for databases or log files has changed and the most recent recovery point was created before the path change, the recovery copies the files to the old path and tries to mount the databases. If the databases can be mounted, the recovery appears to succeed.

If this occurs, you can take one of the following actions:

- Change the databases back to the original path and then recover the storage group again.
- Recover the databases using the **Copy to a network folder** option. Specify the new location of the databases as the copy destination. Select the **Bring database to a clean shutdown after copying the files** option. Mount the database after recovery.

If you recover an Exchange 2007 storage group after the path for databases or log files has changed and the most recent recovery point was created before the path changed, DPM will recover the databases to the new location.

When you change the path of log files for a storage group that uses disk-to-tape backup and only incremental backups have been performed since the path change, recovery of a storage group using **Latest** as the recovery point will fail. To avoid this issue, perform one of the following actions:

- Run a full backup and then retry the storage group recovery.
- Recover individual databases, rather than the storage group.
- Recover the storage group to a network folder as files.

Renaming Storage Groups

To rename a protected storage group, complete the following procedure.

To change the name of a protected storage group

1. Rename the storage group.
2. Restart the information store.
3. Stop the protection with retain data.
4. Reprotect the database.

   If you do not reprotect the database, the backups will continue to work, but the mailbox enumeration will fail.

Warning

Recovery to the original location from the recovery points that were created before you renamed the storage group will fail. To recover from those recovery points, rename the storage group to the old name .

Moving Databases Between Storage Groups

The following table describes the impact on data protection when you move a database between storage groups.

Data Protection When Databases Are Moved Between Storage Groups

From	To	Result
A protected storage group	A protected storage group	DPM continues protection of the database. Run a consistency check for both storage groups after the move.
A protected storage group	A storage group that is not protected	DPM stops protection of that database. Run a consistency check for the protected storage group after the move.
A storage group that is not protected	A protected storage group	DPM begins protection of that database if the database files are on a volume protected by DPM. If the database files are not on a protected volume, run the Modify Group Wizard. Run a consistency check for the protected storage group after the move.

Improving DPM Recoverable Object Search

The time required for DPM Recoverable Object Search to return recovery points that meet the specified criteria increases as the number of recovery points grows and as the DPM database (DPMDB) becomes more fragmented. You can reduce the search time by performing regular maintenance on the DPM database.

To improve the performance of the recovery point search for a data source, you need to rebuild or reorganize the indexes related to that data source. The following table lists the database tables for which indexes need to be rebuilt for a specific data source.

Data source	Tables in DPMDB
SharePoint	tbl_RM_SharePointRecoverableObject tbl_RM_RecoverySource
Exchange Mailbox	tbl_RM_DatasetROMap tbl_RM_RecoverableObject tbl_RM_RecoverySource

Rebuilding Indexes

Rebuilding an index deletes the index and creates a new one. Rebuilding an index removes fragmentation and reclaims disk space by compacting the pages that are using the specified or existing fill factor setting, and the index rows are reordered in contiguous pages, allocating new pages as needed. This can improve SQL query performance by reducing the number of page reads required to obtain the requested data.

Query to rebuild an index

```
USE DPMDB
GO
ALTER INDEX ALL ON <tableName> REBUILD
GO
```

Reorganizing Indexes

Reorganizing an index defragments the leaf level of clustered and nonclustered indexes on tables and views by physically reordering the leaf-level pages to match the logical order (left to right) of the leaf nodes. Having the pages in order improves index-scanning performance. The index is reorganized within the existing pages allocated to it; no new pages are allocated. If an index spans more than one file, the files are reorganized one at a time. Pages do not migrate between files.

Reorganizing an index also compacts the index pages. Any empty pages created by this compaction are removed providing additional available disk space. In some cases, the gain might not be significant. It is also takes longer than rebuilding the index.

Query to rebuild indexes

```
USE DPMDB
GO
ALTER INDEX ALL ON <tableName> REORGANIZE
GO
```

Rebuilding Compared To Reorganizing

Rebuilding	Reorganizing
Takes the table whose indexes are being currently rebuilt offline. Rebuilding should be done when it will least affect normal operations.	Leaves the table whose indexes are being reorganized online and working normally. Does not affect normal operations.
Substantial performance gains in search and browse operations.	Moderate performance gains in search and browse operations.
Not a time intensive operation.	Usually a time intensive operation.

Rebuilding	Reorganizing
Most effective when index is heavily fragmented.	Most effective when index is not heavily fragmented.

Additional Resources

ALTER INDEX (Transact-SQL)

Renaming Mailboxes

If you need to rename your mailbox, follow these steps to ensure continued protection of your data. This procedure is the same for Exchange 2007 and Exchange 2012.

Protecting a renamed mailbox

1. Rename the mailbox.
2. Stop protection for the mailbox with Retain Data.
3. Reprotect the database.

Warning
Recovery to original location from recovery points created before renaming the database will fail. Revert to the old name, if you want to recover from these recovery points

Managing Clustered Exchange Servers

On planned failover of a cluster, System Center 2012 – Data Protection Manager (DPM) continues protection. On unplanned failover, DPM issues an alert that a consistency check is required.

For a non-shared disk cluster, planned failover might also require a consistency check.

In This Section

Changing Exchange Server Cluster Members

Changing Resource Groups on Clustered Exchange Servers

Changing Exchange Server Cluster Members

When you make changes to a server cluster that is protected by System Center 2012 – Data Protection Manager (DPM), DPM takes the following actions:

- When a new server is added to a cluster, DPM issues an alert to install a protection agent on the new cluster node and protection fails.
- When a server is removed from a cluster, DPM detects that a node has left the cluster and the server now appears separate from the cluster with no data protected on it.

For example, assume you have a server cluster that contains four computers: Node1, Node2, Node3, and Node4. You need to replace computer Node4 with a new computer, named Node5.

You use the administration console for your cluster service to add Node5 to the cluster and configure the resources that can be failed over to Node5.

DPM issues an alert that protection of the server cluster will fail until a protection agent is installed on Node5. You install the protection agent on Node5.

You fail over the resources from Node4 to other nodes in the cluster. When no resources remain on Node4, you remove it from the cluster. DPM detects the failovers and continues protection of the cluster.

DPM detects that Node4 has left the cluster—it appears as a stand-alone node now. If it no longer exists on the network, you can remove the record for this server in DPM Administrator Console.

Changing Resource Groups on Clustered Exchange Servers

A cluster node can have any number of resource groups. Moving a protected data source to a resource group, between resource groups, or out of a resource group can cause protection job failures. To successfully make any of those changes to resource group membership, perform the following steps:

1. Stop existing protection of the data source. The data source could belong to a protection group as a single data source on a protected server or as a data source as a member of a resource group.
2. Begin protection of the data source according to its new status, either as a single data source on a protected server or as a data source as a member of a resource group. This will allocate a new replica for the data source.

Changing the name of a resource group will affect the protection of all data sources in the resource group. To change the name of a resource group, perform the following steps:

1. Stop protection of the resource group.
2. Change the name of the resource group.
3. Begin protection of the resource group under its new name.

Recovering Exchange Data

When you select a Microsoft Exchange database for recovery, you can select from the following recovery options:

- **Recover the database to its original location**.

  This option is available only if you select **Latest** as the recovery point.

  If you select this option, and the recovery destination contains files that have the same names as the files you are recovering, the current database files will be overwritten during recovery.

  For Exchange 2003 only: You must configure the target database to allow it to be overwritten by the recovered data. For instructions, see "How to Configure the Exchange Databases so That the Restore Process Overwrites Them".

- **Recover the database to another database on an Exchange 2007 server**.

  This option is available only for Exchange 2007.

  This option is not available if you select **Latest** as the recovery point. You must specify an existing database to which the selected database will be recovered. You must configure the target database to allow it to be overwritten by the recovered data. For instructions, see How to Configure the Exchange Databases so That the Restore Process Overwrites Them.

- **Recover to Recovery Storage Group**.

  This option is available only for Exchange 2007.

  This option is not available if you select **Latest** as the recovery point.

- **Copy the database to a network folder**.

  This option is not available if you select **Latest** as the recovery point. System Center 2012 – Data Protection Manager (DPM) creates the following directory structure at the destination that you specify:

  DPM_Recovery_Point_*timestamp***DPM_Recovered_At**_*timestamp**Server name**Exchange application**Database name**Files*

  To use the **Bring the database to a clean shutdown after copying the files option**, the DPM protection agent and the Eseutil utility must be installed on the destination server. The Eseutil utility can be installed as part of either an Exchange Server installation or an Exchange Server Administrator-only-mode installation.

- **Copy the database to tape**.

  This option is not available if you select **Latest** as the recovery point. This option copies the replica of the storage group that contains the selected database.

In This Section

How to Recover a Database to an Alternate Database
How to Copy Exchange Data to a Network Folder
How to Copy Exchange Data to Tape
Recovering Mailboxes
Recovering Data to Clustered Servers

How to Recover a Storage Group to its Original Location

When you recover a storage group to its original location, and the recovery destination contains files that have the same names as the files you are recovering, the current database files will be overwritten during recovery.

How to recover a storage group to its original location

1. On the server to which the storage group will be recovered, configure each database to allow it to be overwritten by the recovered data. For instructions, see How to Configure the Exchange Databases so That the Restore Process Overwrites Them.
2. In DPM Administrator Console, click **Recovery** on the navigation bar.
3. Using the browse functionality, select the storage group to recover.
4. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
5. On the **Recovery time** menu, select the recovery point you want to use.
6. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts. The wizard options vary depending on the version of Exchange.
7. On the **Review recovery selection** page, click **Next**.
8. Select **Recover to original Exchange Server location**, and then click **Next**.
9. On the **Specify recovery options** page, you can select **Send an e-mail when this recovery completes.**

   Select this option to specify an e-mail address or addresses to notify upon recovery completion. If you select this option, you must enter the e-mail address to notify. Multiple e-mail addresses must be separated by a comma.
10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover a Database to Its Original Location
How to Recover a Database to an Alternate Database

How to Copy Exchange Data to a Network Folder
How to Copy Exchange Data to Tape
Recovering Mailboxes
Recovering Data to Clustered Servers

How to Recover a Database to Its Original Location

When you recover a Microsoft Exchange Server 2003 database to the original location, System Center 2012 – Data Protection Manager (DPM) does not use the latest log files from the protected server; therefore, the recovery is to the last saved state. To perform a database recovery without losing data, recover the database to the original location using one of the following methods:

- If there are no databases mounted under the storage group, recover the storage group using the **Latest** recovery point.
- If any database is mounted under the storage group, create a recovery point for the storage group, and then recover the database using the **Latest** recovery point.

If you select **Latest** as the recovery point for an Exchange Server 2007 database, DPM applies the log files from the protected server and performs a lossless recovery without any additional steps.

Note
In Exchange 2007, if there are multiple databases in a storage group, all databases will be dismounted during recovery. An Exchange 2007 best practice is to have one database per storage group.

How to recover a database to its original location

1. On the server to which the database will be recovered, configure the target database to allow it to be overwritten by the recovered data. For instructions, see How to Configure the Exchange Databases so That the Restore Process Overwrites Them.
2. In DPM Administrator Console, click **Recovery** on the navigation bar.
3. Using the browse functionality, select the database to recover.
4. On the **Recovery time** menu, select **Latest**.

   You must select the most recent recovery point to recover the storage group to its original location.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts. The wizard options will vary depending on the version of Exchange.
6. On the **Review recovery selection** page, click **Next**.

7. Select **Recover to original Exchange Server location**, and then click **Next**.
8. On the **Specify recovery options** page, you can select **Send an e-mail when this recovery completes.**

   Select this option to specify an e-mail address or addresses to notify upon recovery completion. If you select this option, you must also enter the e-mail address to notify. Multiple e-mail addresses must be separated by a comma.
9. On the **Summary** page, review the recovery settings and then click **Recover**.

See Also

How to Recover a Storage Group to its Original Location

How to Recover a Database to an Alternate Database

How to Copy Exchange Data to a Network Folder

How to Copy Exchange Data to Tape

Recovering Mailboxes

Recovering Data to Clustered Servers

How to Recover a Database to an Alternate Database

Use the following procedure to recover a database to an alternate database.

How to recover a database to an alternate database

1. On the server to which the database will be recovered, configure the target database to allow it to be overwritten by the recovered data. For instructions, see How to Configure the Exchange Databases so That the Restore Process Overwrites Them.
2. In DPM Administrator Console, click **Recovery** on the navigation bar.
3. Using the browse functionality, select the database to recover.
4. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
5. On the **Recovery time** menu, select the recovery point you want to use.
6. In the **Actions** pane, click **Recover**.

   The Recovery Wizard launches. The wizard options will vary depending on the version of Exchange.
7. On the **Review recovery selection** page, click **Next**.
8. Select **Recover to another database on an Exchange Server**, and then click **Next**.
9. On the **Specify recovery options** page, you can select **Send an e-mail when this recovery completes**.

Select this option to specify an e-mail address or addresses to notify upon recovery completion. If you select this option, you must enter the e-mail address to notify. Multiple e-mail addresses must be separated by a comma.

10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover a Storage Group to its Original Location

How to Recover a Database to Its Original Location

How to Copy Exchange Data to a Network Folder

How to Copy Exchange Data to Tape

Recovering Mailboxes

Recovering Data to Clustered Servers

How to Copy Exchange Data to a Network Folder

When you copy a storage group to a network folder, System Center 2012 – Data Protection Manager (DPM) creates the following directory structure at the destination that you specify:

DPM_Recovery_Point_*timestamp***DPM_Recovered_At**_*timestamp**Server name**Exchange application**Database name**Files*

Example:

DPM_Recovery_Point_8-12-2007_0.1.54AM\DPM_Recovered_At_8-13-2007_10.49.21AM\Server1.DPM.LAB\J-Volume\Files

The DPM protection agent and the Eseutil utility must be installed on the destination server. The Eseutil utility can be installed as part of either a Microsoft Exchange Server installation or an Exchange Server Administrator-only-mode installation.

How to copy Exchange data to a network folder

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using the browse functionality, select the storage group or database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Time** menu lists the time for each available recovery point.
4. On the **Time** menu, select the recovery point you want to use. Do not select **Latest** for the recovery point.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts. The wizard options vary depending on the version of

Exchange.

6. On the **Review recovery selection** page, click **Next**.
7. Select **Copy to a network folder**, and then click **Next**.
8. Specify the destination path to which the storage group or database should be copied.
9. On the **Specify recovery options** page, you can select from the following options:
   - **Bring the database to a clean shutdown after copying the files**.

     This option is available if you are copying a database, and it brings the database files to a mountable condition by copying the logs. Select this option only if the destination is an Exchange-based server that has the same version of the Exchange application and the same or later version of Eseutil.exe as at the time of protection.
   - **Send an e-mail when this recovery completes.**

     Select this option to specify an e-mail address or addresses to notify upon recovery completion. If you select this option, you must enter the e-mail address to notify. Multiple e-mail addresses must be separated by a comma.
10. On the **Summary** page, review the recovery settings and then click **Recover**.

See Also

How to Recover a Storage Group to its Original Location

How to Recover a Database to Its Original Location

How to Recover a Database to an Alternate Database

How to Copy Exchange Data to Tape

Recovering Mailboxes

Recovering Data to Clustered Servers

How to Copy Exchange Data to Tape

Use the following procedure to copy Exchange data to tape.

How to copy Exchange data to tape

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using the browse functionality, select the storage group or database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Time** menu lists the time for each available recovery point.
4. On the **Time** menu, select the recovery point you want to use. Do not select **Latest** for the recovery point.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts. The wizard options vary depending on the version of

Exchange.

6. On the **Review recovery selection** page, click **Next**.
7. Select **Copy to tape**, and then click **Next**.
8. On the **Specify Library** page, in **Primary library**, select a library to use for recovery. (**Copy library** is available only when the job cannot be completed using only the tape library selected in **Primary library**.)
   - When the data is being copied from disk, the library you select in **Primary library** will copy the data to tape.
   - When the data is being copied from tape and the tape library has multiple tape drives, the library you select in **Primary library** will read from the source tape and copy the data to another tape.
   - When the data is being copied from tape and the tape library has only a single tape drive, the library you select in **Primary library** will read from the source tape and the library you select in **Copy library** will copy the data to tape.
9. Enter a label for the tape on which the storage group will be copied.
10. Specify if the data that is copied should be compressed.
11. On the **Specify recovery options** page, you can select **Send an e-mail when this recovery completes**.

    Select this option to specify an e-mail address or addresses to notify upon recovery completion. If you select this option, you must enter the e-mail address to notify. Multiple e-mail addresses must be separated by a comma.
12. On the **Summary** page, review the recovery settings, and then click **Recover**.

Additional Resources

How to Copy a Tape

See Also

How to Recover a Storage Group to its Original Location

How to Recover a Database to Its Original Location

How to Recover a Database to an Alternate Database

How to Copy Exchange Data to a Network Folder

Recovering Mailboxes

You can recover deleted e-mail messages using Microsoft Outlook. For instructions, see How to Recover a Deleted Item. To recover a deleted mailbox, use the Exchange Management Shell or the Exchange Management Console. For instructions, see How to Recover a Deleted Mailbox.

If you cannot recover the mailbox using the Exchange Management Shell or the Exchange Management Console, such as when the retention period is expired, you can use System Center 2012 – Data Protection Manager (DPM) to recover the mailbox.

To recover a mailbox, DPM must copy the entire database because this is the recommended method that Exchange supports, as explained in Knowledge Base article 904845, Microsoft support policy for third-party products that modify or extract Exchange database contents.

When you select a mailbox for recovery, you cannot select **Latest** as the recovery point. The **Latest** option recovers the data from the most recent recovery point, and then applies all committed transactions from the server logs. This functionality is not available for individual mailboxes.

Item details will not appear on the Recovery Wizard Summary page for Exchange Server mailboxes.

In This Section

How to Recover an Exchange 2003 Mailbox

The procedure for recovering a mailbox to Microsoft Exchange 2003 includes the use of Eseutil.exe and Exmerge.exe. For more information on the Exchange Server Database Utilities tool (Eseutil.exe), see Eseutil. For more information on Exmerge.exe, see Knowledge Base article 174197, "Microsoft Exchange Mailbox Merge program (Exmerge.exe) information".

Caution

System Center 2012 – Data Protection Manager (DPM) needs to restore the entire Exchange database before you can recover an individual mailbox. Please make sure you have sufficient space on the server to which you are restoring the database.

How to recover a previous version of an active Exchange 2003 mailbox

1. Use the **Search** tab and a date range to locate the mailbox you want to recover.
2. Select a recovery point for the database that contains the mailbox to be restored.
3. In the **Actions** pane, click **Recover**. The Recovery Wizard starts.
4. Review your recovery selection, and then click **Next**.
5. On the **Select Recovery Type** page, select **Copy to a network folder**.
6. On the **Specify Destination** page, enter a volume on an Exchange server that has a recovery storage group enabled.
7. On the **Select Recovery Options** page, select the **Bring the database to a clean shut down state after copying the files** check box.

8. Move the database file to the location of the Exchange recovery storage group database.
9. Mount the database under the recovery storage group. For more information, see Restoring Databases to a Recovery Storage Group in Exchange Server 2003.
10. Complete the Recovery Wizard.
11. Extract the mailbox from the recovered database.
    - For Exchange Server 2003, use the Microsoft Exchange Server Mailbox Merge Wizard (ExMerge).
    - For Exchange Server 2003 SP1, extract and merge data using Exchange 2003 System Manager.

How to recover a disabled or deleted Exchange 2003 mailbox

1. Use the **Search** tab and a date range to locate the mailbox you want to recover.
2. Select a recovery point for the database that contains the mailbox to be restored.
3. In the **Actions** pane, click **Recover**. The Recovery Wizard starts.
4. Review your recovery selection, and then click **Next**.
5. On the **Select Recovery Type** page, select **Recover mailbox to an Exchange server database**.
6. On the **Specify Destination** page, enter the full names of the Exchange server, including the domain, storage group, and database.

   The database should be dismounted and configured to allow it to be overwritten by the recovered data. For instructions, see How to Configure the Exchange Databases so That the Restore Process Overwrites Them.
7. Complete the Recovery Wizard. DPM recovers the database.
8. Extract the mailbox from the recovered database.
    - For Exchange Server 2003, use the Microsoft Exchange Server Mailbox Merge Wizard (ExMerge).
    - For Exchange Server 2003 SP1, extract and merge data using Exchange 2003 System Manager.

See Also

How to Copy Exchange Data to a Network Folder

Recovering Mailboxes

How to Recover an Exchange 2007 Mailbox

How to Recover an Exchange 2007 Mailbox

To recover a Microsoft Exchange 2007 mailbox, the recovered .edb and .log files need to be attached to the Recovery Storage Group in Exchange and you must use Exchange-supported tools, such as Exmerge.exe, to extract a .pst file.

The procedure you use depends on whether there is an existing mailbox to which you want to recover a previous version or the mailbox no longer exists and you want to recover it.

Caution

System Center 2012 – Data Protection Manager (DPM) needs to restore the entire Exchange database before you can recover an individual mailbox. Please make sure you have sufficient space on the server to which you are restoring the database.

How to recover an Exchange 2007 mailbox for an existing mailbox

1. If you do not have an existing Recovery Storage Group, create one by using the new-storagegroup cmdlet in Exchange Management Shell.
2. Create a recovery database in the Recovery Storage Group by using the new-mailboxdatabase cmdlet in Exchange Management Shell.
3. Configure the recovery database to allow it to be overwritten by using the set-mailboxdatabase cmdlet in Exchange Management Shell.
4. In DPM Administrator Console, click the **Search** tab and select a date range to locate the mailbox you want to recover.
5. Select a recovery point that contains the mailbox to be restored, and then click **Recover**.

   DPM recovers the database that contains the selected mailbox.
6. On the **Review Recovery Selection** page, click **Next**.
7. On the **Select Recovery Type** page, select **Recover mailbox to an Exchange server database**.
8. On the **Specify Destination** page, enter the full names of the Exchange server, including the domain, the name of the Recovery Storage Group that you created in step 1, and the name of the recovery database that you created in step 2.
9. Complete the Recovery Wizard. DPM recovers the database.
10. Configure the destination database to allow it to be overwritten by using the set-mailboxdatabase cmdlet in Exchange Management Shell.
11. Merge the mailbox data in the recovery database to the production mailbox database, using the restore-mailbox cmdlet in Exchange Management Shell.

Example

You need to retrieve some items from a mailbox for an employee who has left the organization. The following is the identification of the mailbox:

- Exchange Server: exchangeserver1

- Storage group: SG1
- Database: DB11
- Mailbox: John

Storage group SG1 is protected by DPM. You decide to recover the mailbox John to the manager's mailbox so that he can retrieve the necessary items. The following is the identification of the manager's mailbox:

- Exchange Server: exchangeserver1
- Storage group: SG2
- Database: DB21
- Mailbox: Simon

To recover the mailbox John to the mailbox Simon, you perform the following steps:

1. Create a Recovery Storage Group (RSG) by running the following Exchange Management Shell cmdlet:

   new-storagegroup -Server exchangeserver1 -LogFolderPath C:\RSG\ -Name RSG -SystemFolderPath C:\RSG\ -Recovery

   This creates a storage group named RSG on exchangeserver1.
2. Add a recovery database to the RSG by running the following Exchange Management Shell cmdlet:

   new-mailboxdatabase -mailboxdatabasetorecover exchangeserver1\SG1\DB11 -storagegroup exchangeserver1\RSG -edbfilepath C:\RSG\DB11.edb

   This creates a mailbox on exchangeserver1\RSG\DB11. The .edb file name must be the same as the .edb file name for the mailbox you are recovering.
3. Set the recovery database to allow overwrites by running the following Exchange Management Shell cmdlet:

   set-mailboxdatabase -identity exchangeserver1\RSG\DB11 -AllowFileRestore 1
4. Open DPM Administrator Console and click **Recovery** on the navigation bar.
5. Expand the tree and select SG1.
6. Double-click database DB11.
7. Select **John**, and click **Recover**.
8. In the Recovery Wizard, on the **Review Recovery Selection** page, click **Next**.
9. On the **Select Recovery Type** page, select **Recover mailbox to an Exchange server database**.
10. On the **Specify Destination** page, enter the following information:
    - For Exchange server: exchangeserver1
    - For storage group: RSG
    - For database: DB11
11. Specify your recovery options, and then click **Recover**.
12. Set the destination database to allow overwrites by running the following Exchange Management Shell cmdlet:

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

The destination database is the database that contains the mailbox to which we want to recover the e-mail from the John mailbox.

13. When the recovery is complete, run the following Exchange Management Shell cmdlet:

    Restore-Mailbox -RSGMailbox 'John' -RSGDatabase 'RSG\DB11' -id 'Simon' -TargetFolder 'John E-mail'

    The manager opens his mailbox and finds a new folder named John E-mail, which contains the e-mail items from the recovered mailbox.

See Also

Recovering Mailboxes

How to Recover an Exchange 2003 Mailbox

Recovering Data to Clustered Servers

Stand-alone and Shared Disk Cluster Recovery

To recover the storage group or database to the latest point in time

1. Set the Exchange server database property **Override by restore** to **True**.
2. On the DPM server, recover the storage group or database, selecting the **Restore to original location** option.

To recover the storage group to a previous point in time

1. Delete the existing log files and checkpoint files on the Exchange server.
2. Set the Exchange server database property **Override by restore** to **True**.
3. On the DPM server, recover the storage group or database, selecting the **Restore to original location** option.

To recover a storage group or database in clean shutdown state to a network share, you cannot select **Latest** as the recovery point.

To recover the storage group or database in clean shutdown state to a network share

1. On the DPM server, recover the storage group or database, selecting the **Copy to a network folder** option.
2. On the **Specify Destination** page, specify a folder on a server running Exchange 2007 server.
3. On the **Specify Recovery Options** page, select the **Bring the database to a clean**

shutdown state after copying the files option.

4. On the **Summary** page, click **Recover**.

Cluster Continuous Replication and Local Continuous Replication Recovery

System Center 2012 – Data Protection Manager (DPM) will always recover to the active node, regardless of protection topology.

To recover from failure on the active node

1. Set the Exchange Server database property **Override by restore** to **True**.
2. On the DPM server, recover the storage group or database, selecting the **Restore to original location** option.
3. On the Exchange server, in Exchange Management Shell, run **get-storagegroupcopystatus** to verify the copy status.

   After recovery, you should synchronize the passive nodes with the active node.

If the database or logs on the passive node are corrupt, use either of the following procedures to recover data.

To recover from failure on the passive node

1. On the Exchange server, in Exchange Management Shell, run **suspend-storagegroupcopy** for the failed storage group.
2. Delete all .logs, .chk, and .edb files from the copy location (passive node).
3. In the DPM Recovery Wizard, copy the database files without running database clean shutdown to the passive node.
4. Move the files to appropriate locations in the passive node.
5. Remove the common log files (between active and passive nodes) from the passive node. For example, a failover might have created a new log stream with the same log file names.
6. On the Exchange server, in Exchange Management Shell, run **resume-storagegroupcopy** for the failed storage group.

To recover from failure on the passive node (if both copies are corrupt)

1. Set the Exchange Server database property **Override by restore** to **True**.
2. In the DPM Recovery Wizard, recover to the active node.
3. On the Exchange server, in Exchange Management Shell, run **get-storagegroupcopystatus** to verify the copy status.
4. After recovery, synchronize the passive nodes with the active node.

See Also

Managing Clustered Exchange Servers

Recovering Exchange Data

Managing Exchange SCR Servers

System Center 2012 – Data Protection Manager (DPM) provides support for backup and recovery of Microsoft Exchange Server while supporting backup and recovery of the SCR server. For more information, see Exchange Server 2007 - Standby Continuous Replication.

In the current scenario, an onsite DPM server protects the Exchange server or cluster. The DPM server is protected by an offsite DPM server for disaster recovery. The Exchange server also replicates its logs and databases to the SCR server at a remote location. By using this deployment, you make sure that you have disaster recovery options both onsite and offsite. However, this also means that both Exchange and DPM are sending data across the network.

In the new scenario, instead of having both DPM and Exchange send data over the network, you use each DPM server to protect the local Exchange servers. The onsite DPM protects the onsite Exchange server (SCR source); the offsite DPM protects the SCR server (SCR target). This deployment lets you continue having a disaster recovery scenario both onsite and offsite without the cost of both applications transporting data over the network.

Depending on business requirements, you can choose to protect either both the SCR source and the SCR target server or just one of them.

Note

- Incremental backups are not enabled for all Exchange data sources on an SCR target.
- SCR protection requires a dedicated protection group.
- DPM does not support configurations where a stand-alone Exchange server uses a clustered SCR or vice versa.

Important

If SCR protection was enabled at the time of backup, make sure that it is also enabled at the time of recovery.

Supported Scenarios

- Both SCR source and target servers are Exchange Server 2007 in standalone mode.
- Both SCR source and target servers are Exchange Server 2007 in SCC mode.
- Both CCR source and target servers are Exchange Server 2007 in CCR mode.

In This Section

Protecting an Exchange Server 2007 SCR Target Server Configured as Single Node Cluster

All scripts that are used in the procedure can be found under the <DPM Installation folder>\Bin folder of the computer on which the action is being performed. For example, if the script has to be run on the SCR server, the script is in .\Program Files\Microsoft Data Protection Manager\DPM\Bin. On the DPM server, the script is in .\Program Files\Microsoft DPM\DPM\Bin. DPM scripts must be run in the DPM Management Shell.

Scripts on the SCR server must be run in the Exchange Management Shell.

Important
If you are using a Single Copy Cluster (SCC) server as your SCR source, you must set the registry key EnableSccForScr of type DWORD under HKLM\Software\Microsoft\Microsoft Data Protection Manager\Agent\2.0 to 1 before proceeding with the following procedure on SCR target server.

Procedure to enable protection for an SCR server

1. Create a resource group with same name as the resource group on SCR target cluster. This is required by the DPM naming convention for clusters. Create an IP address resource under this resource group and bring it online.
2. Enable SCR protection on the DPM server by using the Enable-ExchangeSCRProtection script.
   You only have to enable SCR protection one time for an SCR server.
   Syntax: **Enable-ExchangeSCRProtection.ps1 <DPM Server Name> <Resource Group>.<Cluster FQDN>**

   Where Cluster FQDN for the cluster must be provided in the format <Cluster Name>.<Domain>.
   Example: **Enable-ExchangeSCRProtection.ps1 DPMTest**

ExchangeSCRCluster.DRCLUSTER.contoso.com

Note
You can check if Exchange SCR protection has been enabled by running get-ExchangeSCRProtection.ps1.

The value for <Cluster FQDN> must be provided in the following format - <Cluster Name>.<Domain Name>.

3. Run the Add-SCRSG script from the SCR target server.
   Syntax: **add-SCRSG.ps1 <SCRSourceFQDN> <Storage Group Name> <Size of Storage Group in MB> <SCRTargetFQDN> <is cluster>**
   Where target FQDN for the cluster must be provided in the format <Resource Group Name>.<Cluster Name>.<Domain>.
   Example: **add-SCRSG.ps1 ExchangeCluster.DRCluster.contoso.com testSG 1024 ExchangeSCRCluster.contoso.com $true**

   Note
   In case of clusters, the source FQDN must be entered as <Resource Group Name>.<Domain>.

4. On the DPM server, start the Create New Protection Group wizard.

   Note
   On the Specify Short-Term Goals page of the Create New Protection Group wizard, you can only select **Express full backups for SCR protection**.

   Important
   After activating the SCR server as the primary Exchange server, you must run Remove-SCRSG.ps1 on the SCR server to enable DPM protection. After fallback, you must run Add-SCRSG.ps1 on the SCR server to enable DPM protection.

Protecting an Exchange Server 2007 SCR Server in Standalone Mode

All scripts used in the procedure can be found under the <DPM Installation folder>\Bin folder of the computer on which the action is being performed. For instance, if the script has to be run on the SCR server, the script is in .\Program Files\Microsoft Data Protection Manager\DPM\Bin. On the DPM server, the script is in .\Program Files\Microsoft DPM\DPM\Bin.
Scripts on the SCR server must be run in the Exchange Management Shell.

DPM scripts must be run in the DPM Management Shell.

Procedure to enable protection for an SCR server

1. Enable SCR protection on the DPM server using the Enable-ExchangeSCRProtection script. You only have to enable SCR protection one time for a SCR server.
   Syntax: **Enable-ExchangeSCRProtection.ps1 <DPMServerName> <SCRTargetFQDN>**
   Example: **Enable-ExchangeSCRProtection.ps1 DPMTest ExchangeSCR.contoso.com**

   Note
   You can check if Exchange SCR protection has been enabled by running get-ExchangeSCRProtection.ps1.
2. Create a storage group and database, with .log, .sys and .ebd files, with the same name as the source at some temporary location on the SCR server.

   Caution
   Ensure that the log file path does not point to the location where the log files for the SCR source exist. This can lead to the replication service failing.
3. Add the SCR server to the protection group using the Add-SCRSG script from the Exchange Management Shell.
   Syntax: **add-SCRSG.ps1 <SCRSourceFQDN> <SGName> <Size of storage group in MB> <SCRTargetFQDN> <is cluster> <cluster name>**
   Example: **add-SCRSG.ps1 ExchangeServer.contoso.com testSG 1024 ExchangeCluster.contoso.com $false**

   Important
   If the SCR server has been activated (if it is now the primary Exchange server), you do not need to run this script as the Exchange writer will provide this information to DPM.
4. Follow the wizard to create a new protection group on the DPM server.

Modifying Protection For an Exchange Server 2007 SCR

The procedure of modifying protection is similar to the procedure to modify protection for an Exchange server.

Note
On the Specify Short-Term Goals page of the Modify Group wizard, you can only select express full backups for SCR protection.

Recovering an Exchange Server 2007 SCR Server

The procedure to recover an Exchange Server 2007 SCR is similar to the procedure to recover an Exchange server.

Note

- On the **Recovery** tab in DPM Administrator Console, you cannot expand the SCR server to display individual items.
- You can only recover the SCR server to a network share.

Stopping Protection for an Exchange Server 2007 SCR Server

All scripts used in the procedure are under the <DPM Installation folder>\Bin folder of the computer on which the action is being performed. For example, if the script has to run on the SCR server, the script is in .\Program Files\Microsoft Data Protection Manager\DPM\Bin. On the DPM server, the script is in .\Program Files\Microsoft DPM\DPM\Bin.

Scripts on the SCR server run in the Exchange Management Shell.

Stopping protection for an SCR server

1. Stop protection for the computer through DPM Administrator Console.
2. Remove the SCR server from the protection group using Remove-SCRSG.ps1 on the SCR server in the Exchange Management Shell.
   Syntax: **remove-SCRSG.ps1 [SCRSourceFQDN] [StorageGroupName]**
   Example: **remove-SCRSG.ps1 ExchangeSCRCluster.contoso.com testSG**

Disabling Protection for an Exchange Server 2007 SCR Server

By disabling Exchange SCR protection on a server, all data sources using SCR protection on that DPM server are affected.
You can disable protection for the SCR server using Disable-ExchangeSCRProtection.ps1 on the DPM server.

Note

All scripts used in the procedure can be found under the <DPM Installation folder>\Bin folder of the computer on which the action is being performed. For example, if the script has to be run on the SCR server, the script is in .\Program Files\Microsoft Data Protection Manager\DPM\Bin. On the DPM server, the script is in .\Program Files\Microsoft DPM\DPM\Bin.

Scripts on the SCR server must be run in the Exchange Management Shell.

Syntax **(standalone server)**: **Disable-ExchangeSCRProtection.ps1 <DPMServerName> <ScrPSFQDN>**
Example: **Disable-ExchangeSCRProtection.ps1 DPMTest ExchangeSCR.contoso.com**
Syntax **(clustered server)**: **Disable-ExchangeSCRProtection.ps1 <DPMServerName> <ResourceGroup>.<ClusterFQDN>**
Example: **Disable-ExchangeSCRProtection.ps1 DPMTest ExchangeSCRCluster.DRCLUSTER.contoso.com**

Protecting an Exchange Server 2007 SCR Server Post-Activation

Activation of an SCR target is done in case of a major disaster that results in no easier options to recover the Exchange server. When such a disaster happens, you have to remove protection for the SCR server to allow DPM to protect it as the primary Exchange server.
Use Remove-SCRSG.ps1 on the SCR server to remove it from the protection group.

Important

After you activate the SCR server as the primary Exchange server, a new SCR server has to be put in place to continue SCR protection. You must specifically enable protection for the new SCR target.

Protecting SQL Servers

In This Section

Performing SQL Server Management Tasks

This section provides instructions and guidelines for managing a protected SQL Server and making changes after the initial configuration of Data Protection Manager.

In This Section

Upgrading SQL Server 2000 to SQL Server 2005

If you upgrade a protected server running SQL Server 2000 to SQL Server 2005, you must reprotect the databases after the upgrade by performing the following steps:

1. Stop protection of the databases, choosing the retain data option.
2. Start the SQL Writer Service on the upgraded server.
3. Add the databases on the upgraded server to a new protection group.

You will be able to use the retained replica to recover data from points in time before the upgrade. Data created by SQL Server 2000 must be restored to a computer running SQL Server 2000.

You can also use the retained replica to manually create the initial replica for each database in the new protection group.

Note

After you reconfigure protection, DPM Administrator Console displays the protected database as two separate nodes. The protection status in the Protection task area appears as **Inactive replica** for one of the database nodes, and the Recovery task area displays two database nodes with the same name.

Moving SQL Servers Between Domains

You cannot do the following for protected computers:

- Change the domain of a protected computer and continue protection without disruption.
- Change the domain of a protected computer and associate the existing replicas and recovery points with the computer when it is re-protected.

We recommend that you do not change the domain of a protected computer. If you must change the domain of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection while the computer retains its original domain membership.
- Protect the data source on the computer after it becomes a member of another domain.

To change the domain membership of a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the domain membership of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

   For information about performing tasks involving protection agents and protection groups, see DPM Help.

How to Rename a Computer Running SQL Server

System Center 2012 – Data Protection Manager (DPM) uses the computer name as a unique identifier for replicas, recovery points, DPM database entries, reporting database entries, and so on.

You cannot do the following:

- Change the name of a protected computer and continue protection without disruption.
- Change the name of a protected computer and associate the existing replicas and recovery points with the new computer name.

We recommend that you do not change the name of a protected computer. If you must change the name of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection (the old computer name).

- Protect the data source on the computer (the new computer name).

To rename a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the name of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

   For information about tasks that involve protection agents and protection groups, see DPM Help.

Changing the Recovery Model of a Database

SQL Server databases can have one of three types of recovery models: simple, full, or bulk-logged. By default, new databases are usually created in the full recovery model. The following table describes how each model uses log backups.

SQL Server Database Recovery Models

Recovery model	Use of log backups
Simple	Does not use log backups.
Full	SQL Server maintains the transactions logs for the databases, allowing log backups to be taken. The logs must be truncated explicitly; otherwise, they continue to grow.
Bulk-logged	Similar to the full recovery model except that certain types of transactions are not logged in the transaction log.

When a database is added to a protection group, System Center 2012 –
Data Protection Manager (DPM) detects the recovery model that the database is configured to use. DPM does not allow log, or incremental, backups for databases configured in the simple recovery model. Log backups are only allowed for databases configured in the full and bulk-logged recovery models.

When the recovery model of a protected database is changed from simple to full or bulk-logged, DPM protection continues as configured. When the recovery model of a protected database is changed from full or bulk-logged to simple, express full backups will continue to succeed, but incremental backups will fail.

To change the recovery model of a protected database to the simple recovery model

1. Stop protection of the database, selecting the retain replica option.
2. Change the recovery model on the SQL Server database.
3. Add the database to a protection group.

You should also stop protection of a database before you configure log shipping for the database or change the database to Read Only. After you make the changes to the database, you can reconfigure protection for the database.

When protecting SQL Server databases that are configured to use the full or bulk-logged recovery models, DPM creates a folder on the SQL Server that is being protected. This folder is created in the same location as the first log file (*.ldf) of each protected database.

This folder is used as a temporary store for logs during SQL Server log backup and SQL Server log restore by DPM. If DPM finds the folder missing, DPM will re-create the folder.

Replacing a Disk on a SQL Server

You might replace a disk on a SQL Server to upgrade capacity or to replace a failed disk. If you replace a disk that contains SQL Server data protected by System Center 2012 – Data Protection Manager (DPM), you should assign the same drive letter to the new disk. You can then recover the protected data from the DPM server to the new disk.

Adding Databases to a SQL Server

System Center 2012 – Data Protection Manager (DPM) allows you to protect SQL Server databases through SQL Server instance auto-protection. This enables DPM to automatically identify and protect SQL Server databases that are added to instances of SQL Server to be automatically protected.

Enabling SQL Server Instance Auto-Protection

SQL Server instance auto-protection is turned on by default for any instance of SQL Server that you protect. When you add an instance of SQL Server to a protection group, auto-protection is automatically enabled on the instance.

You can use the cmdlet Start-AutoProtection to force DPM to immediately check for new databases and add them to protection if you cannot wait for the nightly job.

Disabling SQL Server Instance Auto-Protection

To disable auto-protection for SQL Server instance, right-click the instance on the Create Protection Wizard or on the Modify Protection Wizard, and then select **Turn off auto-protection**. When you turn off auto-protection for an instance of SQL Server, DPM will not discover any new databases created on that instance. To protect any new databases, you must manually add them to the protection group.

Changing the Path of a SQL Server Database

When a path associated with a protected database changes, backup jobs will fail. To resolve this issue, remove the database from protection and then add the database back to the protection group. This change to the protection group will require a consistency check. After the consistency check completes successfully, normal protection jobs will resume.

Renaming a SQL Server Database

If you rename a database that is protected by System Center 2012 – Data Protection Manager (DPM), you must add the database under its new name to an existing or new protection group and then remove the database under its old name from its protection group. The database will be protected as a new data source.

Running Parallel Backups

System Center 2012 – Data Protection Manager (DPM) supports running parallel backups of data sources in the same protection group to optimize your network usage. However, there are restrictions to performing parallel backups for SQL Server databases from the same protected computer because of restrictions in SQL Server.

Supported Scenarios

The following is a list of scenarios in which you can perform parallel backups of a SQL data source.

- The databases are on Microsoft SQL Server 2008.

  Note
  Both the databases must be on different protection groups.
- Both the databases are on different versions of SQL Server. For example, one is on Microsoft SQL Server 2000 and the other on Microsoft SQL Server 2005.

Unsupported Scenarios

Neither Microsoft SQL Server 2000 nor Microsoft SQL Server 2005 support parallel backups. If two databases from the same version and instance of SQL Server are scheduled for backup at the same time, the backup will happen serially.

Managing Clustered SQL Servers

On planned failover of a cluster, System Center 2012 – Data Protection Manager (DPM) continues protection. On unplanned failover, DPM issues an alert that a consistency check is required.

For a non-shared disk cluster, planned failover may also require a consistency check.

You cannot backup and recover the master database for clustered SQL Servers.

In This Section

Changing SQL Server Cluster Members

When you make changes to a server cluster that is protected by System Center 2012 – Data Protection Manager (DPM), DPM takes the following actions:

- When a new server is added to a cluster, DPM issues an alert to install a protection agent on the new cluster node and protection fails.
- When a server is removed from a cluster, DPM detects that a node has left the cluster and the server now appears separate from the cluster with no data protected on it.

For example, assume you have a server cluster that contains four computers: Node1, Node2, Node3, and Node4. You need to replace computer Node4 with a new computer named Node5.

You use the administration console for your cluster service to add Node5 to the cluster and configure the resources that can be failed over to Node5.

DPM issues an alert that protection of the server cluster will fail until a protection agent is installed on Node5. You install the protection agent on Node5.

You fail over the resources from Node4 to other nodes in the cluster. When no resources remain on Node4, you remove it from the cluster. DPM detects the failovers and continues protection of the cluster.

DPM detects that Node4 has left the cluster – it appears as a stand-alone node now. If it no longer exists on the network, you can remove the record for this server in DPM Administrator Console.

Changing Resource Groups on Clustered SQL Servers

A cluster node can have any number of resource groups. Moving a protected data source to a resource group, between resource groups, or out of a resource group can cause protection job failures. To successfully make any of those changes to resource group membership, perform the following steps:

1. Stop existing protection of the data source. The data source could belong to a protection group as a single data source on a protected server or as a data source as a member of a resource group.
2. Begin protection of the data source according to its new status, either as a single data source on a protected server or as a data source as a member of a resource group. This will allocate a new replica for the data source.

Changing the name of a resource group will affect the protection of all data sources in the resource group. To change the name of a resource group, perform the following steps:

1. Stop protection of the resource group.
2. Change the name of the resource group.
3. Begin protection of the resource group under its new name.

Managing Mirrored SQL Servers

System Center 2012 – Data Protection Manager (DPM) protects SQL Server databases and clusters that use SQL Server mirroring technology. This support does not translate into any major changes in the procedure to protect or recover SQL Server databases in DPM. The following sections will call out any changes in procedure.

Prerequisites to protect mirrored databases

Before you protect a mirrored SQL Server database, make sure that you meet the following prerequisites:

- Install agents on both partners of the mirror.
- Do not mirror the database on the same computer.

Protect a mirrored SQL Server database

The procedure to protect a mirrored database is the same as to protect a SQL Server database. When you select a mirrored database to add to the protection group in the **Create New Protection Group** wizard, DPM automatically detects that the database is mirrored and displays the mirror details on the **Select Group Members** page.

Protect a mirrored SQL Server cluster

DPM also supports protection of mirrored SQL Server clusters. The procedure to protect SQL Server clusters that are mirrored is the same as to protect a mirrored SQL Server database.

Note
DPM agents must be installed on all the computers in the cluster.

DPM protects all the following configurations:

- Principal is clustered, mirror is not.
- Principal is not clustered, mirror is.
- Both principal and mirror are clustered.

Common scenarios

A protected SQL Server database gets mirrored

At the time of backup, DPM will detect that the database was mirrored and will raise an alert. You will need to remove protection (with retain data) for the database, and then reprotect it.

Note
DPM will maintain a single replica for the mirror.

A mirror is broken

When the mirror is broken for a mirrored SQL Server database that is currently protected by DPM, backups will fail with alerts. Remove protection (with retain data) for the SQL Server database and reprotect it.

Principal partner in a mirror fails over and fails back before the next backup

This scenario does not affect protection, because DPM is not informed about the fail over, unless a backup of the mirror is in progress.

Principal partner fails and the mirror server takes over

When DPM detects that the mirror is the principal partner, it stops the back-up job, and it performs a consistency check on the database that failed over after 30 minutes.

Note
If during these 30 minutes the database fails back to the original principal, DPM will detect this, and it will resume protection after performing a consistency check.

If you try to back up the mirrored database before the scheduled consistency check (after 30 minutes), an alert that indicates that a consistency check is required will be created on the DPM Monitor tab, and the back-up will not start until a consistency check is done. To start the backup immediately, do a consistency check and retry the backup.

One protected database is made the mirror of another protected database

If one SQL Server database that is protected by DPM is made the mirror of another protected database, protection will fail for both partners of the mirror. To continue protection, you must protect the principal partner.

Recover a mirrored SQL Server database

When you recover a mirrored SQL Server database, always use the **Recover to alternate location** option. Even if you want to recover the database to the original location, use the alternate location option and provide the path to either of the partners of the mirror.

Unsupported scenarios

DPM does not support the following scenarios for mirrored SQL Server databases:

- If the database is mirrored on the same server.
- If the SQL Server mirroring session uses an explicitly configured IP address.
- If the AlwaysOn feature in SQL Server 2012 is turned on.

Protecting SQL Server Data

This topic provides important information that you should consider when you plan to protect SQL Server data with System Center 2012 – Data Protection Manager (DPM).

Protect data in file shares

If you have a database with files on a remote file share, protection will fail with Error ID 104. DPM does not support protection for SQL Server data on a remote file share.

Protect SQL Server 2012

Consider the following scenarios that are specific to SQL Server 2012 protection.

Things to remember

- You must explicitly add the system account NTAuthority\System to the Sysadmin group on SQL Server.

- DPM cannot protect databases that are stored on remote SMB shares.
- Ensure that the availability group replicas are configured as read-only.
- When you protect databases that use the AlwaysOn feature, DPM has the following limitations:
    - DPM will honor the backup policy for availability groups that is set in SQL Server based on the backup preferences, as follows:
        - Prefer secondary—Backups should occur on a secondary replica except when the primary replica is the only replica online. If there are multiple secondary replicas available then the node with the highest backup priority will be selected for backup. In the case that only primary replica is available then backup should occur on the primary replica.
        - Secondary only—Backup shouldn't be performed on the primary replica. If the primary replica is the only one online, the backup shouldn't occur.
        - Primary—Backups should always occur on the primary replica.
        - Any Replica—Backups can happen on any of the availability replicas in the availability group. The node to be backed up from will be based on the backup priorities for each of the nodes.

      Note the following:
        - Backups can happen from any readable replica i.e. primary, synchronous secondary, asynchronous secondary.
        - If any replica is excluded from backup, for example Exclude Replica is enabled or is marked as not readable, then that replica will not be selected for backup under any of the options.
        - If multiple replicas are available and readable then the node with the highest backup priority will be selected for backup.
        - If the backup fails on the selected node then the backup operation fails.
        - Recovery to the original location is not supported.
- When you perform an alternate location recovery for a partially contained database, you must ensure that the target SQL instance has the Contained Databases feature enabled.

Protect SQL Server with the AlwaysOn feature enabled

SQL Server 2012 introduces a new high availability feature, named AlwaysOn. You can add your databases to Availability Groups, which are basically containers for databases that are configured for failover. System Center 2012 SP1 DPM supports protection of databases that are part of Availability Groups. The salient features of the DPM support for the AlwaysOn feature are:

- DPM detects Availability Groups when running inquiry at protection group creation.
- DPM detects a failover and continues protection of the database.
- DPM supports multi-site cluster configurations for an instance of SQL Server.

Protect an Availability Group

The **New Protection Group** wizard allows you to create protection groups that contain Availability Groups. DPM shows the Availability Groups under Cluster Group.

To protect the whole group, select the group name. This way, any databases that you added to the group are automatically protected.

To protect the selected databases in a group, expand the group name and select the individual databases that you want to protect.

Recovering SQL Server Data

When you recover SQL Server data, you can choose from the following options:

- Recover the database to its original location
- Recover the database with a new name to its original location or to a different instance of SQL Server
- Recover the database to a different instance of SQL Server
- Copy the database to a network folder
- Copy the database to tape

When you recover a SQL Server 2000 database to a different instance of SQL Server, the recovery path on the new server must be the same as the path of the database when it was protected on the source server. For example, DB1 on D:\sample on server1 can be recovered only to D:\sample on server2. If you want to recover to a completely new path, then you will only be able to recover express full backups (typically one copy per day).

When you recover a SQL Server 2005 database to a different instance of SQL Server, you can recover the database to any chosen path on the new server. You can back up once every 15 minutes and recover to any point in time on the target SQL Server.

In both SQL Server 2000 and SQL Server 2005, you can rename the database and recover to the original SQL instance.

You cannot recover a database from an instance of SQL Server on a computer running Windows Server 2008 to an instance of SQL Server on a computer running Windows Server 2003.

You cannot recover a system database to a different instance of SQL Server.

In This Section

How to Recover a SQL Database to Its Original Location

To recover a database to its original location

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using the browse functionality, select the database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Recover to original SQL Server location**, and then click **Next**.
8. If you selected a recovery point other than **Latest**, on the **Specify Database State** page, select **Leave database operational**.
9. Specify recovery options for network bandwidth usage throttling, SAN-based recovery, and e-mail notifications, and then click **Next**.
10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover and Rename a SQL Database

How to Recover a Database to a Different Instance of SQL Server

How to Copy a SQL Database to a Network Folder

How to Copy a SQL Database to Tape

How to Recover a SQL Database and Allow Additional Log Backups

How to Recover and Rename a SQL Database

To recover and rename a database, use the **Recover to any SQL instance** option. This option is unavailable if you select **Latest** as the recovery point from which to recover the database.

To recover and rename a database

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using either the browse or search functionality, select the database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use. Do not select **Latest** for the recovery point.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard launches.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Recover to any SQL instance**, and then click **Next**.
8. On the **Specify recovery destination** page, enter the path to recover the database to, and specify a new name for the recovered database.
9. Specify recovery options for network bandwidth usage throttling, SAN-based recovery, and e-mail notifications, and then click **Next**.
10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover a SQL Database to Its Original Location

How to Recover a Database to a Different Instance of SQL Server

How to Copy a SQL Database to a Network Folder

How to Copy a SQL Database to Tape

How to Recover a SQL Database and Allow Additional Log Backups

How to Recover a Database to a Different Instance of SQL Server

To recover a database to a different instance of SQL Server, you use the **Recover to any SQL instance** option. This option is unavailable if you select **Latest** as the recovery point from which to recover the database.

Note

When recovering a databases to a different instance of SQL Server

- You cannot recover a database from an instance of SQL Server on a computer running Windows Server 2008 to an instance of SQL Server on a computer running Windows Server 2003.
- You cannot recover a SQL Server 2008 database to a SQL Server 2005 instance.

To recover a database to a different instance of SQL Server

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using either the browse or search functionality, select the database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use. Do not select **Latest** for the recovery point.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Recover to any SQL instance**, and then click **Next**.
8. On the **Specify recovery destination** page, the actions you can take depend on the version of SQL Server database:
   - If you are recovering a database created by SQL Server 2000, specify the alternate instance of SQL Server to which the database should be recovered. The database must use the same complete path that it used in its original location.
   - If you are recovering a database created by SQL Server 2005, specify the alternate instance of SQL Server to which the database should be recovered. You can also specify a path for the database that differs from the path that it used in its original location.
9. Specify recovery options for network bandwidth usage throttling, SAN-based recovery, and e-mail notifications, and then click **Next**.
10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover a SQL Database to Its Original Location

How to Recover and Rename a SQL Database

How to Copy a SQL Database to a Network Folder

How to Copy a SQL Database to Tape

How to Recover a SQL Database and Allow Additional Log Backups

How to Copy a SQL Database to a Network Folder

You can only copy a SQL Server database from a recovery point that was created from an express full backup.

To copy a database to a network folder

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using the browse functionality, select the database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Copy to a network folder**, and then click **Next**.

   If the recovery point that you selected was not created from an express full backup, you will be presented with new recovery point choices.
8. Specify the destination path to which the database should be copied.
9. On the **Specify recovery options** page, you can select either or both of the following options:
   - **Restore security**

     Specify whether to use the security settings of the data being recovered or the security settings of the target destination.
   - **Send an e-mail when this recovery completes.**

     Select this option to specify an e-mail address or addresses to notify upon recovery completion. If you select this option, you must enter the e-mail address to notify. Multiple e-mail addresses must be separated by a comma.
10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover a SQL Database to Its Original Location

How to Recover and Rename a SQL Database

How to Recover a Database to a Different Instance of SQL Server

How to Copy a SQL Database to Tape

How to Recover a SQL Database and Allow Additional Log Backups

How to Copy a SQL Database to Tape

You can copy a SQL Server database to tape only from a recovery point that was created from an express full backup.

To copy a database to tape

1. In DPM Administrator Console, click **Recovery** on the navigation bar.

2. Using either the browse or search functionality, select the database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use.

   You must select the most recent recovery point to recover the storage group to its original location.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Copy to tape**, and then click **Next**.

   If the recovery point that you selected was not created from an express full backup, you will be presented with new recovery point choices.
8. On the **Specify Library** page, in **Primary library**, select a library to use for recovery. (**Copy library** is available only when the job cannot be completed using only the tape library selected in **Primary library**.)
   - When the data is being copied from disk, the library you select in **Primary library** will copy the data to tape.
   - When the data is being copied from tape and the tape library has multiple tape drives, the library you select in **Primary library** will read from the source tape and copy the data to another tape.
   - When the data is being copied from tape and the tape library has only a single tape drive, the library you select in **Primary library** will read from the source tape and the library you select in **Copy library** will copy the data to tape.
9. Enter a label for the tape on which the storage group will be copied.
10. Specify if the data that is copied should be compressed or encrypted.
11. On the **Set notification** page, you can select **Send an e-mail when this recovery completes.**
12. On the **Summary** page, review the recovery settings, and then click **Recover**.

Additional Resources

How to Copy a Tape

See Also

How to Recover a SQL Database to Its Original Location

How to Recover and Rename a SQL Database

How to Recover a Database to a Different Instance of SQL Server

How to Copy a SQL Database to a Network Folder

How to Recover a SQL Database and Allow Additional Log Backups

How to Recover a SQL Database and Allow Additional Log Backups

The System Center 2012 – Data Protection Manager (DPM) recovery process uses SQL Server functionality to recover a database such that all uncommitted transactions are rolled back. The recovery process opens the transaction log to identify uncommitted transactions. Uncommitted transactions are undone by being rolled back, unless they hold locks that prevent other transactions from viewing transactionally inconsistent data. This step is called the undo, or roll back, phase.

In some circumstances, the SQL Server administrator might require the database to be restored in a mode that allows log backups to be selectively played back. Using DPM, you can recover a database and leave it in a restoring state in which additional log backups can be applied to the database.

To recover a database without transaction roll back

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using the browse functionality, select the database to recover.
3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use. You can select any recovery point except **Latest**.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Recover to original SQL Server location** or **Recover to any SQL instance**, and then click **Next**.
8. If you select **Recover to any SQL instance**, on the **Specify recovery destination** page, specify the instance of SQL Server to which the database should be recovered.
9. On the **Specify Database State** page, select **Leave database non-operational but able to restore additional transaction logs**.
10. Select **Copy SQL transaction logs between the selected recovery point and latest available recovery point**, specify a copy destination for the transaction logs, and then click **Next**.

    DPM must have Write permission for the copy destination for the transaction logs.
11. Specify recovery options for network bandwidth usage throttling, SAN-based recovery, and e-mail notifications, and then click **Next**.
12. On the **Summary** page, review the recovery settings, and then click **Recover**.
13. Use the Restore Transact-SQL command with the HeaderOnly argument to retrieve the header information for the transaction logs. The header contains information that allows the log backup sequences to be correctly ordered.

14. Use the Restore command with the Log argument to apply the desired logs to the database in the right order.

    For more information on the Restore command, see RESTORE Arguments (Transact-SQL).

See Also

How to Recover a SQL Database to Its Original Location

How to Recover and Rename a SQL Database

How to Recover a Database to a Different Instance of SQL Server

How to Copy a SQL Database to a Network Folder

How to Copy a SQL Database to Tape

Protecting SharePoint Servers

This section provides information about how System Center 2012 – Data Protection Manager (DPM) protects servers running Microsoft SharePoint. All information in this section pertains to Microsoft SharePoint 2010 products, Microsoft Office SharePoint Server 2007, and Windows SharePoint Services 3.0 and Windows SharePoint Services 3.0 SP Search unless otherwise specified.

In This Section

Configuring SharePoint Protection

Protecting a SharePoint Farm

Protecting SharePoint Front-End Web Server

Protecting SharePoint Search

Recovering SharePoint Data

Performing SharePoint Protection Management Tasks

Performing General Maintenance on Servers Running SharePoint

Troubleshooting SharePoint Protection and Recovery

Configuring SharePoint Protection

System Center 2012 – Data Protection Manager (DPM) allows you to natively protect the following components of a SharePoint farm:

- SharePoint farm content
- Front-end Web server content

- SharePoint Search

This section deals with configuration settings and prerequisite software that is required on the DPM server and the protected computers to ensure that the SharePoint farm components are protected correctly.

In This Section

Configuring the DPM Server for SharePoint Protection

Configuring SharePoint Farm Servers

Configuring the DPM Server for SharePoint Protection

Before protecting a SharePoint farm, you must ensure that the following prerequisites are installed on the System Center 2012 – Data Protection Manager (DPM) server.

DPM Server Prerequisites

- System Center 2012 – Data Protection Manager (DPM)
- For every 10 million items in the farm, there must be at least 2 GB of space on the volume where the DPM folder is located. This space is required for catalog generation. To enable you to use DPM to perform a specific recovery of items (site collections, sites, lists, document libraries, folders, individual documents, and list items), catalog generation creates a list of the URLs contained within each content database. You can view the list of URLs in the recoverable item pane in the **Recovery** task area of DPM Administrator Console.

Configuring SharePoint Farm Servers

Before protecting a SharePoint farm with System Center 2012 – Data Protection Manager (DPM), you must perform series of configuration tasks on the SharePoint farm servers.

Install DPM Protection Agents

To protect data on SharePoint servers, ensure that the DPM protection agents are installed on all the servers of the farm. For more information about how to install DPM agent, see Installing Protection Agents.

In This Section

Configuring the Front-End Web Server

Configuring the SQL Backend Servers

Configuring the Front-End Web Server

Before protecting a SharePoint farm, ensure that the following prerequisites are installed on the front-end Web server.

Prerequisites for Front-end Web Server

If the front-end Web server is running Windows Server 2003 and you have installed Knowledge Base article 940349, ensure that the following prerequisites are installed:

- Windows SharePoint Services 3.0 with Service Pack 2, Windows SharePoint Services 3.0 with Service Pack 1, Microsoft Office SharePoint Server 2007 with Service Pack 2, Microsoft Office SharePoint Server 2007 with Service Pack 1, Microsoft SharePoint Foundation 2010, or Microsoft SharePoint Server 2010.
- For every 10 million items in the farm, at least 2 GB of space on the volume that is installed on the DPM server. This is required for catalog generation. To perform item-level recovery by using DPM, (site collections, sites, lists, document libraries, folders, individual documents and list items), catalog generation provides you with a list of URLs that are contained in each content database. In DPM Administrator console, this list of URLs is displayed in the **Recoverable Item** pane.
- If you are running Windows SharePoint Services 3.0 SP1 or MOSS 2007 SP1, download and install Knowledge Base article 941422.

  Note
  You must install Knowledge Base article 941422 on all protected servers on which Windows SharePoint Services 3.0, Microsoft Office SharePoint Server 2007 with SP1, and Microsoft Office SharePoint Server 2007 are installed.

- Run ConfigureSharePoint.exe on the front-end Web server. For more information about using ConfigureSharePoint, see Using ConfigureSharePoint.

- In the SharePoint farm, if you have SQL Server databases that are configured with SQL Server aliases, install the SQL Server client components on the front-end Web server that DPM will protect.

Using ConfigureSharePoint

Before you begin to protect a SharePoint farm, you must configure protection for SharePoint by using the ConfigureSharePoint.exe tool.

In DPM, ConfigureSharePoint.exe is a tool that is required to be run on the front-end Web server from where you plan to protect SharePoint farm data. The ConfigureSharePoint.exe file can be found in the <DPM Installation Path>\bin folder on the front-end Web server. This tool must be run in the following scenarios:

- Before you begin to protect a SharePoint farm
- Change in SharePoint farm administrator password
- Change in SharePoint farm administrator account

Permissions

To run the ConfigureSharePoint.exe tool, ensure that you meet the following prerequisites:

You must be a member of the Administrators group on the local computer to run this tool.

You must run this tool from an elevated command prompt.

The ConfigureSharePoint.exe tool provides the following permissions to the farm administrator on the front-end Web server:

- Read and Execute to all DPM directories: DPM has to load the DLLs from the DPM Bin directory when WSSCmdletWrapper.exe runs.
- Read, Execute, and Write (all) access on the Temp directory in the DPM directory: DPM has to create a directory inside the DPM Temp directory where item-level catalog dumps are created. DPM also creates a log file, WSSCmdletWrapperCurr.errlog, inside the DPM Temp directory.
- Read permissions to the DPM hive in the registry.

Syntax

ConfigureSharePoint [-EnableSharePointProtection] [-EnableSPSearchProtection] [-ResolveAllSQLAliases] [-SetTempPath <path>**]**

Note

To run this command, you must be a local administrator on the front-end Web server. In Windows Server 2008 and later versions, ensure that you run this command from an elevated command prompt.

Parameters

Parameter	Description
EnableSharePointProtection	• To enable SharePoint farm protection using a DPM server, you must ensure that you run this option on the front-end Web server from where you plan to protect SharePoint farm data. Do not run this option on more than one front-end Web server. To run this option on multiple servers, run the command “Stsadm –o unregisterwsswriter” on the front-end Web servers from where you do not plan to protect SharePoint farm data. This option performs the following: • Enables the SharePoint VSS writer required for SharePoint farm protection. • Registers the identity of the DCOM application WssCmdletsWrapper to run as a user whose credentials are entered with this option. If you are prompted to enter your user credentials, then enter the credentials of a farm administrator.
EnableSPSearchProtection	• You must run this option from any one of the front-end Web servers from where you plan to protect the Windows SharePoint Services 3.0/MOSS 2007 Search service. This server can be an indexing service or any other front-end Web server. Do not run this option on multiple servers. If you want to run this option on multiple servers, then delete the registry key **SharePointSearchEnumerationEnabled** under **HKLM\Software\Microsoft\ Microsoft Data Protection Manager\Agent\2.0** on the front-end Web server that is not used for protecting SharePoint Search services. • Enables the protection of SP Search and MOSS 2007 SSP by using the registry key **SharePointSearchEnumerationEnabled** under **HKLM\Software\Microsoft\ Microsoft Data Protection**

Parameter	Description
	Manager\Agent\2.0 on the front-end Web Server. • Registers the identity of the DCOM application WssCmdletsWrapper to run as a user whose credentials are entered with this option. If you are prompted to enter your user credentials, then enter the credentials of a farm administrator.
ResolveAllSQLAliases	This option displays all the aliases reported by the SharePoint VSS writer and resolves them to the corresponding SQL Server. It also displays their resolved instance names. If the servers are mirrored, it also displays the mirrored server. It reports all the SQL Server aliases that are not being resolved to a SQL Server.  **Note** This option can be run only after you run the ConfigureSharePoint [-EnableSharePointProtection] or ConfigureSharePoint [-EnableSPSearchProtection] command on the front-end Web server.
SetTempPath	Sets the environment variables TEMP and TMP to the specified path. Item-level recovery fails if a large site collection, site, list, or item is being recovered and there is insufficient space in the farm administrator Temporary folder. This option allows you to change the folder path of the temporary files to a volume that has sufficient space to store the site collection or site being recovered.

Configuring the SQL Backend Servers

The following prerequisites are required on the SQL Server backend servers:

SQL Server Prerequisites

If you are running Windows Server 2003 and have installed Knowledge Base article 940349, then you must install at least Microsoft SQL Server 2005 with Service Pack (SP1) or Microsoft SQL Server 2000 with SP4.

Note

System Center 2012 – Data Protection Manager (DPM) supports Standard, Enterprise, Workgroup, and Express Editions of SQL Server.

You must start the SQL Server VSS Writer Service on computers running SQL Server before you can start protecting SQL Server data. The SQL Server VSS Writer Service is turned on by default on computers running SQL Server. To start the SQL Server VSS Writer service, in the **Services** console, right-click SQL Server VSS writer, and then click **Start**.

Protecting a SharePoint Farm

To protect a SharePoint farm, you must perform the following steps:

1. Install DPM protection agents on all SharePoint servers that you plan to protect. For more information about how to install DPM agents, see Installing Protection Agents.
2. Enable SharePoint protection by configuring a front-end web server. For more information about how to configure front-end web servers, see Configuring the Front-End Web Server.
3. If you want to enable protection for Windows SharePoint Services 3.0/Microsoft Office Sharepoint Server 2007 Search, you must configure a front-end web server to enable Microsoft Office SharePoint Server 2007 for Search protection.
4. On the DPM server, run the **Create New Protection Group** Wizard to protect the SharePoint data that exists under a front-end web server that is configured for protection. For more information about how to create a protection group, see DPM Help.

Warning

DPM does not support protecting remote FILESTREAM. The FILESTREAM should be part of the database.

In this section

Protecting a SharePoint Farm by Using Mirrored Databases

Protecting a SharePoint Farm by Using Databases With SQL Server Aliases

Long-Term Protection for a SharePoint Farm on Tape

Protecting a SharePoint Farm by Using Mirrored Databases

System Center 2012 – Data Protection Manager (DPM) extends support for Microsoft SharePoint to include support for SharePoint content databases that uses SQL Server database mirroring technology. This additional support does not translate into any major changes in the procedure to protect or recover SharePoint data in DPM.

Prerequisites

Install the DPM protection agent on both the computers that are running the instance of SQL Server and hosts the principal and mirror database.

Note
DPM does not support mirroring the database on the same instance of SQL Server.

Common Scenarios

A protected SharePoint database gets mirrored

At the time of the backup, DPM detects that the database has been mirrored and raises an alert that farm configuration has been changed. DPM treats the mirrored database as a new database in the farm and automatically protects it. Although the alert is not deactivated, all the content in the SharePoint farm will continuously be protected. To inactivate this alert, you must stop protection for the farm (with retain data) and re-protect it.

Note
Even if failovers between principal and mirrored copies of the database occur, DPM maintains a single replica for the mirror.

Principal partner in a mirror fails over and fails back before next backup

This scenario does not affect protection in any way unless a backup is in progress.

Principal partner fails and the mirror server takes over

DPM detects that the mirror is now the principal partner, stops the backup job, and performs a consistency check after 30 minutes on the database that failed over. Alternatively, you can start a manual consistency check on the farm after the alert is raised.

Note

If, during these 30 minutes, the database fails back to the original principal, DPM detects this and resumes protection after performing a consistency check.

A mirror is broken

When the mirror is broken for a mirrored SQL Server database that is currently protected by DPM, backups fail with alerts. This is similar to the behavior when the protected SharePoint database gets mirrored.

Protecting a SharePoint Farm by Using Databases With SQL Server Aliases

System Center 2012 – Data Protection Manager (DPM) supports protection of a SharePoint farm that uses SQL Server databases configured with SQL Server aliases. This additional support does not require any major changes in the procedure you use to protect or recover SharePoint data with DPM.

Important
You can use only TCP/IP aliases.

Prerequisites

- You must configure SQL Server aliases and define all SQL Server aliases in the farm on the front-end Web Server. We recommend that you use one SQL Server alias per database.
- The SQL Server client connectivity components must be installed on the front-end Web Server.

See Also

How to: Create a Server Alias for Use by a Client (SQL Server Configuration Manager)

Long-Term Protection for a SharePoint Farm on Tape

When protecting a SharePoint farm, DPM takes the disk backup for all the databases that are online at that time. When DPM retries backup for failed databases, two different recovery points are created for the farm.

If long-term backup is configured for a SharePoint farm, DPM needs to find databases across multiple recovery points and ensure that the complete set of databases in the farm are backed up on tape. To do this, DPM does the following:

Checks the list of databases present in the latest topology of the SharePoint farm. The latest topology is stored in DPM.

Checks the latest recovery point on the disk and copies the databases on the disk to the tape.

Checks the previous recovery point for all the databases that were missing in the latest recovery point.

Similarly, DPM traverses older recovery points one-by-one unless the recovery points of all the databases are found.

If there is a database for which a recovery point was not created since the last successful scheduled tape backup, then that database's recovery point on the tape fails.

Note
Long-term protection for a SharePoint farm on tape is available only on the primary DPM server.

Protecting SharePoint Front-End Web Server

System Center 2012 – Data Protection Manager (DPM) supports the protection of front-end Web server computers of a SharePoint farm that are deployed on either physical computers or on virtualized environments such as Hyper-V.

Front-End Web Server Running on Hyper-V Virtual Machine

With DPM, you can perform backup and recovery of virtual machines that are running on Hyper-V. For more information about how to protect Hyper-V virtual machines, see Protecting virtual machines with SMB storage and Recovering virtual machines. If the front-end Web server of a SharePoint farm is on a computer that is running on any other virtualization technology, you can protect it just as you would a physical computer.

Front-End Web Server Running on Physical Computer

With DPM, you can perform backup and recovery of physical computers by using Bare Metal Recovery (BMR). For more information, see Setting Up BMR Protection and Recovering BMR.

Protecting SharePoint Search

The procedure to protect a SharePoint Search requires a few tasks to be performed before you start the Create New Protection Group Wizard. For details on protecting Windows SharePoint Services 3.0 SP Search and MOSS 2007 Shared Services Provider (SSP), see the other topics in this section.

In This Section

Protecting Windows SharePoint Services 3.0 SP Search Service Data

Protecting Microsoft Office SharePoint Server 2007 SSP Search

Protecting Windows SharePoint Services 3.0 SP Search Service Data

System Center 2012 – Data Protection Manager (DPM) enables you to back up and restore indexes that are created by Windows SharePoint Services 3.0 SP Search Service Data.

Protecting Windows SharePoint Services 3.0 SP Search Service Data

When you create a protection group for a SharePoint farm, DPM detects and lists the Windows SharePoint Services 3.0 SP Search instance. The following procedure lists the steps to protect Windows SharePoint Services SP Search Service data:

1. Enable SPSearch protection on the protected computer by using ConfigureSharePoint.exe. For more information about ConfigureSharePoint.exe, see Using ConfigureSharePoint.
2. Use the Create New Protection Group Wizard to protect the SPSearch instance, which is listed under the farm in which it was created.

For DPM support for Windows SharePoint Services index protection, consider the following:

- During the backup process, DPM pauses the index crawl and all background processes. After the backup process is complete, DPM automatically resumes these processes.
- If the backup schedule for the Search database overlaps the schedule for other databases on the same server that belong to another protection group, it results in a longer pause of the index crawl. We recommend that you schedule backups to minimize the pause of the index crawl.

- DPM performs express full backups for the Search database, but for index files it performs only consistency checks.

Protecting Microsoft Office SharePoint Server 2007 SSP Search

With System Center 2012 – Data Protection Manager (DPM), you can backup and restore SharePoint Search created by Microsoft Office SharePoint Server 2007.

Protect Microsoft Office SharePoint Server 2007 for Search and Microsoft Office SharePoint Server 2007 SSP

DPM recognizes and lists the Microsoft Office SharePoint Shared Service Provider (SSP) instance when you create a protection group for the SharePoint farm. The following procedure lists the steps to take to protect a computer that runs Microsoft Office SharePoint Server 2007 SSP.

To Protect a Computer that runs Microsoft Office SharePoint Server 2007 SSP

1. To enable SPSearch protection on the protected computer, use ConfigureSharePoint.exe. For more information about ConfigureSharePoint.exe, see Using ConfigureSharePoint.
2. To protect the Microsoft Office SharePoint Server SSP instance, which is listed under the SharePoint farm in which it was created, use the **Create New Protection Group** wizard.

Note

During the backup process, DPM pauses the index crawling and all background processes. After the backup process is complete, DPM automatically resumes these processes. This procedure does not affect the search function.

Recovering SharePoint Data

The following points apply to the recovery of SharePoint data:

- The Central Administration content database is the first content database created with the Central Administration when you set up your farm.

Caution

Do not directly recover the Central Administration content database or the configuration database because this could cause data corruption in the SharePoint farm.

- The recovery point time for SharePoint data displayed on the **Browse** tab may differ from the time displayed on the **Search** tab. The **Browse** tab displays the backup time for the farm, while the **Search** tab lists the correct recovery point time for sites, documents, and folders.

The following table shows you the various possible recovery scenarios for SharePoint.

	Using recovery farm		**Without recovery farm**	
	Microsoft Office SharePoint Server 2007	Microsoft SharePoint Server 2010	Microsoft Office SharePoint Server 2007	Microsoft SharePoint Server 2010
Optimized recovery	No	Yes	Yes	Yes
Unoptimized recovery	No	Yes	Yes	Yes

In This Section

Recovering SharePoint Front-End Web Server

Front-end Web servers for a SharePoint farm can be deployed either on physical computers or on virtual machines such as those found in a Hyper-V virtual environment.

Recovering a Front-End Web Server Deployed on a Physical Computer

To recover a front-end Web server that was backed up by using the Bare-Metal Recovery (BMR) option, see Recovering BMR.

Recovering a Front-End Web Server Deployed on a Hyper-V Virtual Machine

The steps to recover a front-end Web server deployed on a Hyper-V virtual machine are similar to how you recover a virtual machine. For more information, see How to Recover a Virtual Machine.

Recovering SharePoint Farm Content

To recover a SharePoint farm, the recovery destination must meet the following requirements:

- The front-end Web servers are configured the same as they were when the recovery point was created.
- The farm structure must be created on the front-end Web server; the farm data will be recovered to the existing structure.
- The instances of SQL Server are configured with the same names as when the recovery point was created.
- The instances of SQL Server are configured with the same drive configuration as when the recovery point was created.
- The recovery farm must have all service packs, language packs, and patches installed on the primary farm.

Caution

You cannot perform a full farm recovery to a new location.

You can encounter two situations when restoring a complete farm:

- A farm configuration exists as it did at the time of taking the backup. In this case, you will be restoring to a functioning farm.
- The Configuration database is corrupt and the servers in the farm are down.

To recover farm data to a functioning farm

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. In the **Protected data** pane, expand the server that contains the farm you want to recover, and then click **All Protected SharePoint Data**.

   The farm displays in the **Recoverable item** pane as *server name\farm name*.
3. Use the calendar and **Recovery time** menu to select a recovery point.
4. In the **Recoverable item** pane, click the farm item.

5. Click **Recover** in the **Actions** pane.
6. Complete the wizard.

To recover farm data when the protected farm is unavailable

1. Create a new farm that uses the same instance of SQL Server and the same front-end Web server as the original protected farm.
2. On the front-end Web server that DPM uses to recover farm data, run the following command at the command prompt::

   ConfigureSharePoint-EnableSharePointProtection
3. On the DPM server, in DPM Administrator Console, click **Recovery** on the navigation bar.
4. In the **Protected data** pane, expand the server that contains the farm you want to recover, and then click **All Protected SharePoint Data**.

   The farm displays in the **Recoverable item** pane as *server name\farm name*.
5. Use the calendar and the **Recovery time** menu to select a recovery point.
6. In the **Recoverable item** pane, click the farm item.
7. In the **Actions** pane, click **Recover**.
8. Complete the wizard.
9. On the main front-end Web server for the server farm, run the SharePoint Products and Technologies Configuration Wizard and disconnect the front-end Web server from the farm.

   Note
   If the main front-end Web server for the server farm is not the front-end Web server that DPM uses to protect the farm, you must also disconnect the front-end Web server that DPM uses to protect the farm.
10. Open Internet Information Services (IIS) and delete all Web site and application pool entries related to the farm.
11. Run the SharePoint Products and Technologies Configuration Wizard, select to connect to an existing server farm, and specify the server name and database name for the farm you created in step 1.

    Note
    Perform step 11 for all front-end Web servers for the server farm.
12. On the **Completing the SharePoint Products and Technologies Configuration Wizard** page, click **Advanced Settings**, and then click **Next**.
13. On the **Advanced Settings** page, select the option **Use this machine to host the web site**, and complete the wizard.

In This Section

Recovering a SharePoint Farm by Using Databases with SQL Server Aliases

Recovering a SharePoint Farm by Using Mirrored Databases

Recovering a SharePoint Farm by Using Databases with SQL Server Aliases

Recovering a farm that uses a database with a SQL Server alias

The procedure to recover a farm with SQL Server aliases configured is the same as the procedure to recover a farm without aliases configured.

Before you perform a recovery, ensure that aliases that correspond to the respective databases are configured in the same manner as they were configured when the recovery point for the SharePoint farm was created.

You can retrieve all the SQL Server aliases used using the following command in the DPM Management Shell

$RecoveryPoint.GetSqlaliases()

To enumerate $RecoveryPoint, you must start by retrieving the protection groups. For more information, refer to the DPM Management Shell Help using the following cmdlet

get-help get-recoverypoint -full

See Also

Recovering SharePoint Data

Recovering a SharePoint Farm by Using Mirrored Databases

Recovering a farm with a mirrored database to its original location

The procedure to recover a farm with a mirrored database is the same as the procedure to recover a farm with stand-alone databases. Additionally you will find the following options when you select the **Recover all SharePoint content and components** option on the **Select Recovery Type** page of the Recovery Wizard.

Name	Description
Typical recovery	Select this option to recover the mirrored SQL Server databases to the instances of SQL Server that were hosting these databases as the principal database when the selected recovery point was created.
Custom recovery	Select this option to recover the mirrored SQL Server databases of the SharePoint farm to the instances of SQL Server. At the point of recovery point creation, for each mirrored SQL Server database, you can select either of its partner instances of SQL Server (principal/mirror). Before you select the instance of SQL Server, make sure of the following: • The selected instance of SQL Server is online. • The SQL alias being used on the front-end Web server points to the selected instance of SQL Server.

The default selection is the partner from which the database was last backed up.

If you are using a SQL Server alias for the mirrored database, then before the recovery ensure that aliases corresponding to the respective databases are configured such that they refer to the SQL Server instance location selected on the Recovery Wizard page.

Otherwise the farm recovery fails at the end because it cannot attach the databases after recovery. For more information, see Recovering a SharePoint Farm by Using Databases with SQL Server Aliases.

See Also

Recovering SharePoint Data

Recovering SharePoint Web Application

Use the procedure in this topic to recover a protected Web application in Windows SharePoint Services 3.0.

Procedure to recover a Web application

1. Create a Web application in the target farm.

   Note
   If you want to retain the same URL for the application, ensure that the host header and port are the same as the original application.
2. Restore all the databases in that Web application to either the original location or to a different SQL Server.
3. Attach each content database to the Web application by using the stsadm command or from the Central Administrator site

See Also

Addcontentdb: Stsadm operation (Office SharePoint Server)

Recovering SharePoint Content Database

The procedure to recover a SharePoint database is similar to how to recover a SQL Server database by using System Center 2012 – Data Protection Manager (DPM). For more information about how to recover a SQL Server database, see Recovering SQL Server Data.

Note
After a SharePoint database is recovered, it cannot be left in a recovering state.

Note
To recover a mirrored database to its original instance of SQL Server, select the **Recover to any SQL Instance** option, and then, on the **Specify Alternate Recovery Location** page, specify the recovery destination path of the original instance of SQL Server.

Recovering SharePoint Items

The following points apply to the recovery of SharePoint items:

- Item details do not appear on the Recovery Wizard Summary page for SharePoint sites and items.
- If document versioning is enabled, documents in SharePoint might be in one of the following states:

  Created not checked in - Visible only to the creator

  Checked in - Visible to administrator and users with permission to publish

  Published - Visible to users with permission to approve

  Approved - Visible to all viewers

- When you recover SharePoint data, only documents that are checked in, published, or approved are recovered. The following documents are not recovered:
  - Documents not checked in on the user computer
  - Documents in either the user computer Recycle Bin or the site collection Recycle Bin
- Recovery of Windows SharePoint Services internal items, such as default.aspx, is not supported.

In This Section

Using a Recovery Farm

A *recovery farm* is a temporary staging SharePoint where the content database that contains the item to be restored is temporarily hosted. The SharePoint APIs extract the item from the content database in the recovery farm and then import the item into the target farm.

In This Section

Creating a Recovery Farm

A recovery farm is a single-computer SharePoint farm running both SharePoint front-end Web server and SQL Server 2005 with SP2. The recovery farm server should have a local instance of SQL Server running.

Note

The version of SQL Server must be the same or higher than what was installed at the time of backup.

SQL Server VSS Writer should be running on the recovery farm.

This computer must be separate from the DPM server, Active Directory, domain controller, any server on which SharePoint data is protected by DPM and farm computers.

To create a recovery farm

1. Install the DPM agent on the recovery farm computer through the DPM server backing up the farm.
2. Run ConfigureSharepoint.exe. For more information on running ConfigureSharePoint.exe, see Using ConfigureSharePoint.
3. If you protect a MOSS farm, then the recovery farm must also be MOSS.
4. The features and templates installed on the recovery farm must match those of the target farm as it was at the time of backup. Any customized templates, added or modified, on the production farm, must be added to the recovery farm to ensure a successful recovery.

   Note
   You can enable all the features and templates installed on the recovery farm and use it for the different farms existing in your SharePoint environment.
5. If a service pack or update is installed on the protected farm, the recovery farm must have the same service pack or update installed otherwise item-level restore operations could fail.
6. Both the recovery and target farms must be in the same language and have the same language packs installed.
7. Create a Web application and name it DPMRecoveryWebApplication. To create a new Web application, see the instructions at Create or extend Web applications (Windows SharePoint Services).
8. Ensure that no content database is already attached to the recovery web application (DPMRecoveryWebApplication) as this will cause recoveries to fail. The web application name **DPMRecoveryWebApplication** is a required name and it must be created for DPM to be able to restore any SharePoint data.

When you restore a site, DPM restores the database to the recovery farm, extracts the site from the recovery farm, and imports it into the target farm. During this process, DPM creates a temporary file on the recovery farm at a location specified in the Recovery Wizard. You should periodically delete the temporary files at that location.

Note
The recovery farm must have enough hard disk space to store the largest content database in the environment. Best practice would dictate that an additional 10-20% be allocated on the temporary storage volume to provide a cushion for growth and reduce the risk of running out of space when trying to recover time-sensitive SharePoint data.

See Also

Create a recovery farm (Office SharePoint Server 2007)

Recovering a SharePoint Site Collection

Use the procedure in this topic to recover a protected SharePoint site collection.

Procedure to recover a site collection

1. Create an empty site collection with the same name on the target farm.
2. Apply the same features and templates to the site collection that was used at the time of backup. If they do not match, SharePoint will raise an error to indicate that the site templates do not match, which causes the DPM site restoration to fail.
3. Recover the top-level site from the site collection. For more information about how to recover a SharePoint site, see Recovering a SharePoint Site.

   Note
   If a content database contains only one site collection, you can chose to recover the database directly, and then attach it to the farm using the stsadm command.

See Also

Addcontentdb: Stsadm operation (Office SharePoint Server)

Recovering a SharePoint Site

With System Center 2012 – Data Protection Manager (DPM), you can recover a Windows SharePoint site either to its original backup location or to another location on the same farm from which the site was backed up.

If you are recovering to the original location, DPM does not overwrite the files; instead, it performs a merge. The following example explains this behavior.

Assume that a document library has two files – TextFile1 and TextFile2. At a point in time (T1), DPM creates a recovery point (R1) for the library. The following day, three changes occur to the library – TextFile1 is deleted; TextFile2 is changed, creating TextFile2.1; and TextFile3 is added to the library. At another point in time (T2), DPM creates a second recovery point (R2) for the library.

If you then recover the site by using the first recovery point (R1), the document library has the files TextFile1, TextFile2, and TextFile3. Note that TextFile2.1 is lost because it is overwritten with TextFile2.

Note
This recovery process does not work with lists. If you are trying to restore lists, you must manually delete all lists under the site, and then restore the site.

Whether you recover a SharePoint site to its original location or to another location on the same farm, the overall steps are the same. First, you create a recovery farm, and then you use DPM to recover the site by using the recovery farm.

Note

You can use DPM to recover items (site collections, sites, document libraries, lists, documents, and list items) from a Microsoft SharePoint Foundation 2010 or Microsoft Office SharePoint Server 2010 farm both with and without a recovery farm.

To recover a SharePoint site

1. Create a farm that DPM can use for the recovery. To create a recovery farm, see the instructions at Creating a Recovery Farm.
2. In DPM Administrator Console, click **Recovery** on the navigation bar.
3. In the **Protected data** pane, expand the server that contains the farm you want to recover, and then click **All Protected SharePoint Data**.

   The farm appears in the **Recoverable Item** pane as *server name\farm name*.
4. Double-click the farm item.

   The databases for the farm appear in the **Recoverable Item** pane.
5. Navigate to the recoverable item objects and locate the site that you want to recover.
6. Select a recovery point for the site that you want to recover, and then, in the **Actions** pane, click **Recover**.
7. On the **Review Recovery Selection** page, confirm that the correct item is being recovered based on **Recovery Item**.
8. On the **Select Recovery Type** page, select one of the following options:
   - **Recover to original site**
   - **Recover to an alternate site**
9. This step applies only to SharePoint 2010:

   On the **Select Recovery Process** page, select one of the following options:

   a. **Recover without using a recovery farm**. Select this option if the version of the target Microsoft SharePoint 2010 farm is the same as the version at the time of the selected recovery point, and then click **Next**.

      i. On the **Specify Temporary Server** page, do the following:

         - In the **SQL instance** field, browse to the instance of SQL Server that can be used temporarily to stage a copy of the SharePoint content database.

      The temporary instance of SQL Server can be:

         - An instance of SQL Server that is a member of the protected SharePoint farm
         - DPM's instance of SQL Server
         - Any other instance of SQL Server that can be accessed by DPM and by

the front-end Web server of the protected SharePoint farm

noteDXDOC112778PADS Note

If you are using DPM's instance of SQL Server or any other instance of SQL Server, ensure that its version is equal to or later than the version of the production SQL Server. The selected instance of SQL Server can be a Microsoft Cluster Server (MSCS).

- In the **Database file location** field, browse to the instance of SQL Server on that server, and then select the temporary location where the database files can be copied.

b. **Recover using a recovery farm**. Select this option if the version of the target Microsoft SharePoint 2010 farm has changed since the selected recovery point was created, and then click **Next**. For more information about how to create a recovery farm, see Creating a Recovery Farm.

i. On the **Specify Temporary Server** page, do the following:

1. In the **Front-end Web server** field, browse for the recovery farm server where DPMRecoveryWebApplication has been created to temporarily stage data prior to recovery.
2. In the **SQL instance** field, browse to the instance of SQL Server that can be used temporarily to stage a copy of the SharePoint content database that contains the requested site before recovery.
3. In the **Database file location** field, browse to the instance of SQL Server on that server and then select the temporary location where the database files can be copied to a recovery farm.

10. This step applies only if you are recovering to an alternate location.

    In the **Recovery target site** section, enter the URL for the alternate site. A site can be restored to a different location within the same farm to which it belongs. Therefore, specify a URL within the same SharePoint farm under which you want to recover the selected SharePoint site.

    Note

    The target site URL must be based on the same site template as the site that is being restored. For example, SharePoint will not allow a site that was created by using a Wiki Site template to be restored onto a site that was created by using a Team Site, Blank Site, Blog, or Document Workspace templates. A custom template must reside on the recovery farm and be used to create the alternate site to which the recovery is being made.

11. On the **Specify Staging Location** page, enter a directory where the SharePoint can be temporarily stored pending recovery to the original or alternate site.

    Note

    Note the following:

- Network bandwidth usage throttling is used when there are concerns about the restore process using excessive bandwidth for bandwidth-sensitive applications.

- The SAN Recovery option is only available if the attached SAN is capable of snapping clones and splitting clones.
- The Notification section is only to notify administrators and other personnel of the completion of the recovery process.

12. On the **Specify Recovery Options** page, in the **Restore Security** section, specify whether security settings and metadata from the recovery point or the original site will be applied to the recovered site data.

    Important
    This is an important consideration if there have been any changes to the security settings since the recovery point was taken.

13. On the **Summary** page, confirm all settings, and then click **Recover** to begin the recovery process.

See Also

Recovering SharePoint Data

Recovering SharePoint Items

Recovering a List, List Item, Document Library, or Document

With System Center 2012 – Data Protection Manager (DPM), you to recover items from a SharePoint 2010 farm. You can use DPM to recover SharePoint items, such as sites, site collections, documents, document libraries, lists and list items from a DPM recovery point to the original site or to an alternate site.

When you restore a SharePoint item, DPM restores the database to a temporary instance of SQL Server, extracts the item from the content database, and then imports it into the targeted farm. During this process, DPM creates a temporary file on the recovery farm at the location you specify in the Recovery Wizard. You should periodically delete the temporary files DPM creates at that location.

To recover a SharePoint item to its original location

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. In the **Protected data** pane, expand the server that contains the farm you want to recover, double-click **All Protected SharePoint Data**, and then double-click the server farm name.

   Content databases display in the **Recoverable item** pane.
3. Use the calendar and **Recovery time** menu to select a recovery point.
4. In the **Recoverable item** pane, select the content database, browse to the item that you

want to recover and select it.

Note

You can only select and recover one object at a time. If you want to recover more than one object, consider recovering a higher level folder to an alternate location and then recovering the individual objects from within the SharePoint Central Administration website.

5. In the **Actions** pane, click **Recover**, and then, on the **Review Recovery Selection** page, confirm the recovery details.
6. On the **Select Recovery Type** page, select **Recover to original site**.
7. The following step applies only to SharePoint 2010:

   On the **Select Recovery Process** page select any one of the following two options that are listed below:

   a. **Recover without using a recovery farm.** Select this option if the version of the target Microsoft SharePoint 2010 farm is same as at the time of the selected recovery point, and then click **Next**.

      i. On the **Specify Temporary Server** page, do the following:

         1. In the **SQL instance** field browse for the instance of SQL Server that can be used temporarily to stage a copy of the SharePoint content database that contains the requested item before recovery.
         2. In the **Database file location** field, browse for the instance of SQL Server on that server and then select the temporary location where the database files can be copied.

      The temporary instance of SQL Server can be:

         a. An instance of SQL Server that is a member of the protected SharePoint farm
         b. DPM's instance of SQL Server
         c. Any other instance of SQL Server that can be accessed by DPM and by the front-end Web server of the protected SharePoint farm

noteDXDOC112778PADS Note

If you are using DPM's instance of SQL Server or any other instance of SQL Server, ensure that its version is equal to or later than the version of the production SQL Server. The selected instance of SQL Server can be a Microsoft Cluster Server (MSCS).

   b. **Recover using a recovery farm**. Select this option if the version of the target Microsoft SharePoint 2010 farm has changed from the time, the selected recovery point was created, and then click **Next**.

      i. On the **Specify Temporary Server** page, enter the information for recovery farm. For more information about how to create a recovery farm, see Creating a Recovery Farm.

1. In the **Front-end Web server** field, browse for the recovery farm server where DPMRecoveryWebApplication has been created to temporarily stage data prior to recovery.
2. In the **SQL instance** field, browse for the instance of SQL Server that can be used temporarily to stage a copy of the SharePoint content database that contains the requested item before recovery.
3. In the **Database file location** field, browse for the instance of SQL Server on that server, and then select the temporary location where the database files can be copied on to a recovery farm.

8. On the **Specify Staging Location** page, enter a directory where the SharePoint data will be temporarily stored, pending recovery to the original site.
9. On the **Specify Recovery Options** page, specify whether the recovery point's security settings or the original site's security settings will be applied to the recovered data object in the **Restore Security** section.

   This is an important consideration if there have been security settings changes since the recovery point was taken.

   Note

   The network bandwidth usage throttling is used when there are concerns about the restore process consuming excessive bandwidth.

   The SAN Recovery option is only available if the attached SAN is capable of snapping clones and splitting clones.

   The **Notification** section is simply to notify administrators and other personnel of the completion of the recovery process.
10. On the Summary page, confirm the settings, and then click **Recover** to begin the process.

To recover a SharePoint item to its original location

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. In the **Protected data** pane, expand the server that contains the farm you want to recover, double-click **All Protected SharePoint Data**, and then double-click the server farm name.

   Content databases display in the **Recoverable item** pane.
3. Use the calendar and **Recovery time** menu to select a recovery point.
4. In the **Recoverable item** pane, select the content database, browse to the item that you want to recover and select it.

Note

You can only select and recover one object at a time. If you want to recover more than one object, consider recovering a higher level folder to an alternate location and then recovering the individual objects from within the SharePoint Central Administration Web site.

5. In the **Actions** pane, click **Recover**, and then, on the **Review Recovery Selection** page, confirm the recovery details.
6. On the **Select Recovery Type** page, select **Recover to original site**.
7. This step applies only to SharePoint 2010:

   On the **Select Recovery Process** page select one of the following options:

   a. **Recover without using a recovery farm.** Select this option if the version of the targeted Microsoft SharePoint 2010 farm is same as the version at the time of the selected recovery point, and then click **Next**

      i. On the **Specify Temporary Server** page, do the following:

         1. In the **SQL instance** field browse for the instance of SQL Server that will be used to temporarily stage a copy of the SharePoint content database that contains the requested item before recovery.
         2. In the **Database file location** field, browse for the instance of SQL Server on that server, and then select the temporary location to which the database files can be copied.

      The temporary instance of SQL Server can be:

         a. An instance of SQL Server that is a member of the protected SharePoint farm
         b. DPM's instance of SQL Server
         c. Any other instances of SQL Server that can be accessed by DPM and by the front-end Web server of the protected SharePoint farm

noteDXDOC112778PADS Note

If you are using DPM's instance of SQL Server or any other instance of SQL Server, ensure that its version is equal to or later than the version of the production SQL Server. The selected instance of SQL Server can be a Microsoft Cluster Server (MSCS).

   b. **Recover using a recovery farm**. Select this option if the version of the targeted Microsoft SharePoint 2010 farm has changed from the time that the selected recovery point was created, and then click **Next**.

      i. On the **Specify Temporary Server** page, enter the information for the recovery farm. For more information about how to create a recovery farm, see Creating a Recovery Farm.

         1. In the **Front-end Web server** field, browse for the recovery farm server where DPMRecoveryWebApplication has been created to temporarily

stage data prior to recovery.

2. In the **SQL instance** field, browse for the instance of SQL Server that will be used temporarily to stage a copy of the SharePoint content database that contains the requested item before recovery.
3. In the **Database file location** field, browse for the instance of SQL Server on that server and then select the temporary location where the database files can be copied on to a recovery farm.

8. On the **Specify Staging Location** page, enter a directory where the SharePoint data will be temporarily stored, pending recovery to the original site.
9. On the **Specify Recovery Options** page, specify whether the recovery point's security settings or the original site's security settings will be applied to the recovered data object in the **Restore Security** section.

   This is an important consideration if there have been security settings changes since the recovery point was taken.

   Note

   Network bandwidth usage throttling is used when there are concerns about the restore process consuming excessive bandwidth.

   The SAN Recovery option is available only if the attached SAN is capable of snapping clones and splitting clones.

   The **Notification** section is to notify administrators and other personnel of the completion of the recovery process.
10. On the **Summary** page, confirm the settings, and click **Recover** to begin the process.

To recover an object to an alternate location

Note

An alternate location can be on the same SharePoint farm but with a different site name or port number.

1. Create a farm that DPM can use for the recovery. For more information, go Creating a Recovery Farm.
2. In DPM Administrator Console, click **Recovery** on the **Actions** pane.
3. In the **Protected data** pane, expand the server that contains the farm you want to recover, double-click **All Protected SharePoint Data**, and then double-click the server farm name.

   Content databases display in the **Recoverable item** pane.
4. Use the **Calendar and Recovery Time** menu to select a recovery point.
5. In the **Recoverable item** pane, select the content database, and then browse to the item you want to recover.

Note

You can select and recover only one object at a time. If you want to recover more than one object, consider recovering a higher level folder to an alternate location, and then recovering the individual objects from within the SharePoint Central Administration Web site.

6. In the **Actions** pane, click **Recover**, and then, on the **Review Recovery Selection** page, confirm the recovery details.
7. On the **Select Recovery Type** page, select **Recover to an alternate site**.
8. The following step applies only to SharePoint 2010:

   On the **Select Recovery Process** page, select one of the following options:

   a. **Recover without using a recovery farm.** Select this option if the version of the targeted Microsoft SharePoint 2010 farm is same as it was at the time of the selected recovery point, and then click **Next**.

      i. On the **Specify Temporary Server** page, do the following:

         1. In the **SQL instance** field browse for the instance of SQL Server that can be used temporarily to stage a copy of the SharePoint content database that contains the requested item before recovery.
         2. In the **Database file location** field, browse for the instance of SQL Server on that server and then select the temporary location where the database files can be copied

      The temporary instance of SQL Server can be:

         a. An instance of SQL Server that is a member of the protected SharePoint farm.
         b. DPM's instance of SQL Server.
         c. Any other instances of SQL Server that can be accessed by DPM and by the front-end Web server of the protected SharePoint farm.

noteDXDOC112778PADS Note

If you are using DPM's instance of SQL Server or any other instances of SQL Server then make sure that its version is equal to or a has a later version than the version of the production SQL Server. The selected instance of SQL Server can be a Microsoft Cluster Server (MSCS).

   b. **Recover using a recovery farm**. Select this option if the version of the target Microsoft SharePoint 2010 farm has changed from the time, the selected recovery point was created. Click **Next**

      i. On the **Specify Temporary Server** page, enter the information for recovery farm. For more information about how to create a recovery farm, see Creating a Recovery Farm.

         1. In the **Front-end Web server** field, browse for the recovery farm server

where DPMRecoveryWebApplication has been created to temporarily stage data prior to recovery.

2. In the **SQL instance** field, browse for the instance of SQL Server that can be used temporarily to stage a copy of the SharePoint content database that contains the requested item before recovery.
3. In the **Database file location** field, browse for the instance of SQL Server on that server and then select the temporary location where the database files can be copied on to a recovery farm.

9. In the Recovery target site field, enter the URL for alternate site. An item can be restored to a different location within the same farm to which it belongs to. Therefore specify a URL within the same SharePoint farm under which you would want to recover the selected SharePoint item.

   Note

   The site URL entered into the Target site URL field must be based on the same site template as the site hosting the object which is being restored. For example, SharePoint will not allow an object created in a site using a 'Wiki Site' template to be restored onto a site created using the 'Team Site', 'Blank Site', 'Blog', or 'Document Workspace' templates. If custom templates have been used, those same templates must reside on the recovery farm as well as having been used to create the alternate site where the recovery is being made to.

10. On the Specify Staging Location page, enter a directory where the SharePoint data will be temporarily stored, pending recovery to the original site.
11. On the Specify Recovery Options page, specify whether the recovery point's security settings for the object being recovered or the original site's security settings will be applied to the recovered data object in the Restore Security section. This is an important consideration if there have been security settings changes since the recovery point was taken.

    Note

    The network bandwidth usage throttling is used when there are concerns about the restore process consuming excessive bandwidth from bandwidth sensitive applications.

    The SAN Recovery option is only available if the attached SAN is capable of snapping clones and splitting clones.

    The Notification section is simply to notify administrators and other personnel of the completion of the recovery process.

12. Confirm the settings on the Summary page and click **Recover** to begin the process.

Note

See Also

Recovering SharePoint Data

Recovering a SharePoint Site

DPM Cataloging to Recover SharePoint Items

SharePoint cataloging is the process of collecting lists of URLs (such as site collections, sites, documents, or lists) in a SharePoint farm.

In DPM, cataloging is a separate task from the task to create a recovery point for a SharePoint farm. The catalog task is scheduled automatically when you configure SharePoint farm protection. SharePoint cataloging happens automatically only once a day, regardless of the number of backups that are taken each day.

By default, the catalog task is scheduled to run three hours after the first scheduled backup of the corresponding SharePoint farm in the day. To modify the default schedule, run the **Set-DPMProtectionJobStartTime** cmdlet in DPM Management Shell on the DPM server.

In DPM, creating a catalog of the farm (list of URLs within the farm) is tightly tied to the backup of the SharePoint farm.

Syntax

Set-DPMProtectionJobStartTime–ProtectionGroup <ProtectionGroup Object> –CatalogOffset <Offset in Minutes>

Parameters

Parameter	Description
ProtectionGroup	Provide the protection group that contains the SharePoint farm. **Note** The offset will change for all the SharePoint farms in this protection group. For more information about the ProtectionGroup object, type **Get-help Get-DPMProtectionGroup –Full** in DPM Management Shell.
CatalogOffset	Provide the offset from the time of the first scheduled backup in a day for the SharePoint

Parameter	Description
	farm. The value entered here should be in minutes. Default is 180 minutes.

When you change the offset for the catalog task, ensure that cataloging for the SharePoint farm begins only after the recovery point prior to the task is completed.

To run the catalog task by using DPM Management Shell

Use the following syntax to run the cmdlet Start-DPMCreateCatalog:

Start-DPMCreateCatalog –DataSource <DataSourceObject>

Parameter

DataSource - Provides the DataSource object for the SharePoint farm for which the catalog needs to be run. For more information about the DataSource object, type **Get-Help Get-DPMDataSource –Full** in DPM Management Shell.

Optimized item-level recovery for SharePoint

Item level recovery for SharePoint farms is already supported by DPM 2010. However, the process was time consuming as it required the transfer of the entire database on a recovery point over the network to a staging location before you could recover an item.

System Center 2012 – Data Protection Manager (DPM) reduces the time and storage space required to restore an item by not requiring the entire database to be recovered and mounted, instead it attaches database files on the recovery point to a SQL Server instance remotely and recovers the item from the database.

This enhancement does not affect the protection or recovery of a SharePoint farm or database. For detailed steps on how to perform item-level recovery on SharePoint farms, see Recovering SharePoint Items.

Important

The SQL Server instance must run under an account that can be resolved by Active Directory services. This means that the SQL service must be running under a domain account, or under Local System or Network Service of the computer.

Warning

Item-level recovery must be performed in sequence one after the other. Parallel recoveries do not work.

This feature is available for farms on SharePoint 2007 and SharePoint 2010.

The following are not supported

- Filestream databases
- Tape recovery
- SharePoint sites using Variations.

Item-level recovery of Filestream items

You must set the following registry key on the DPM server to enable SharePoint item-level recovery for items in SQL Server Filestream content databases.

Key	HKLM\Software\Microsoft\Microsoft Data Protection Manager\Configuration\SharePoint
Value	AutoTriggerUnOptimizedILR
Data	
Type	DWORD

Note
When you try to recover a Filestream item, you will see a critical alert for recovery failure followed by an informational alert for a successful recovery. You should ignore the critical alert.

Forcing unoptimized recovery

DPM always tries optimized recoveries and switches to unoptimized if it is unable to do an optimized recovery. However, if unoptimized recovery is unable to start, set the following registry key and try the recovery. After the recovery is done, remove the registry entry.

Key	Software\Microsoft\Microsoft Data Protection Manager\Configuration\SharePoint
Value	DisableOptimizedILR
Data	1
Type	DWORD

Recovering SharePoint Search

With System Center 2012 – Data Protection Manager (DPM), you can backup and restore SharePoint Server Search service data created by Windows SharePoint Services 3.0 and MOSS 2007 Shared Services Provider (SSP).

In This Section

Recovering Windows SharePoint Services 3.0 SP Search Service Data

With DPM, you can back up and restore SharePoint Search service data created by Windows SharePoint Services 3.0.

Recovering Windows SharePoint Services 3.0 SP Search Service Data

You can recover SP Search data to either the original location or as individual files to an alternate location.

Important
The farm administrator should have administrator rights on the Indexing Service. If this is not the case, DPM is not able to stop the search service to ensure a proper recovery.

Recovering to original location

The procedure to recover SP Search data is similar to the recovery of any data source. You begin the recovery process from the DPM Administrator Console. This brings up the Recovery wizard which guides you through the process. The recovery process automatically deletes existing index files and resumes the SP Search service after the recovery is complete.

In the case of disaster recovery, you must configure SP Search with the original configuration of the latest recovery point before performing a recovery.

Recovering as files

1. Stop the SP Search service.
2. Delete the index files at the original location.
3. Restore the individual components (Search database and index files).
4. Perform a manual attachment of the database in SQL Server.
5. Start the SP Search service.

Recovering Microsoft Office SharePoint Server 2007 SSP Search

To recover Microsoft Office SharePoint Server 2007 SSP Search

1. Start the **Recovery** wizard from the DPM Administrator Console.
2. Select the point in time from which you want to recover data. The **Recovery** wizard displays the Shared Services Provider (SSP) components for the Microsoft Office SharePoint farm.

   Important
   If you recover the data to the original location, you must delete the SSP and its index files from the original location before you proceed with recovery. This must be done even if the default SSP uses the **-Force** parameter. The location details of these files are available on the **Summary** page of the **Recovery** wizard.
3. After the recovery process is completed, you must run RestoreSSP command on the protected computer with the **KeepIndex** parameter to ensure that the index file is not reset during the process of recreating the SSP.

To recover an index with mirrored database in Microsoft Office SharePoint Server 2007 SSP Search

If the SharePoint farm uses a mirrored database, you cannot recover the index to the original location. In this case, you must recover the individual components of the index and manually reattach them to the instance of the SQL Server.

1. Break the mirroring session of the mirrored SSP databases.
2. Start the **Recovery** wizard from DPM Administrator Console.
3. Select the point in time from which you want to recover data.
   The **Recovery** wizard displays SSP components for the SharePoint farm.
4. Recover the individual items to a temporary location and then host the databases to the instance of SQL Server manually.
5. Run the RestoreSSP command on the protected computer with the **KeepIndex** parameter to ensure that the index file is not reset during the process of recreating the

SSP.

See Also

Restoressp: Stsadm operation (Office SharePoint Server)

Performing SharePoint Protection Management Tasks

This section provides instructions and guidelines for managing a protected server running SharePoint and making changes after the initial System Center 2012 – Data Protection Manager (DPM) configuration.

In This Section

Changing the SharePoint Farm Administrator Password

When the SharePoint farm administrator password is changed, you have to rerun the ConfigureSharePoint.exe tool on the front-end Web server that is configured for SharePoint protection in System Center 2012 – Data Protection Manager (DPM). For more information about how to use ConfigureSharePoint.exe, see Using ConfigureSharePoint.

If you do not rerun ConfigureSharePoint.exe after changing the farm administrator password, SharePoint farm backups will continue with the following limitations:

- DPM will be unable to discover any changes in the SharePoint farm topology (for example, adding a new database or deleting an existing database).

- In DPM, the list of URLs in the SharePoint farm cannot be updated. Therefore, item-level recovery for newly added items will not be available for protection.
- Recovery of the complete farm content cannot be triggered from DPM. The databases must be recovered one by one.
- Databases in the farm cannot be recovered by using the **Recover to original Instance of SQL Server** option in the DPM Recovery Wizard. You can recover the databases to the original location by using the **Recover to any SQL Instance** option.
- The alert “DPM Alert – BackupMetaDataEnumeration Failed” is generated in DPM. See the **Details** pane for more information about the cause of this alert.

Adding a Database to a SharePoint Farm

When a database is added to a SharePoint farm, System Center 2012 – Data Protection Manager (DPM) will skip the backup of this database and continue to back up other databases in the SharePoint farm. It will mark the replica as inconsistent and alert the backup administrator.

DPM runs a task at night that automatically discovers the newly added databases and adds them to protection. If DPM is successful in adding the database to protection, then it creates a recovery point for the database and resolves the alert shown to the administrator.

DPM Alert- Farm Configuration Changed

This is a warning alert that is generated in DPM when automatic protection of the SharePoint database fails. See the alert **Details** pane for more information about the cause of this alert.

Recommended action

The following recommended actions associated with this alert are provided in the alert details:

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Display** pane, select the protection group for the SharePoint farm.
3. In the **Actions** pane, click **Modify protection group**. This starts the Modify Protection Group Wizard.
4. On the **Select Group Members** page, ensure that the node that corresponds to the SharePoint front-end Web server is marked for selection.
5. Complete the Modify Protection Group Wizard.
6. Run a consistency check for the SharePoint farm.

Removing a Database from a SharePoint Farm

When a database is removed from a SharePoint farm, System Center 2012 – Data Protection Manager (DPM) will skip the backup of that database, continue to back up other databases in the SharePoint farm, and alert the backup administrator.

DPM Alert - Farm Configuration Changed

This is a warning alert that is generated in DPM when automatic protection of a SharePoint database fails. See the alert **Details** pane for more information about the cause of this alert.

To resolve this alert, follow these steps:

1. Verify with the SharePoint administrator if the database has actually been removed from the farm. If the database has been removed from the farm, then it must be removed from active protection in DPM.
2. To remove the database from active protection:
    a. In DPM Administrator Console, click **Protection** on the navigation bar.
    b. In the **Display** pane, right-click the protection group for the SharePoint farm and then click **Stop Protection of member**.
    c. In the **Stop Protection** dialog box, click **Retain Protected Data**.
    d. Click **Stop Protection**.

You can add the SharePoint farm back for protection by using the Modify Protection Group Wizard.

Adding or Removing Servers in SharePoint Farm

System Center 2012 – Data Protection Manager (DPM) uses its protection agents to communicate with the servers that are member of the SharePoint farm. When you add new servers to the SharePoint farm which contains data that has to be backed up, ensure that DPM protection agents are installed on those servers.

DPM uses a single front-end Web server to protect the server farm. When you add other front-end Web servers or remove front-end Web servers other than the server used by DPM, there is no impact on protection of the farm.

To remove the front-end Web server that DPM is using while continuing protection of the server farm, see Switching the Front-End Web Server.

Switching the Front-End Web Server

To protect a server farm on servers running Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007, you start the Windows SharePoint Services VSS Writer service (SharePoint VSS Writer service) and install the DPM protection agent on a single front-end Web server. System Center 2012 – Data Protection Manager (DPM) uses this front-end Web server to perform backups.

The following procedure uses the example of a server farm with two front-end Web servers, Server1 and Server2. DPM uses Server1 to protect the farm. You need to change the front-end Web server that DPM uses to Server2 so that you can remove Server1 from the farm.

Note

If the front-end Web server that DPM uses to protect the farm is unavailable, use the following procedure to change the front-end Web server by starting at step 4.

To change the front-end Web server that DPM uses to protect the farm

1. Stop the SharePoint VSS Writer service on Server1 by running the following command at a command prompt:

   stsadm -o unregisterwsswriter
2. On Server1, open the Registry Editor and navigate to the following key:

   HKLM\System\CCS\Services\VSS\VssAccessControl
3. Check all values listed in the VssAccessControl subkey. If any entry has a value data of 0 and another VSS writer is running under the associated account credentials, change the value data to 1.
4. Install a protection agent on Server2.

   Caution

   You can only switch Web front-end servers if both the servers are on the same domain.
5. On Server2, at a command prompt, change the directory to *DPM installation location*\bin\ and run ConfigureSharepoint. For more information about ConfigureSharePoint, see Using Using ConfigureSharePoint.
6. There is a known issue when the server farm is the only member of the protection group and the protection group is configured to use tape-based protection. If your server farm is the only member of the protection group using tape-based protection, to change the front-end Web server that DPM uses to protect the farm, you must temporarily add another member to the protection group by performing the following steps:
   a. In DPM Administrator Console, click **Protection** on the navigation bar.
   b. Select the protection group that the server farm belongs to, and then click **Modify protection group**.
   c. In the Modify Group Wizard, add a volume on any server to the protection group. You can remove this volume from the protection after the procedure is completed.

d. If the protection group is configured for short-term disk-based protection and long-term tape-based protection, select the manual replica creation option. This avoids creating a replica for the volume that you are temporarily adding to the protection group.

e. Complete the wizard.

7. Remove Server1 from the protection group, selecting to retain the replicas on disk and tape.
8. Select the protection group that the server farm belongs to, and then click **Modify protection group**.
9. In the Modify Group Wizard, on the **Select Group Members** page, expand Server2 and select the server farm, and then complete the wizard.

   A consistency check will start.
10. If you performed step 6, you can now remove the volume from the protection group.

Upgrading SharePoint versions

If you upgrade an earlier version of Microsoft SharePoint to a later version, then you must reconfigure protection of the data.

The Microsoft SharePoint farm is updated in the following two scenarios:

- During SQL Server hardware upgrade
- When instances of SQL Server do not change

SQL Server hardware upgrade

If the hardware of the computer that runs the SQL Server is upgraded, then the databases are moved from one instance of the SQL Server to another. During the upgrade process, both farms are online, and the older farm is read-only (databases are moved in phases). You can protect the new SharePoint farm during the upgrade. To do this, perform the following steps:

1. Install the DPM protection agents on the new SharePoint farm servers.
2. Protect the SharePoint farm as a new SharePoint farm.
3. Move databases from the old farm to the new farm.

   Note
   DPM will automatically discover the databases that were moved in the new farm and will start to protect them. DPM generates a warning - **Farm Configuration Changed** for the old SharePoint farm. You can ignore this warning.
4. When all the databases are moved to the new server, perform **Stop protection** of the old SharePoint farm, by selecting the **retain data** option.

When instances of SQL Server do not change

When instances of SQL Server do not change, and databases are detached from the existing farm and are added to the upgraded farm, follow these steps:

1. Create a recovery point for the SharePoint farm on the DPM server. For example, DPMServer1.
2. Perform **Stop protection** of the SharePoint farm on DPMServer1 by selecting the **Retain Replica** option.
3. Run SetDPMServer.exe on all the servers of the SharePoint farm to point the DPM agent to another DPM server, for example, to DPMServer2.
4. Protect the SharePoint farm by using DPMServer2.
5. When the retention range for all the recovery points expires on DPMServer1, delete the protected data on DPMServer1 by using the **Remove Inactive Protection** option.

Moving SharePoint Servers Between Domains

You cannot do the following for protected computers:

- Change the domain of a protected computer and continue protection without disruption.
- Change the domain of a protected computer and associate the existing replicas and recovery points with the computer when it is re-protected.

We recommend that you do not change the domain of a protected computer. If you must change the domain of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection while the computer retains its original domain membership.
- Protect the data source on the computer after it becomes a member of another domain.

To change the domain membership of a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the domain membership of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

   For information about performing tasks involving protection agents and protection groups, see DPM Help.

Renaming a SharePoint Server

System Center 2012 – Data Protection Manager (DPM) uses the computer name as a unique identifier for replicas, recovery points, DPM database entries, reporting database entries, and so on.

You cannot:

- Change the name of a protected computer and continue protection without disruption.
- Change the name of a protected computer and associate the existing replicas and recovery points with the new computer name.

We recommend that you do not change the name of a protected computer. If you must change the name of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection (the old computer name).
- Protect the data source on the computer (the new computer name).

To rename a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data remains accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the name of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

   For information about tasks that involve protection agents and protection groups, see DPM Help.

Improving DPM Recovery Search for SharePoint Items

The time required for DPM Recoverable Object Search to return recovery points that meet the specified criteria will increase over time as the number of recovery points grow and the DPMDB gets more and more fragmented. You can improve the time taken by the search by carrying out regular maintenance on the DPMDB.
The following table lists the set of tables for which indexes need to be rebuilt for a specific data source. To improve the performance of the recovery point search for a data source, you need to rebuild or reorganize the indexes related to that data source.

Data source	Tables in DPMDB
SharePoint	tbl_RM_SharePointRecoverableObject tbl_RM_RecoverySource
Exchange Mailbox	tbl_RM_DatasetROMap tbl_RM_RecoverableObject tbl_RM_RecoverySource

Rebuilding Indexes

Rebuilding an index drops the index and creates a new one. In doing this, fragmentation is removed, disk space is reclaimed by compacting the pages using the specified or existing fill factor setting, and the index rows are reordered in contiguous pages (allocating new pages as needed). This can improve SQL query performance by reducing the number of page reads required to obtain the requested data.

Query to rebuild indexes

```
USE DPMDB
GO
ALTER INDEX ALL ON <tableName> REBUILD
GO
```

Reorganizing Indexes

Reorganizing an index defragments the leaf level of clustered and nonclustered indexes on tables and views by physically reordering the leaf-level pages to match the logical order (left to right) of the leaf nodes. Having the pages in order improves index-scanning performance. The index is reorganized within the existing pages allocated to it; no new pages are allocated. If an index spans more than one file, the files are reorganized one at a time. Pages do not migrate between files.

Reorganizing also compacts the index pages. Any empty pages created by this compaction are removed providing additional available disk space.

In some cases, the gain might not be significant. It is also a longer running operation compared to rebuilding the index.

Query to rebuild indexes

```
USE DPMDB
GO
ALTER INDEX ALL ON <tableName> REORGANIZE
GO
```

Rebuilding v/s Reorganizing – A Comparison

Rebuilding	Reorganizing
Takes the table whose indexes are being currently rebuilt offline. It should be done when it will least affect normal operations.	Keeps the table whose indexes are being currently reorganized online and working normally. Does not affect normal operations.
Substantial performance gains in search and browse operations.	Moderate performance gains in search and browse operations.
Not a time intensive operation.	Usually a time intensive operation.
Most effective when index is heavily fragmented.	Most effective when index is not heavily fragmented.

See Also

ALTER INDEX (Transact-SQL)

Performing General Maintenance on Servers Running SharePoint

General maintenance includes tasks such as disk and file maintenance, updating operating systems and applications, and protecting data by using antivirus software and performing regular backups. Some special considerations apply when you are performing server maintenance on computers running SharePoint that are protected by System Center 2012 – Data Protection Manager (DPM).

When you need to perform maintenance on a protected server and do not want protection jobs to continue for the duration of the maintenance, you can disable the protection agent.

To disable a protection agent

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. On the **Agents** tab, in the display pane, select the name of the computer with the protection agent you want to disable.
3. In the **Actions** pane, click **Disable protection agent**.
4. In the dialog box, click **OK** to confirm that you want to proceed.

In This Section

Performing SharePoint Protection Management Tasks

Performing SharePoint Maintenance Tasks

If you schedule automatic deletion of inactive Web sites, coordinate the automatic deletion schedule with the protection schedule to ensure you have a recent copy of the site backed up.

Troubleshooting SharePoint Protection and Recovery

This topic documents the following known issues and resolutions relating to protection and recovery of SharePoint data protected by System Center 2012 – Data Protection Manager (DPM):

- Unable to search SharePoint items in the Recovery task area.
- SharePoint farm protection fails with ID 956
- Recovery of a SharePoint content database fails with ID 0x80070003
- On a secondary DPM server (DPM-DR), even though incremental and express full jobs happen successfully for a SQL Server database that belongs to a SharePoint farm, recovery points are not displayed in the Recovery task area and no alerts are triggered
- SharePoint documents checked out or in the recycle bin during backup cannot be restored
- DPM Protection Report shows incorrect data for SharePoint farms
- SharePoint protection not working properly
- SharePoint site or item recovery fails when a shared folder is used as a temporary location
- SharePoint farm protection fails with ID 30111
- SharePoint index backups fail during profile import
- ConfigureSharepoint.exe fails with error code 997

Unable to search SharePoint items in the Recovery task area.

In DPM, to search for SharePoint items such as list items in the Recovery task area, follow these steps:

1. On the **Search** tab, in the **Search** list, select **SharePoint**.
2. In the **SharePoint search** pane, click **Search Documents**.
3. In the **Name** list, select **Contains** as the search string.
4. Enter the name of the list item you want to recover.

Note

- To search list items, you must select only **Contains** as the search string.
- Ensure that you have selected the correct SharePoint farm name.

SharePoint farm protection fails with ID 956

This happens when in the SharePoint farm, the name of the SQL Server is not configured as a fully qualified domain name (FQDN), and only a NETBIOS name is provided. To resolve this issue, reconfigure the SharePoint server with the FQDN of the SQL Server by running the command **Stsadm –o renameserver** on the front-end Web server from where you plan to protect the SharePoint farm data.

Recovery of a SharePoint content database fails with ID 0x80070003

When rebuilding the primary DPM server from the secondary DPM server data, one of the old recovery points shows databases that were not backed up. To resolve this issue, try to recover that database from another recovery point that might be older or newer.

On a secondary DPM server (DPM-DR), even though incremental and express full jobs happen successfully for a SQL Server database that belongs to a SharePoint farm, recovery points are not displayed in the Recovery task area and no alerts are triggered

In a DPM primary server, if you are protecting a SQL Server database that belongs to a SharePoint farm, then ensure that you do not protect that database independently on the secondary DPM server. To resolve this issue, you must identify all such databases, perform Stop protection with the delete data option, and then re-protect the SharePoint farm.

SharePoint documents checked out or in the recycle bin during backup cannot be restored

In SharePoint, if documents were checked out from the documentation library or were located in the first or second stage of the recycle bin during the time your data was backed up, they cannot be restored. To restore these documents, you must pick a point in time at which the documents were not checked out or in the recycle bin before restoring the data.

DPM Protection Report shows incorrect data for SharePoint farms

DPM does not calculate the expected number of recovery points correctly in the DPM Protection Report. Therefore the percentage that shows the historical recovery point availability against the existing recovery points is incorrect.

SharePoint protection not working properly

If you are having trouble continuing protection of a SharePoint site that is already part of a protection group after adding a content database, check to see if you have met all the DPM prerequisites for protecting Microsoft SQL Server 2005. In the process of adding a content database for protection, DPM may implicitly protect the back-end SQL database without validating the prerequisites.

SharePoint site or item recovery fails when a shared folder is used as a temporary location

When a shared folder is specified as the temporary location for the recovery of a SharePoint site or item the recovery will fail. To resolve this issue, use a local folder as the temporary location for either the recovery farm or the production farm.

SharePoint farm protection fails with ID 30111

If your SharePoint farm protection is failing with the ID 30111 error on the **Jobs** tab in the **Monitoring** pane in DPM Administrator Console, it could be because there is a volume with no mount points on the front-end Web server of your SharePoint farm. To resolve this issue, assign a mount point or drive letter to the dismounted volume and perform a consistency check.

SharePoint index backups fail during profile import

Due to constraints in SharePoint, DPM cannot pause a profile import. Backups scheduled to run when a profile import is taking place will fail. The backups fail with error code 32010.
Message: **DPM was unable to get the Content Sources of the SSP <Name of data source>; to a consistent state.**
Recommended action:

- Check to see that the protected SSP is online and running.
- Check to see that the WSSCmdletWrapper DCOM component is configured correctly on the front-end Web server hosting the protected farm.
- Retry the operation and make sure no other application or process is trying to resume the crawl of the SSP during backup.

ConfigureSharepoint.exe fails with error code 997

If this is happening after you have changed the administrator password, do the following to resolve the issue:

1. From the command prompt, run **dcomcnfg**.
2. In the DCOM Config utility, search for the WSSCmdletWrapper object. Right-click the object and select **Properties**.
3. On the **Identity** tab, enter the new password.

Protecting Virtual Servers

This section provides guidance on performing common maintenance tasks on protected servers. It also provides guidance on making changes to the computer configuration after the computer is protected by System Center 2012 – Data Protection Manager (DPM).

For in depth information about how DPM protects virtualized environments, see the Protect Your Windows Virtual Environment with System Center Data Protection Manager TechNet Webcast.

In This Section

Performing Virtual Server Management Tasks

This section provides instructions and guidelines for managing a protected virtual server and making changes after the initial DPM configuration.

In This Section

Moving Virtual Servers Between Domains

You cannot do the following for protected computers:

- Change the domain of a protected computer and continue protection without disruption.
- Change the domain of a protected computer and associate the existing replicas and recovery points with the computer when it is re-protected.

We recommend that you do not change the domain of a protected computer. If you must change the domain of a protected computer, you must complete two tasks:

- Remove the data sources on the computer from protection while the computer retains its original domain membership.
- Protect the data source on the computer after it becomes a member of another domain.

To change the domain membership of a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for end-user recovery.
2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the domain membership of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

How to Rename Virtual Servers

System Center 2012 – Data Protection Manager (DPM) uses the computer name as a unique identifier for replicas, recovery points, DPM database entries, reporting database entries, and so on.

You cannot:

- Change the name of a protected computer and continue protection without disruption.
- Change the name of a protected computer and associate the existing replicas and recovery points with the new computer name.

We recommend that you do not change the name of a protected computer. If you must change the name of a protected computer, you must:

- Remove the data sources on the computer from protection (the old computer name).
- Protect the data source on the computer (the new computer name).

To rename a protected computer

1. Remove all members from protection groups.

   If you retain the replicas and recovery points, the data will remain accessible for administrative recovery until you delete the replicas. However, it will not be accessible for

end-user recovery.

2. Uninstall the protection agent by using DPM Administrator Console on the DPM server.
3. Change the name of the computer.
4. Install a protection agent by using DPM Administrator Console on the DPM server.
5. Add the data sources to protection groups on the DPM server.

Renaming Virtual Machines

Renaming a virtual machine changes the name of the virtual machine configuration (.vmc) file, the virtual machine name shown in the Administration Web site, and the display name of the virtual machine window, but not the name of the folder containing the virtual machine.

If you change the name of a virtual machine that is protected as a guest on a Virtual Server, System Center 2012 – Data Protection Manager (DPM) continues protection and captures the change as it does any other change to protected data.

Moving a Virtual Machine or Virtual Hard Disk

Moving a Virtual Machine

To move a virtual machine that is protected by DPM

1. Copy the virtual machine to the new host. For instructions, see Copying, managing, and renaming virtual machines.
2. Add the copied virtual machine to a protection group.
3. Remove the original virtual machine from the original host. For instructions, see Removing virtual machines.
4. Stop protection of the original virtual machine.

Moving a Virtual Hard Disk

You might want to move a virtual hard disk to store a large amount of data or improve disk performance. A virtual hard disk for a virtual machine is stored as a .vhd file. To continue protection of a virtual hard disk that is moved to a new volume, run the Modify Group Wizard for the protection group to which it belongs, and then run a consistency check.

Protecting Application Data on Virtual Machines

When you add a virtual machine to a protection group, you are protecting the complete configuration of the virtual machine, including operating system, applications, and application data. However, you cannot specifically recover application data from the recovery points for the virtual machine; you can only recover the entire virtual machine. When you recover the virtual machine, applications are recovered with all data that was present at the time that the recovery point was created.

It is not necessary to install a DPM protection agent on a virtual machine to protect it as a virtual machine on the Virtual Server host.

To recover only application data for applications running in virtual machines, you must install a protection agent on the virtual machine and select the application data explicitly as a protection group member.

You can protect both the virtual machines as guests on the Virtual Server host and the application data within the virtual machines as applications.

Recovering Virtual Server Data

In This Section

How to Recover the Virtual Server Host

When you protect a Virtual Server host and its virtual machines, the recoverable items are the Virtual Server configuration and each virtual machine. You should recover the Virtual Server configuration before you recover the individual virtual machines.

To recover a virtual machine

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Browse or search for the virtual server name you want to recover, and then select the data in the results pane.
3. Select the bold date for the recovery point you want to recover. Available recovery points are indicated in bold on the calendar in the recovery points section.

4. In the **Recoverable item** pane, click the Virtual Server configuration item.
5. In the **Actions** pane, click **Recover**. The Recovery Wizard starts.
6. Review your recovery selection, and then click **Next**.
7. Select **Recover to original instance**, and then click **Next**. The current files will be overwritten during recovery.
8. Specify your recovery options, and then click **Next**. The following recovery options are available:
   a. Select **Enable SAN-based recovery using hardware snapshots** to use SAN-based hardware snapshots for quicker recovery.

      This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.
   b. In the **Notification** area**,** click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
9. Review your recovery settings, and then click **Recover**.

See Also

How to Recover a Virtual Machine

How to Recover Virtual Machines as Files

How to Recover a Virtual Machine

When you protect a Virtual Server host and its virtual machines, the recoverable items are the Virtual Server configuration and each virtual machine. You should recover the Virtual Server configuration before you recover the individual virtual machines.

When you recover the virtual machine, applications are recovered with all data that was present at the time that the recovery point was created.

To recover a virtual machine

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Browse or search for the virtual machine name you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the virtual machine item you want to recover.
5. In the **Actions** pane, click **Recover**. DPM starts the Recovery Wizard.

6. Review your recovery selection, and then click **Next**.
7. Select **Recover to original instance**, and then click **Next**. The current files will be overwritten during recovery.
8. Specify your recovery options, and then click **Next**.
    a. Select **Enable SAN-based recovery using hardware snapshots** to use SAN-based hardware snapshots for quicker recovery.

       This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.
    b. In the **Notification** area**,** click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
9. Review your recovery settings, and then click **Recover**.

See Also

How to Recover the Virtual Server Host

How to Recover Virtual Machines as Files

How to Recover Virtual Machines as Files

You can recover the Virtual Server configuration and virtual machines as files to a network folder, enabling you to copy those files to an alternate Virtual Server host.

The following files are recovered to the network folder:

- For the Virtual Server configuration, options.xml
- For each virtual machine, all associated .vhd, .vmc, and .vsv files

When you restore a virtual machine to a network folder and then copy the files to a new Virtual Server host and start the virtual machine, you may see an error message that the server shut down unexpectedly. This can occur because DPM cannot mark the recovery files as an expected shutdown. The recovered files are otherwise application-consistent.

When the .vhd file for a virtual machine is stored in the root of a volume and you recover the virtual machine to an alternate location as files, the .vhd file will be recovered with directory attributes set to hidden and system. To view the recovered .vhd file, you must remove the directory attributes.

To recover virtual machines as files

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Using either the browse or search functionality, select the storage group to recover.

3. On the calendar, click any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point.
4. On the **Recovery time** menu, select the recovery point you want to use.
5. In the **Actions** pane, click **Recover**.

   The Recovery Wizard starts.
6. On the **Review recovery selection** page, click **Next**.
7. Select **Copy files to network location**, and then click **Next**.
8. On the **Specify destination** page, specify the network folder to which the files should be copied.
9. Specify your recovery options:
   a. Select **Apply security settings of the destination computer** or **Apply the security settings of the recovery point version**.
   b. Select **Enable SAN-based recovery using hardware snapshots** to use SAN-based hardware snapshots for quicker recovery.

      This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create and split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.
   c. In the **Notification** area, click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
10. On the **Summary** page, review the recovery settings, and then click **Recover**.

See Also

How to Recover the Virtual Server Host

How to Recover a Virtual Machine

Protecting Computers with DPM

System Center 2012 – Data Protection Manager (DPM) allows you to protect your data on client computers. Client computers include desktop computers that are connected to the network, and laptop and notebook computers that are intermittently connected to your corporate environment. Backup administrators can centrally configure data protection for the client computers in their environment using the DPM Client. Additionally, administrators can give their end users the ability to define and manage their own backups. DPM enables end users to perform their own recoveries by leveraging the Previous Versions feature in Windows.

Laptop and notebook computers will not be connected to the network at all times and the number of protected client computers can be much larger than the number of protected file servers.

These scenarios have resulted in the following changes about how DPM manages client computer protection.

- The administrator can configure protection for the client computer that they want to protect without being online. We recommend that administrators use software distribution mechanisms such as Microsoft System Center Configuration Manager to install and configure the DPM protection agent.
- The client computer polls the DPM server at 15 minute intervals and obtains the backup schedule that the administrator specifies for the protection group. The client computer starts the backup according to the schedule, or by user demand. Alternatively, once the administrator configures a protection group that allows the end user to specify their protected data items, the end user can start a backup at any time from the DPM Client.
- DPM will not show alerts for client computers that usually appear for protected servers. These alerts pertain to failures of individual jobs. For example, a synchronization failure alert will not appear for the DPM administrator to act upon for any of the failed synchronizations. This is because client computers are designed to retry the synchronization in the event of a failure. However, DPM allows you to configure DPM to alert the end user if a client computer has not been backed up for a predefined number of days that the administrator defined when they created the protection group.

In This Section

Client Computer Operating System Requirements

Before protecting your client computers, you must ensure that the following prerequisites are installed on the client computer.

Client Computer Operating System Requirements

Each System Center 2012 – Data Protection Manager (DPM) server can protect up to 3000 client computers that are running either the 32-bit or 64-bit versions of the following operating systems:

- Windows XP with Service Pack 2 (SP2)

Note
Recovery from previous versions of files and folders is not supported on computers running Windows XP.

- Windows Vista or Windows Vista with Service Pack 1 (SP1)
- Windows 7
- Windows 8

Network Requirements

The following sections describe the network requirements for DPM when you are working with various types of client computer connections

Protection across domains

The client computers that you want to protect must have a two-way trust relationship with the domain in which the DPM server is located.

Client computers behind a firewall

If Windows Firewall is configured on the client computer, the DPM protection agent installation will configures the necessary firewall exceptions. If you need to reset the firewall, you can reconfigure it by running SetDpmServer.exe. If you are using a firewall other than Windows Firewall, ensure that the necessary ports for DPM are open.

Client computers over a VPN connection

DPM can perform backups of client computers that are using a virtual private network (VPN) connection.

Note
For backups of client computers that are intermittently connected to the network, and that are expected to connect over a VPN, we recommend that your Internet connection speed be a minimum of 1 Megabit per second (Mbps).

DPM supports the following VPN protocols:

- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Tunneling Protocol (SSTP)
- Layer 2 Tunneling Protocol (L2TP)

Important
To perform backups over a VPN, you must enable Internet Control Message Protocol (ICMP). For more information, see How to enable ICMP traffic from protected SecureNet clients to external hosts in ISA Server 2006 and ISA Server 2004.

Client computers that are always connected to the network

DPM can perform backups of client computers that are either physically or wirelessly connected to the local area network (LAN). For client computers that are continuously connected to the network, ensure that sufficient bandwidth is available for DPM. We recommend a minimum network bandwidth of 256 Kilobits per second (Kbps) for computers that are continuously connected to the network.

Installing Protection Agents

System Center 2012 – Data Protection Manager (DPM) provides several methods to install protection agents on computers with data sources that you want to protect, by using both automated and manual processes. For more information about installing protection agents, see Installing Protection Agents.

Protecting Client Computer Data

You can use the Create New Protection Group Wizard to guide you through the process of protecting your client computer data.

Note that System Center 2012 – Data Protection Manager (DPM) allows you to create a protection group without having to attach the client computers to DPM from the Management task area in DPM Administrator Console. DPM will automatically attach the client computers if they are not already attached.

In This Section

Creating a Protection Group on the Client Computer

Adding a Client Computer and Modifying Disk Allocation

Creating a Protection Group on the Client Computer

To add a client computer using the Create New Protection Group Wizard

1. On the **Welcome** page, click **Next**.
2. On the **Select Protection Group** page, select **Clients**, and then click **Next**.
3. On the **Select Group Members** page, select the computers you want to protect from the list box. Click **Add** to move the computers to the **Selected computers** list box, and then click Next. When selecting the computers you want to protect, note the following:

- If you want to add multiple computers, you can create a .txt file containing the computers you want to add. To add the computers, click **Add Multiple Computers**. You must enter each computer in the file on a new line. We recommend that you provide the fully qualified domain name (FQDN) of the target computers. For example, enter multiple computers in a .txt file as follows:

  Comp1.abc.domain.com

  Comp2.abc.domain.com

  Comp3.abc.domain.com

- If DPM cannot find any of the computers that you specified in the .txt file or that you entered in the **Text file location** box, the failed set of computers is placed in a log file. Click the **Failed to add machines** link at the bottom of the page to open the log file.

4. On the **Specify Inclusions and Exclusions** page, specify the folders to include or exclude for protection on the selected computers. To select from a list of well-known folders, such as **Documents**, click the drop-down list.

   When specifying inclusions and exclusions, note the following:

   - When you exclude a folder, and then specify a separate inclusion rule for a subfolder, DPM does not backup the subfolder. The exclusion rule overrides the inclusion rule.
   - When you include a folder, and then specify a separate exclude rule for a subfolder, DPM backs up the entire folder, except for the excluded subfolder.
   - When you include a well-known folder such as **Documents**, DPM locates the **Documents** folder for all users on the computer, and then applies the rule. For example, if the user profile for computer **Comp1** contains the **Documents** folder for both User1 and User2, DPM will back up both folders.

   a. Type the folder names in the **Folder** column using variables such as *programfiles*, or you can use the exact folder name. Select **Include** or **Exclude** for each entry in the **Rule** column.
   b. Select **Allow users to specify protection members** to give your end users the choice to add more folders on the computer that they want to back up. However, the files and folders you have explicitly excluded as an administrator cannot be selected by the end user.
   c. Under **File type exclusions** specify the file types to exclude using their file extensions, and then click **Next** to continue.

      Figure 1 shows an example of how you can use the **Specify Inclusions and Exclusions** page to include and exclude specific folders. In this example the **My Documents** folder is selected for protection and the **Temporary Internet Files** folder is excluded from protection.

      <Placeholder for graphic>

5. On the **Select Data Protection Method** page, in the **Protection Group Name** box, type a name for the protection group.
6. In the **Protection method** section, select if you want to use short-term disk-based protection or long-term tape-based protection. Click **Next** to continue.

   Note
   DPM supports short-term disk-based protection for desktop and laptop computers, as well as long-term tape-based protection. DPM does not support short-term tape-based backup for desktop and laptop computers.
7. On the **Specify Goals** page, specify your protection goals such as retention range and synchronization frequency. Select the **Alerting option** to receive alerts when the recovery points fails for the selected number of days, and then click **Next**.
8. On the **Allocate Storage** page, specify the size of data to be protected on the computer. We recommend that you co-locate multiple data sources to one DPM replica volume.

   Note
   We recommend that you co-locate your data if you have a large number of client computers. You will not be able to protect 1000 or more client computers with one DPM server without co-locating your data. We recommend that you do not co-locate if you have less than ten client computers in a protection group.
9. Select the **Automatically grow the volumes** check box to automatically grow volumes when more disk space is required for protecting data on the client computers. Click **Next** to continue.
10. On the **Summary** page, review your selections and then click **Create Group** to complete the wizard.

Adding a Client Computer and Modifying Disk Allocation

You can add a client computer by modifying the protection group to reduce the number of steps required to add the client computer.

To add the client computer

1. Right-click an existing protection group for the client computer.
2. Select **Add client computers**.

   A page appears allowing you to select and add new client computers.
3. Click **Next** to add the client computers to the protection group.

To modify disk allocation

1. Right click an existing protection group for the client computer.
2. Select **Modify disk allocation**.

   A page appears allowing you to change the disk allocation for each client computer.

Recovering Client Computer Data

System Center 2012 – Data Protection Manager (DPM) gives administrators the ability to enable their end users to perform their own recoveries by leveraging the Previous Versions feature in Windows. If you do not want to provide this capability to your end users, you recover the data for desktop computers using the following procedures in the Recovery Wizard.

To recover protected data for desktop computers

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Browse or search for the data you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
5. In the **Actions** pane, click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.
7. Specify the type of recovery you would like to perform:
   a. **Recover to the original location**.

      Warning
      If a client computer is connected over a Virtual Private Network (VPN), the recovery will fail. We recommend that you restore the data to an alternate location (such as a share), and then provide that share to the end user so they can copy their data.

   b. **Recover to an alternate location**. Click **Browse** to browse for an alternate recovery destination. On the **Specify Alternate Recovery Destination** dialog box, select the recovery destination and click **OK**.
   c. **Copy to tape**. This option copies the volume that contains the selected data to a tape in a DPM library. Click **Next**, and on the **Specify Library** dialog box, select library details and tape options. You can also choose to compress or encrypt the data on tape.
8. Click **Next** after you have specified one of the preceding options.
9. Specify your recovery options:
   a. **Existing version recovery behavior**. Select **Create copy**, **Skip**, or **Overwrite**. This option is enabled only when you selected **Recover to the original location** in step 7.

b. **Restore security**. Select **Apply settings of the destination computer** or **Apply the security settings of the recovery point version**.

c. **Network bandwidth usage throttling**. Click **Modify** to enable network bandwidth usage throttling.

d. **Enable SAN based recovery using hardware snapshots**. Select this option to use SAN-based hardware snapshots for quicker recovery.

   This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.

e. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.

10. Click **Next** after you have made your selections for the preceding options.
11. Review your recovery settings, and click **Recover**.

Note
Any synchronization job for the selected recovery item will be canceled while the recovery is in progress.

Performing Client Computer Management Tasks

This topic provides instructions and guidelines for managing a protected client computer and making changes after the initial configuration.

In This Section

Using the Disk Utilization Report

Optimizing Client Computer Performance

Scaling up Client Protection

Using the Disk Utilization Report

System Center 2012 – Data Protection Manager (DPM) provides backup administrators with a Disk Utilization Report they can use to see how much disk space is being used by their end users. The report provides a summary view of disk capacity, disk allocation, and disk space

usage for replicas and shadow copy volumes. The data is collected for all client computers per protection group.

Backup administrators can use the Disk Utilization Report to identify the following:

- Current disk usage.
- Users that backup more data than estimated.
- Disk space usage history for estimating data growth and future investments in disk space.

For more information about how to use DPM reports, see Using Reports.

Optimizing Client Computer Performance

On some client computers, you may notice the computer running slow when a backup is in progress. You can improve the computer's responsiveness by setting the following registry key DWORD.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent\ClientProtection
Value	WaitInMSPerRequestForClientRead
Data	50
Type	DWORD

Scaling up Client Protection

You can improve the performance of the System Center 2012 – Data Protection Manager (DPM) server protecting client computers by setting appropriate registry keys.

Scaling up Client Protection

As the number of clients protected on a DPM server increases, you can optimize the performance of the computer by setting a few registry keys.

For task throttling:

Key	Software\Microsoft\Microsoft Data Protection Manager\Configuration\DPMTaskController\MaxRunningTasksThreshold
Value	9037ebb9-5c1b-4ab8-a446-052b13485f57

Data	50
Type	DWORD

Key	Software\Microsoft\Microsoft Data Protection Manager\Configuration\DPMTaskController\MaxRunningTasksThreshold
Value	3d859d8c-d0bb-4142-8696-c0d215203e0d
Data	100
Type	DWORD

Key	Software\Microsoft\Microsoft Data Protection Manager\Configuration\DPMTaskController\MaxRunningTasksThreshold
Value	c4cae2f7-f068-4a37-914e-9f02991868da
Data	50
Type	DWORD

To improve the collocation factor:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Collocation\Client
Value	DSCollocationFactor
Data	30
Type	DWORD

Client Auto Deployment Management Pack

In environments that have many computers, administering the protection of laptop computers can be a very cumbersome process. System Center 2012 – Data Protection Manager (DPM) enables you to automate the deployment and protection of laptop computers by using System Center Operations Manager 2008 R2.

In This Section

Introduction to Client Auto Deployment Management Pack

Introduction to Client Auto Deployment Management Pack

System Center 2012 – Data Protection Manager (DPM) client protection auto-deployment is enabled through System Center Operations Manager 2008 R2 and System Center Configuration Manager. The auto-deployment solution is essentially a management pack with added capabilities.

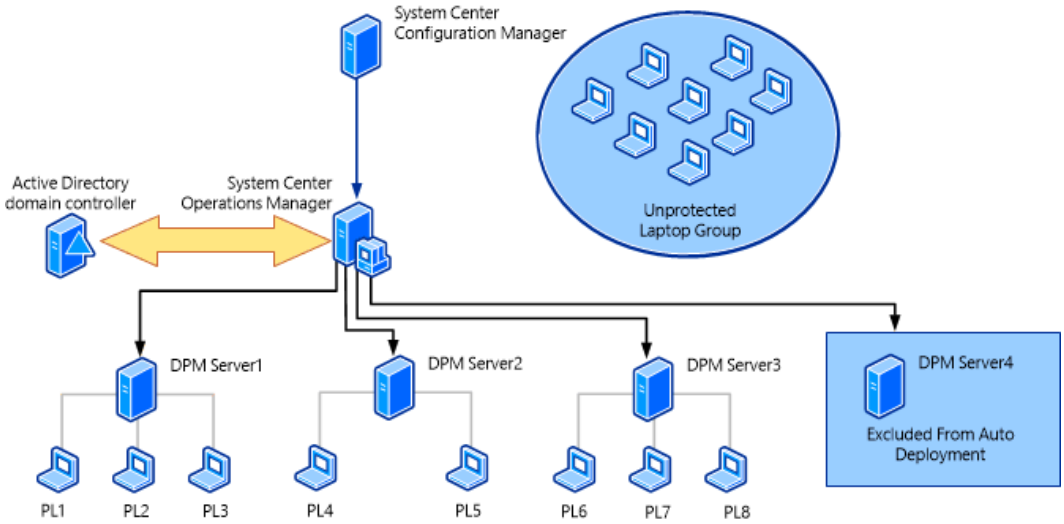
The Parts

The Operations Manager server: Download and install ClientAD.msi on the Operations Manager server on which auto protection will be enabled. The management pack is part of the installation and must be imported for monitoring auto protection status. Download and install the client protection auto-deployment management pack and binaries on this computer.

The DPM servers: Install the Operations Manager agents on these computers and from the Operations Manager console, enable client auto-deployment.

The Laptop computers: When the computer connects to the network, DPM will automatically back up its data.

Topology



Process Overview

To use the auto-deployment solution Download and install ClientAD.msi on the Operations Manager server on which auto protection will be enabled (Download Client Auto Deployment management pack and related binaries) and install it on an Operations Manager server. The management pack is part of the installation and must be imported for monitoring auto protection status. Next, you must install the Operations Manager agents on the DPM servers that you want to use to protect laptop computers. This will make the DPM servers discoverable by the Operations Manager server. This is a repetitive process and Operations Manager will run this query once every 24 hours.

After it has discovered at least one DPM server, the Operations Manager server will make a list of all laptop computers in the protected domains on DPM servers on which auto-protection is enabled (How to configure domains to be protected). This discovery process and runs at regular intervals. The Operations Manager then compares the list of laptop computers with the list of protected and excluded computers and creates a list of the ones that require to be protected but are not yet part of a protection group. Using this list, Operations Manager will then create protection groups assigning a maximum of 100 laptop computers per DPM server per day.

When a laptop computer connects to the network, System Center Configuration Manager will install the DPM protection agent on the computer and assign it to the appropriate DPM server.

After a computer has been added to a protection group, DPM will trigger backups based on the protection intent specified.

How auto deployment works

- Discover DPM servers in the environment.
- Discover protected clients under each DPM server.
- Include one or more DPM servers for auto deployment. Add/Remove DPM Server from Client Auto Deployment
- Exclude one or more DPM servers from auto deployment. Add/Remove DPM Server from Client Auto Deployment
- Specify the maximum DPM capacity for protecting client machines (default is 1000). Setting DPM Server Capacity for Client Auto Deployment
- Discover client machines from active directory domain services for the specified domains.
- Specify client exclusions. How to configure exclusions
- Specify default protection group settings for auto deployment. How to configure protection groups
- Filter protected clients and create batches of client machines for protection on each DPM.
- Auto-protect clients on all DPM servers every day.
- Identify successful/failed clients for each assignment from DPM server’s event log.

Views

The DPM Client Auto Deployment management pack provides the following views on the Operations Manager console:

View Name	Description
Auto deployment alerts	Alerts caused by auto deployment operations such as AD query failed, Auto protection failed due to System Center Operation Manager reboot, and so on.
Auto deployment DPM server state	All the DPM servers discovered with details such as DPM Version, Available free capacity, Included/excluded status, and so on.
Auto deployment server state	State of auto deployment server.
DPM server alerts	Alerts specific to auto protection of a DPM server such as Create protection group failure, SLA threshold not met, and so on.
Protected clients state	View of all protected clients in different DPM servers.
Stale clients state	View of client computers that have not been backed up for 90 days (by default) or the period specified by the administrator.

Prerequisites for Client Auto Deployment Management Pack

In order to use the auto-deployment feature for client computers, you need the following:

- System Center Operations Manager 2007 R2.
- Auto-deployment for Client Computer Protection management pack and binaries.
- System Center Configuration Manager.

Setting up Client Auto Deployment

How to enable client auto deployment

1. Install ClientAD.msi on the Operations Manager server.
2.

On the Operations Manager server

   a. Configure the domains to be protected. How to configure domains to be protected
   b. Configure the exclusions. How to configure exclusions
   c. Configure the protection groups. How to configure protection groups
   d. Import the management pack. How to Import a Management Pack in Operations Manager 2007

3.

On the DPM server

   a. Install DPM update DataProtectionManager2010-KB2465832. Download KB 2465832
   b. Add disks to the DPM server. Adding Disks to the Storage Pool

4.

On the Operations Manager console

   a. Install the Operations Manager agents on the DPM server. Process Manual Agent Installations in Operations Manager 2007
   b. Include the DPM servers to be used for client protection. Add/Remove DPM Server from Client Auto Deployment

5.

On the System Center Configuration Manager server

   a. Download the System Center Configuration Manager integration program.
   b. Open an elevated command prompt and run the following command: **SCCMClientAD.exe –s** <Time of daily run> <Day of global run> <Share path> <Configuration Manager site code>.

How to configure domains to be protected

1. Open the file **DomainsForAutoDeployment.txt** from \Program Files\Microsoft Data Protection Manager\Auto Deployment\Config on the System Center Operations Manager server.
2. Add new line separated entries for the domains from which you want to protect laptop computers.

   Note
   Wildcard characters are supported. For example. XP*.corp.contoso.com includes protection of all clients whose name starts with word ‘xp’ in the domain corp.contoso.com

How to configure exclusions

1. Open the file **Exclusions.txt** from \Program Files\Microsoft Data Protection Manager\Auto Deployment\Config on the System Center Operations Manager server.
2. Add new line separated client system FQDNs for clients which you don’t want to perform auto protection.

   Note
   Wildcard characters are supported. For example. XP*.corp.contoso.com excludes protection of all clients whose name starts with word ‘xp’ in the domain corp.contoso.com

How to configure protection groups

1. Open the file **ClientPGSettings.xml** from \Program Files\Microsoft Data Protection Manager\Auto Deployment\Config on the System Center Operations Manager server. This file has the default settings with which a protection group is created.
2. Edit the details here such as per laptop size, and so on, to set new settings.

   Note
   All protection groups created for all DPM servers involved in auto protection will be of this configuration.

Using DPM 2010 Client Auto Deployment Management Pack

In this section, the various actions you can perform on the System Center 2012 – Data Protection Manager (DPM) servers by using the Client Auto Deployment management pack are described.

In This Section

Add/Remove DPM Server from Client Auto Deployment

How to add a DPM server for client auto deployment

1. On the System Center Operations Manager console, go to the **Monitoring** view, expand **DPM Client Auto Deployment**, and then select **Auto deployment DPM server state**.
2. On the main pane, select the DPM server you want to include. On the **Actions** pane, click **Include DPM for auto deployment**.

How to remove a DPM server from client auto deployment

1. On the System Center Operations Manager console, go to the **Monitoring** view, expand **DPM Client Auto Deployment**, and then select **Auto deployment DPM server state**.
2. On the main pane, select the DPM server you want to remove. On the **Actions** pane, click **Exclude DPM for auto deployment**.

Setting DPM Server Capacity for Client Auto Deployment

By default, each DPM server is set at a capacity of 1000. This means it can protect up to 1000 clients.

How to change DPM server capacity

To change the number of client computers a DPM server can be allotted, use the following DPM Management Shell cmdlet:

Set-DPMGlobalProperty –Dpmservername <DPMServer> **-MaxCapacityForClientAutoDeployment** <NewCapacity>

Changing Protection Group Settings through Client Auto Deployment

System Center 2012 – Data Protection Manager (DPM) Client Auto Deployment allows the administrator to modify the protection group settings for all protection groups created by Client Auto Deployment. You can do this by editing ClientPGSettings.xml and then applying the changes to all of the DPM servers or for selected ones. For more information about how to configure ClientPGSettings.xml, see Setting up Client Auto Deployment.

How to apply protection group changes to all DPM servers included for Client Auto Deployment

1. On System Center Operations Manager console, go to the **Monitoring** view, expand **DPM Client Auto Deployment**, and then click **Auto deployment server state**.
2. Select a System Center Operations Manager server from the main pane.
3. On the **Actions** pane, click **Apply modified PG settings**.
4. On the **Run task** dialog box, click **Run**.

   The changes will be applied to all protection groups created by DPM Client Auto Deployment on all DPM servers included for Client Auto Deployment.

How to apply protection group changes to selected DPM servers

1. On System Center Operations Manager console, go to the **Monitoring** view, expand **DPM Client Auto Deployment**, and then click **Auto deployment server state**.
2. Select a System Center Operations Manager server from the main pane.
3. On the **Actions** pane, click **Apply modified PG settings**.
4. On the **Run task** dialog box, click **Override**.
5. On the **Override Task Parameters** dialog box, provide a comma-separated list of DPM FQDN in the **New Value** text box.
6. Click **Override**.
7. Click **Run**.

Managing Stale Clients

A stale client is a client computer which has been added to a protection group by DPM Client Auto Deployment and has not been backed up for the period specified by the administrator. The default period is 90 days. However, this value can be changed in the registry.

Changing default threshold for marking a client computer as stale

Key	HKLM\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Configuration\Client
Value	StaleClientThresholdInDays
Data	Numeric value of number of days
Type	DWORD

Stopping protection of stale client computers

Key	HKLM\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Configuration\Client
Value	StopProtectStaleClients
Data	1 to stop protection 0 to continue protection
Type	DWORD

Protecting Hyper-V Virtual Machines

Data Protection Manager (DPM) in System Center 2012 provides continuous data protection for virtual machines that are hosted on servers that run Microsoft Hyper-V. This section provides an overview of DPM scenarios for Hyper-V protection and instructions to set up protection.

- System Center 2012 SP1 improvements
- DPM protection overview
- Backup overview
- Prerequisites for virtual machine protection
- Protecting virtual machines in clusters with CSV storage
- Protecting virtual machines during live migration

System Center 2012 SP1 improvements

System Center 2012 Service Pack 1 (SP1) provides a number of new features to improve the DPM backup experience of servers that run Hyper-V and host virtual machines:

- **Improvements for backup of virtual machines by using Cluster Shared Volume (CSV) storage**:
  - Support for Cluster Shared Volumes (CSV) 2.0 that results in a 90 percent improvement in the performance by extending the express full backup to CSV clusters and improved cluster query performance.
  - Parallel backups are supported. This feature eliminates the requirement to disable parallel backup and serialize the guests on multiple CSVs.
  - No performance difference between backups from CSV owner and non-owner nodes.
- **Improvements in scale out**:
  - Increased scale that allows protection of up to 800 virtual machines of 100 GB each on one DPM server and allows multiple DPM servers that support larger clusters.
  - Better storage savings by excluding the page file from incremental backups to improve virtual machine backup performance.
- **Improvements in deduplicated volumes backup**:
  - Data deduplication finds and removes duplication within data without compromising its fidelity or integrity.
  - DPM allows optimized backup of deduplicated volumes, both locally and over the network.
- **Improvements in live migration**—You can move virtual machines from one location to another while the virtual machines sustain connections and with no noticeable drop time-based on these improvements, live migration provides uninterrupted data protection. Live migration can transfer virtual machines between two stand-alone servers, within a cluster or between stand-alone and cluster nodes. DPM can be used to back up data of virtual machines that are configured for live migration.
- **Improvements in online backup—**You can use DPM to back up virtual machines by backup vaults in Windows Azure Backup.
- **Improvements for backup of virtual machines by using SMB 3.0 storage—**Windows Server 2012 supports the use of server message block (SMB) 3.0 file shares as remote storage, which allows Hyper-V to store configuration files, virtual hard disk (VHD) files, and snapshots on SMB file shares. SMB support provides the following benefits for DPM backup:
  - More efficient express full backups.
  - Continued protection even after live migration.
  - Support for SMB shares on a stand-alone file server or on a cluster of file servers.

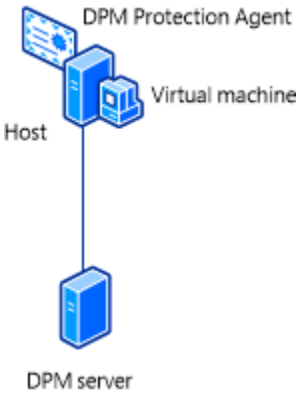
DPM protection overview

DPM protection supports the following scenarios:

- Protects virtual machines that are hosted on stand-alone servers that run Hyper-V and that use local or directly attached storage.
- Protects virtual machines that run on a cluster. The cluster uses Cluster Shared Volumes (CSV) storage.

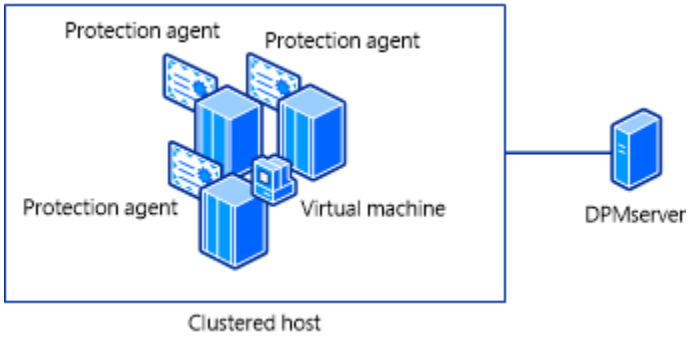
- Protects virtual machines that run on a stand-alone server or cluster and that use SMB 3.0 file server storage.
- Protects virtual machines that are running during a live migration.

Protection for virtual machines on a stand-alone server that is running Hyper-V



This configuration protects one or more virtual machines on a stand-alone host computer. Storage can be local on the host server, or directly attached to it, for example a hard drive, a storage area network (SAN) device, or a network attached storage (NAS) device. Alternatively, the host server might use SMB 3.0 storage on an alternate file server. The DPM protection agent must be installed on all hosts and on the file server if storage is hosted by using SMB 3.0.

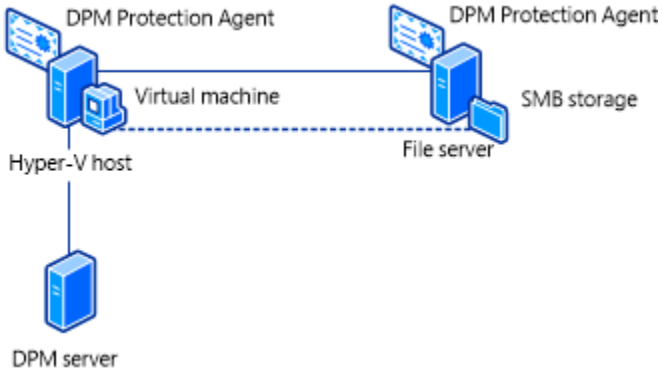
Protection for virtual machines in a cluster of servers that run Hyper-V



This configuration protects virtual machines that are located on servers that run Hyper-V and that run in a failover cluster. Storage can be deployed on Cluster Shared Volumes (CSV) or on a separate SMB 3.0 file server. The DPM protection agent must be installed on all host computers in the cluster, and on the file server where storage is hosted by using SMB 3.0.If you use a clustered host for your virtual machines, you must install the DPM protection agent on all the

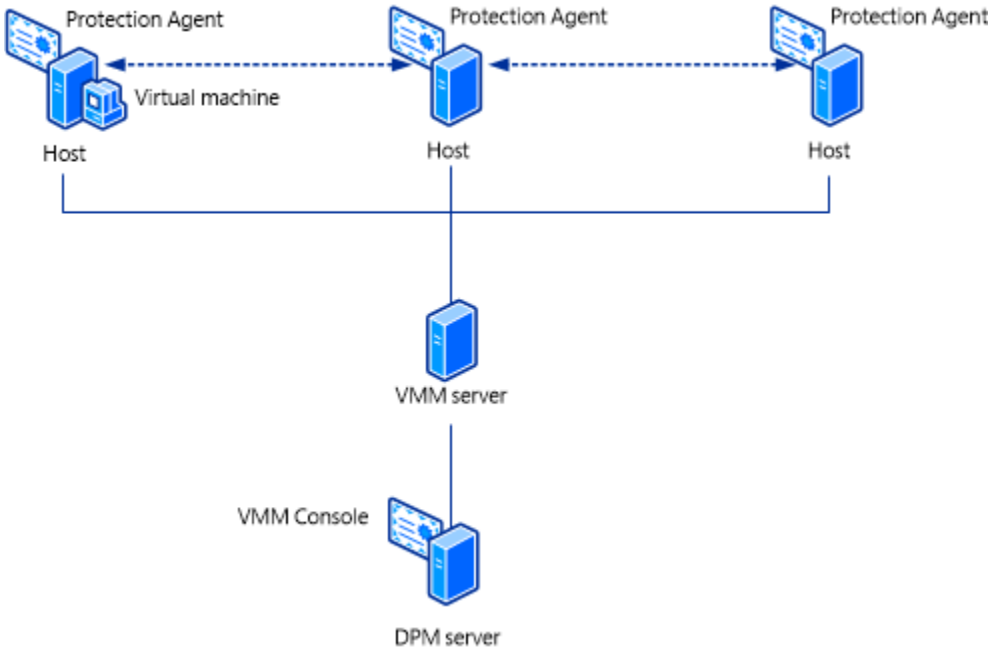
computers in the cluster. For more information, see Protecting virtual machines in clusters with CSV storage.

Protection for virtual machines by using SMB 3.0 storage



If the stand-alone server that is running Hyper-V or the Hyper-V cluster use an external SMB 3.0 file server for storage, the DPM protection agent must be installed on the file server. If the storage server is clustered, the DPM protection agent must be installed on each cluster node. Note that full-share and folder-level permissions are required for the machine$ account of the application server on the SMB share. For more information, see Protecting virtual machines with SMB storage.

Protection of virtual machines during live migration



Live migration enables you to migrate virtual machines from one location to another with no noticeable downtime for users or network applications. You can perform live migration between two stand-alone servers that are running Hyper-V, or between two nodes in the same or different Hyper-V failover clusters. You can also perform a live migration of virtual machine storage so that virtual machines can be moved to new storage locations while they continue to run. The process of running multiple live migrations concurrently is supported.

Migration is often performed independently of backup procedures and can lead to backup failures if not coordinated. DPM addresses this issue by detecting live migration of virtual machines and automatically optimizing backups.

- **Live migration within a cluster**— When a virtual machine is migrated within a cluster, DPM detects the migration, and backs up the virtual machine from the new cluster node without any requirement for user intervention. Because the storage location has not changed, DPM continues with express full backups. In a scaled scenario with two DPM servers to protect the cluster, a virtual machine that is protected by DPM1 continues to be protected by DPM1, no matter where the virtual machine is migrated.
- **Live migration not within a single cluster**—When a virtual machine is migrated between stand-alone servers, different clusters, or between a stand-alone server and a cluster, DPM detects the migration, and can back up the virtual machine without user intervention.

For more information, see Protecting virtual machines during live migration.

Backup overview

DPM provides protection with online backups that do not affect the availability of protected virtual machines. Online backups are supported for servers that are running Hyper-V on the operating systems Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003.

By default, DPM backs up virtual machines in an online state. However, if any of the following conditions are true that are set by the Hyper-V writer, DPM performs backups in an offline state:

- The Backup (Volume Snapshot) Integration Service is disabled or not installed.
- A virtual machine has one or more dynamic disks.
- A virtual machine has one or more volumes that are based on non-NTFS file systems.
- In a cluster configuration, the virtual machine Cluster Resource Group is offline.
- A virtual machine is not in a running state.
- A Shadow Storage assignment of a volume inside the virtual machine is explicitly set to a different volume other than itself.

In these cases, the virtual machine is put in a saved state before a snapshot of host volumes are taken for a backup except when the virtual machine is turned off. The Hyper-V VSS writer adds the virtual machine in the following format: *For offline backups: Backup that uses the saved state\<VMName>. In an online backup, the following format is used: Backup that uses the virtual machine snapshot\<VMName>*

Note the following:

- During offline backups and online backups, the name of the data source remains unchanged even if the virtual machine configuration changes to support online backups or to perform any additional backups.
- DPM supports offline protection for guests that are running older operating systems such as Microsoft Windows NT 4.0 and Microsoft Windows Server 2000, and Linux. Offline backup requires DPM to pause a virtual server, take a snapshot of the server, bring the virtual server online again, and then back up the data on the snapshot.

Backup types

DPM can perform backups by using disk, tape, or cloud-based backups as follows:

- **Disk-Based backup**—Disk-based protection allows for rapid backup and restore of protected data. This speed is critical in that the vast majority of restore operations occur within a relatively short period after a data backup.
- **Tape-based backup**— Although protected data is not initially written to tape, the tape-based backup does have a place in a DPM data protection system. DPM allows backed-up data to be copied to tape to meet data retention and archiving requirements.

For more information, see Backup options.

DPM and VSS

DPM works seamlessly with Hyper-V VSS writer to ensure that consistent versions of virtual machines are captured and protected without affecting virtual machine access. The ability to back up open files is critical for business continuity, and Volume Shadow Copy Services (VSS) is a technology that creates frozen copies of open files. It ensures that virtual machines do not have to be put into hibernation or be shut down before a consistent backup can be made. VSS, DPM, and Hyper-V interact as follows:

- The DPM block-based synchronization engine makes an initial copy of the protected virtual machine and ensures that the copy of the virtual machine is complete and consistent.
- After the initial copy is made and verified, DPM captures backups by using the Hyper-V VSS writer. The VSS writer provides a data-consistent set of disk blocks that are synchronized with the DPM server. This approach provides the benefit of a "full backup" with the DPM server while it minimizes the amount of backup data that have to be transferred across the network.
- The DPM protection agent on a server that is running Hyper-V uses the existing Hyper-V APIs to determine whether a protected virtual machine also supports VSS.
    - If a virtual machine is running guest operating systems beginning with Windows Server 2003, and has the Hyper-V integration services component installed, then the Hyper-V VSS writer recursively forwards the VSS request through to all VSS-aware processes on the virtual machine. This operation occurs without the DPM protection agent being installed on the virtual machine. This recursive VSS request allows the Hyper-V VSS writer to ensure that disk write operations are synchronized so that a VSS snapshot is captured without the loss of data.

- The Hyper-V integration services component invokes the Hyper-V VSS writer in Volume Shadow Copy Services (VSS) on virtual machines to ensure that their application data is in a consistent state.
- If the virtual machine does not support VSS, then DPM automatically uses the Hyper-V APIs to pause the virtual machine before they capture data files.

After the initial baseline copy of the virtual machine synchronizes with the DPM server, all changes that are made to the virtual machine resources are captured in a new recovery point. The recovery point represents the consistent state of the virtual machine at a specific time. Recovery point captures can occur at least one time a day. When a new recovery point is created, DPM uses block-level replication in conjunction with the Hyper-V VSS writer to determine which blocks have been altered on the server that is running Hyper-V after the last recovery point was created. These data blocks are then transferred to the DPM server and are applied to the replica of the protected data.

The DPM server uses VSS on the volumes that host recovery data so that multiple shadow copies are available. Each of these shadow copies provides a separate recovery. VSS recovery points are stored on the DPM server. The temporary copy that is made on the server that is running Hyper-V is only stored for the duration of the DPM synchronization.

In addition to protecting individual virtual machines that are hosted on a server that is running Hyper-V, DPM can also protect workloads that run on a virtual machine for an extra level of protection. This process is the only way in which you can protect data that is stored on pass-through disks. Pass-through disks allow the virtual machine direct access to the storage device and do not store virtual volume data within a VHD file.

Prerequisites for virtual machine protection

This topic summarizes the prerequisites in System Center 2012 - Data Protection Manager (DPM) for the protection of virtual machines that are located on servers that are running Hyper-V.

Server prerequisites

1. Install the Hyper-V role on the DPM server. DPM protects Hyper-V virtual machines even without the role, but you cannot perform item-level recovery (ILR) unless the role is installed.
2. Ensure that the server that acts as the server that is running Hyper-V meets Hyper-V requirements. For more information, see Install the Hyper-V Role and Configure a Virtual Machine.
3. Install the following updates on the server that is running Hyper-V:
   - KB975354
   - KB975921

4. For a Cluster Shared Volumes (CSV) deployment, install the Volume Shadow Copy Services (VSS) hardware provider on the server that is running Hyper-V. Contact your storage area network (SAN) vendor for the VSS hardware provider.
5. Ensure that the following updates are installed on the target server that is running Hyper-V:
   - The customer should be running Hyper-V RTM. The corresponding Windows update is KB950050.
   - Install the following updates:
     - KB951308 on each cluster node for cluster deployment.
       This update provides increased functionality and virtual machine control in the Windows Server 2008 Failover Cluster Management console for the Hyper-V role.
     - KB956697. This update can be applied when the Hyper-V VSS writer appears to be missing due to the presence of corrupt virtual machine configuration files on the server that is running Hyper-V.
     - KB958184. This update can be applied when virtual machine files are saved on a volume that is mounted on a failover cluster by using a volume GUID.
     - KB959962 on the servers that are running Hyper-V. This update for Hyper-V VSS writer is required if the backup fails for one of the following reasons:
       - A transient VSS error occurs, but the operation can be retried.
       - The provider for the VSS application writer is not working as expected
       - The recovery of a virtual machine fails because it has legacy network adapters that are attached.

       Following this update, the Hyper-V Integration Services on each of the virtual machines that are running on the server must be updated by inserting the Integration Services Disk from the **Action** menu in the viVMM console. For this update, the virtual machine must be restarted.

     - KB960038. This update can be applied on all servers that are running Hyper-V. This update for Windows Server 2008 fixes a crashing problem of the server that is running Hyper-V, which you might experience when the Hyper-V VSS writer is used for backups.
   - The version of Integration Components that is running on the virtual machine should be the same as the version of Hyper-V on the server that is running Hyper-V. For Hyper-V RTM, the version is 6.0.6001.18016.
     You can confirm this version number in the Device Manager on the guest virtual machine. In Device Manager, under System Devices, right-click **Hyper-V Volume Shadow Copy**, and then click **Properties**. Check the version on the **Driver** tab. If the version does not match, insert the Integration Services disk by selecting the option under the **Action** menu in the VMM console. Install the integration components, and then restart the virtual machine.

Supported scenarios

DPM can protect the following Hyper-V topologies:

- Protects virtual machines that are hosted on stand-alone servers that are running Hyper-V and that use local or directly attached storage.
- Protects virtual machines that are running on a cluster that uses Cluster Shared Volumes (CSV) storage.
- Protects virtual machines that are running on a stand-alone server or cluster that use Server Message Block (SMB) 3.0 file server storage.
- Protects virtual machines that are running during a live migration.

Unsupported scenarios

- DPM servers and servers that are running Hyper-V must be located in the same domains. Different domains are not supported.
- DPM does not support the backup of virtual machine data on pass-through disks that present volumes to the virtual machine or use a remote virtual hard disk (VHD). For such virtual machines, we recommend that you perform a backup of the VHD files at the level of servers that are running Hyper-V by using DPM and install a DPM protection agent on the virtual machine to back up data that is not visible on the server that is running Hyper-V.
- DPM does not support backup and recovery of virtual machines on replica servers that are running Hyper-V.

Protecting virtual machines during live migration

This section provides information about how you can deploy System Center 2012 - Data Protection Manager (DPM) to effectively protect virtual machines that are running Microsoft Hyper-V during live migration.

- Live migration scenarios
- Storage migration
- Configure DPM protection for live migration

Live migration scenarios

DPM can back up the following live migration scenarios:

- **Live migration within a cluster**—When a virtual machine is migrated within a cluster, DPM detects the migration and backs up the virtual machine from the new cluster node without user intervention. Because there are no changes to storage, DPM continues with express full backups. If two DPM servers protect a cluster, a virtual machine that is protected by the first DPM server continues to be protected by the same DPM server after the migration, no matter where it is located.
- **Live migration outside a single cluster**—When a virtual machine is migrated outside a single cluster, you can perform live migration between two stand-alone servers, between a

stand-alone server and a cluster node, or between two nodes from different clusters. In this scenario, DPM detects the migration and can perform backups without user intervention. The backups require the following configuration:

- The virtual machines are managed in a cloud that is configured on a VMM management server that is running System Center 2012 SP1.
- The DPM servers are connected to the VMM management server on which the private cloud is located.
- All servers that are running Hyper-V are connected to all DPM servers.

With these prerequisites in place, DPM communicates with VMM to locate where the virtual machine currently runs, and can then create a backup from the new server that is running Hyper-V. DPM can communicate with the new server that is running Hyper-V because all servers that are running Hyper-V are connected to all DPM servers. If this connection cannot be established, the backup fails with a message that the DPM protection agent is unreachable.

Storage migration

If a live migration transfers storage, DPM performs a full consistency check of the virtual machine, and then continues with express full backups. If there is no storage migration involved, for example if the source and target locations both use the same server message block (SMB) 3.0 file server, then DPM continues to perform express full backups without the consistency check.

Configure DPM protection for live migration

Before you start, note or do the following:

- DPM protection for live migration is only available on servers that are running Windows Server 2012.
- Live migration protection does not support backup of data to tape, neither disk-to-tape nor disk-to-tape-to-tape.
- DPM performs a one-time consistency check for all live migrations that include storage migration.
- When live migration of storage occurs, Hyper-V reorganizes the virtual hard disk (VHD) or VHDX and therefore there is a one-time spike in the size of DPM backup data.
- Turn on auto-mount on the virtual machine host to enable virtual protection.
- Disable the feature TCP Chimney Offload.
- These steps assume that you have installed the DPM server and have configured DPM storage. For more information, see Installing DPM, and Adding Disks to the Storage Pool.

Then complete the following steps:

1. Verify that the DPM servers, VMM management servers, and servers that are running Hyper-V are located in the same domain.
2. Deploy the DPM protection agent on all computers that are to host virtual machines. For instructions, see Installing and Configuring Protection Agents.

3. Install the VMM console as the VMM client component on all DPM servers to enable the DPM server to communicate with and track the VMM management server. Note the following:
   a. The DPMMachineName$ account should be a read-only administrator account on the VMM management server.
   b. Ensure that the VMM console is of the same version as the VMM management server that is used in the deployment.
4. Set the Global Property value for the KnownVMMServerName by using Windows PowerShell, as follows:

   ```
   Set-DPMGlobalProperty -dpmservername <dpmservername> -knownvmmservers <vmmservername>.
   ```

   This command connects all the servers that are running Hyper-V to all the DPM servers. The cmdlet accepts multiple DPM server names. For usage instructions, see Set-DPMGlobalProperty.
5. Create protection groups in DPM by using the New Protection Group Wizard. Note that automatic consistency check should be enabled at the protection group level for protection under virtual machine mobility scenarios.

   Important
   Enable the DPM VMM communication first. All virtual machines on servers that are running Hyper-V should be discovered before you configure the protection groups. Otherwise, live migration does not work as expected, and the user has to stop to protect data with Retain Data, and then reconfigure protection for the same computer.

After settings are configured, when a virtual machine migrates from one cluster to another, all backups continue as expected. You can then use the Recovery Wizard as required. Note that after you complete the steps, live migration is enabled after the DPM Summary Manager job runs. By default, this job starts at midnight and runs every morning. For information about how to run a live migration immediately, see Manually run a live migration.

Verify that live migration is enabled as expected

Verify settings as follows:

1. Ensure that the service DPM-VMM Helper Service is running. If it is not running, start it. If it already runs, continue to the next step.
2. Open Microsoft SQL Server Management Studio and connect to the instance that hosts the DPM database (DPMDB).
3. On DPMDB, run the following query: `SELECT TOP 1000 [PropertyName] ,[PropertyValue] FROM[DPMDB].[dbo].[tbl_DLS_GlobalSetting]`

   This query contains a property, called **KnownVMMServer**. This value should be the same as the value that you provided with the **Set-DPMGlobalProperty** cmdlet.
4. Run the following query to validate the *VMMIdentifier* parameter in the **PhysicalPathXML** for a particular virtual machine:

```
select cast(PhysicalPath as XML) from tbl_IM_ProtectedObject where DataSourceId in
(select datasourceid from tbl_IM_DataSource where DataSourceName like '%<VMName>%')
```

5. Replace **VMName** with the name of the virtual machine.
6. Open the .xml file that this query returns and validate that the *VMMIdentifier* field has a value.

After completing configuration

After you set up DPM protection for live migration, you might want to complete a number of actions.

Manually run a live migration

After you completed the steps, live migration is enabled after the DPM Summary Manager job runs. By default, live migration starts at midnight and runs every morning. If you want to run a live migration immediately, you can run it manually as follows:

1. Open SQL Server Management Studio and connect to the instance that hosts DPMDB.
2. Run the following query: `select * from tbl_SCH_ScheduleDefinition where JobDefinitionID='9B30D213-B836-4B9E-97C2-DB03C3EB39D7'`. Note that the query returns the **ScheduleID**.
3. In SQL Server Management Studio, expand **SQL Server Agent**, and then expand **Jobs**.
4. Right-click the **ScheduleID** that you noted, and select **Start Job at Step**.

Note that backup performance is affected when the job runs. The size and scale of your deployment determines how much time the job takes to finish.

Change the default DPM-VMM Helper service port

If you want to change the default port of 6070 that is used by DPM to host DPM-VMM Helper Service, do the following:

1. Open the Registry Editor regedit.
2. Navigate to `HKLM\Software\Microsoft\Microsoft Data Protection Manager\Configuration`.
3. Create a 32-bit DWORD value, named `DpmVmmHelperServicePort`.
4. Write the new port number as part of this registry key.
5. Open <Install directory>\Microsoft System Center 2012\DPM\DPM\VmmHelperService\VmmHelperServiceHost.exe.config and change the port number from 6070 to the new port.

   For example: <add baseAddress="net.tcp://localhost:6080/VmmHelperService/" />
6. Restart the DPM-VMM Helper service.
7. Restart the DPM service.

Upgrade the VMM or DPM server

Note that if you upgrade the VMM management server, you must also upgrade the VMM console on the DPM server to maintain protection. If you upgrade DPM, set the Global Property on the DPM server for the KnownVMMServerName by using Windows PowerShell as follows: `Set-DPMGlobalProperty -dpmservername <dpmservername> -knownvmmservers <vmmservername>`

See Also

Providing uninterrupted protection to virtual machines that use live migration

Protecting virtual machines with SMB storage

Windows Server 2012 supports the use of Server Message Block (SMB) 3.0 for remote storage that allows Hyper-V to store configuration files, virtual hard disks as VHD and VHDX files, and snapshots on remote SMB file shares. SMB support provides the following benefits for System Center 2012 System Center 2012 – Data Protection Manager (DPM) backup:

- More efficient express full backups
- Continued protection after live migration of virtual machines and SMB storage
- Backup support for a single SMB file server or for a cluster of file servers

Configure DPM backup for virtual machines using SMB storage

Note the following before you start:

- Turn on auto-mount on the server that is running Hyper-V to enable virtual machine protection.
- Disable TCP Chimney Offload.
- Ensure that all Hyper-V machine$ accounts have full permissions on the specific remote SMB file shares.
- Ensure that the file path for all virtual machine components during recovery to alternate location is less than 260 characters. If not, recovery might succeed, but Hyper-V cannot mount the virtual machine.
- The following scenarios are not supported:
  - Deployments where some components of the virtual machine are on local volumes and some components are on remote volumes.
  - An IPv4 or IPv6 address for storage location file server.
  - Recovery of a virtual machine to a computer that uses remote SMB shares.

Then complete the following steps:

- Step 1: Deploy DPM protection agents
- Step 2: Add a custom cluster resource type—Required for non-Microsoft SMB storage.
- Step 3: Enable the File Server VSS Agent service
- Step 4: Create protection groups

Step 1: Deploy DPM protection agents

The DPM protection agent is software that you install on a computer that you want to protect with DPM. For servers and clusters that use SMB 3.0 storage, you must deploy the DPM protection agent as follows. For more information, see Installing and Configuring Protection Agents.

- On the server that is running Hyper-V in a cluster, deploy the DPM protection agent on each node.
- On the remote SMB file server, if SMB is deployed in a cluster, install the DPM protection agent on all SMB file server cluster nodes.

DPM protection agents can be installed as follows:

- **Using the DPM console**—The DPM console automatically detects a list of available computers in the same domain as the DPM server, so that you can select the computer on which you want to install the DPM protection agent. The use of this method enables you to install DPM protection agents on these computers synchronously. This method can be used for computers that belong to the DPM server domain and do not have a firewall that blocks the installation of the DPM protection agent. For more information, see Installing Protection Agents on Computers Outside of a Firewall. Note that you must have domain credentials that have local administrative rights for all computers on which you want to deploy the DPM protection agent.
- **Manual installation**—This method can be used to install the DPM protection agent on computers that are not domain members or that do not belong to the same domain as the DPM server. It can also be used if a firewall blocks automatic deployment of the DPM protection agent from the DPM console. For more information, see Installing Protection Agents Manually.

Step 2: Add a custom cluster resource type

If you are using non-Microsoft SMB storage, DPM does not discover the cluster automatically. You must add a setting to enable the DPM server to recognize the cluster as follows:

1. To open the Registry Editor, at the command prompt, type **regedit**.
2. Navigate to **Software\Microsoft\Microsoft Data Protection Manager\Agent\Cluster**.
3. Set value **PhysicalDiskResourceType** to the type of non-Microsoft cluster disk service. The value type is REG_SZ.

Step 3: Enable the File Server VSS Agent service

Enable the service on each SMB server as follows:

1. In the Server Manager Dashboard, click **Add roles and features**.

2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, select **Role-based or feature-based installation**.
4. On the **Select destination server** page, select the SMB server on which you want to add the service.
5. On the **Select server roles** page, expand **File and Storage Services**, **File Services**. Select **File Service**, and then select **File Server VSS Agent Service**.
6. On the **Select features** page, click **Next**.
7. In **Confirm installation selection**, verify the service is listed, and then click **Install**.

Step 4: Create protection groups

After the DPM protection agent is deployed, you protect virtual machines by creating protection groups and add servers that are running Hyper-V to those groups. This process enables the backup and restore operation of the servers that are running Hyper-V, and the virtual machines that are running on them. The configuration settings for a protection group specify backup and recovery settings for all servers that are running Hyper-V in the group. They include:

- The choice to perform backups by using tape or disk
- The duration to retain backups on disk
- The recovery point settings to use
- The storage pool settings to assign to the protection group
- The choice to collocate data in the storage pool
- The choice to automatically increase the size of the volumes
- The choice to perform initial replication of virtual machines that are located on servers that are running Hyper-V in the group over the network or manually offline
- The choice of how consistency checks should be performed

Depending on the number of virtual machines that you want to protect and depending on the backup policies for the different virtual machines, you should create virtual machines by using the New Protection Wizard from the DPM user interface (UI) and keep the virtual machines that have the same backup policy in the same group. You should create smaller groups of 50-100 virtual machines per protection group, but this is not a restriction. Use collocation while you create the protection groups to optimize the replica volume and avoid reaching the maximum number of volumes that are supported in a Windows Server.

For more information, see **Creating Protection Groups**.

Scaling out protection for virtual machines

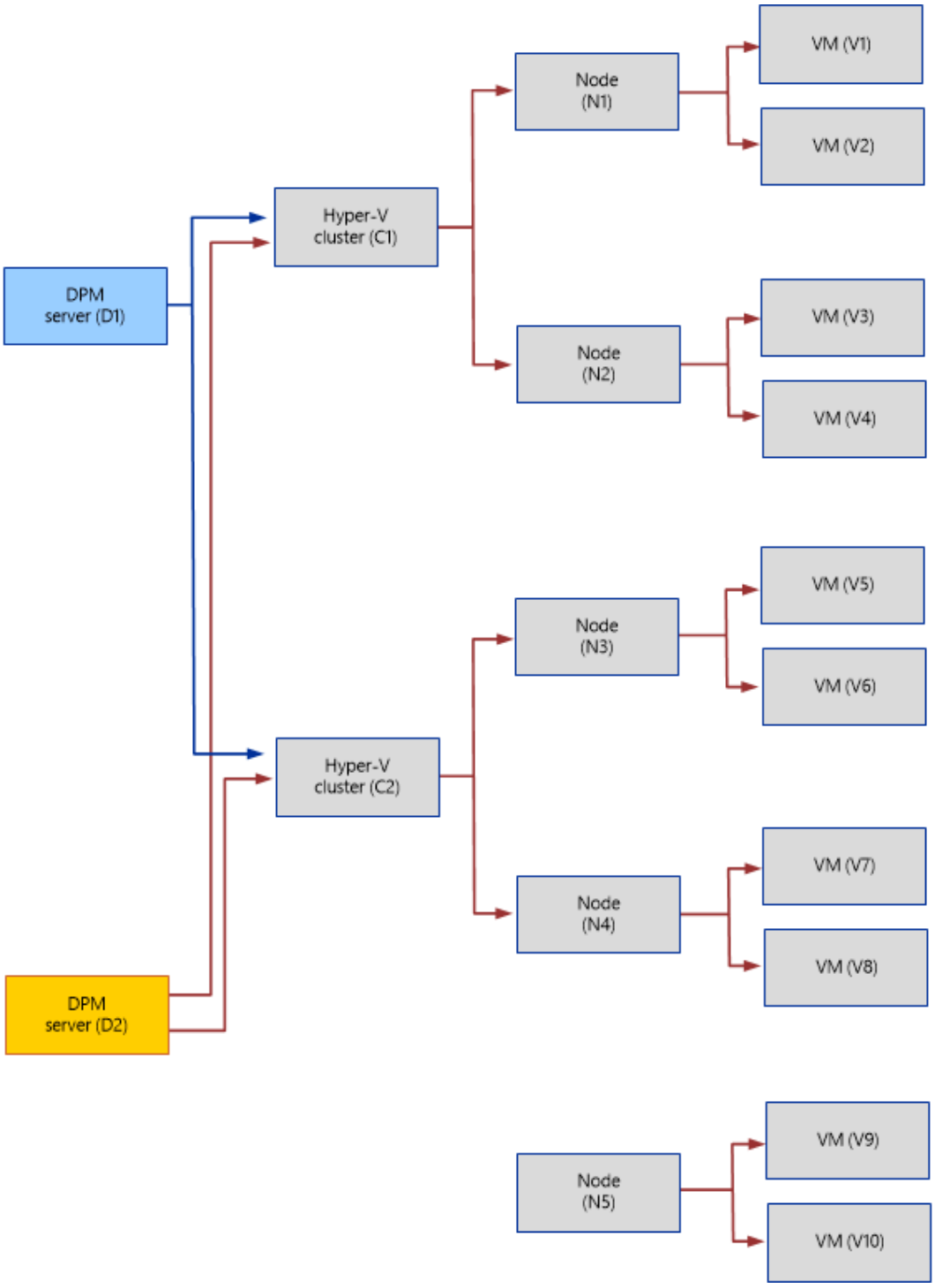
In System Center 2012 Service Pack 1 (SP1) - Data Protection Manager (DPM), you can scale out protection of Hyper-V clusters. The new scale-out feature removes the limit of a one-to-one relationship between a Hyper-V cluster and a DPM server, and the DPM protection agent that

runs on a virtual machine can attach itself to multiple DPM servers. Therefore you can add the virtual machine to a protection group on any of the recognized DPM servers. Note the following:

- This feature is only available for virtual machines that are hosted on servers that are running Windows Server 2012.
- The DPM server must be a clean deployment of DPM in System Center 2012 SP1.
- DPM chaining is not supported.
- All DPM servers and the protected computers must be located in the same domain.
- The scale-out feature does not support protection for remote server message block (SMB) shares for a virtual machine.
- The scale-out feature does not support an IPv4 or IPv6 address for a storage location file.

Deployment scenario

To deploy scale-out protection, you must have a minimum of two DPM servers D1 and D2, which are visible to all virtual machines that are hosted on nodes N1, N2, N3, N4, and N5. When you create protection groups on D1 or D2, you can add any of the virtual machines from V1 to V10 for protection.



Configuring DPM scale-out consists of the following steps:

- Step 1: Deploy DPM protection agents
- Step 2: Make multiple servers visible to virtual machines

- Step 3: Add protection groups
- Step 4: Configure new nodes for protection
- Step 5: Add a new DPM server

Step 1: Deploy DPM protection agents

On the first installed DPM server, install the DPM protection agent on servers that are running Hyper-V. For more information, see Installing and Configuring Protection Agents. DPM protection agents can be installed as follows:

- **Using the DPM console**—The DPM console automatically detects a list of available computers in the same domain as the DPM server, so that you can select the computer on which you want to install the DPM protection agent. By using this method, you can install DPM protection agents on these computers synchronously. This method can be used for computers that belong to the DPM server domain, and do not have a firewall that blocks the DPM protection agent installation. For more information, see Installing Protection Agents on Computers Outside of a Firewall. Note that you must have domain credentials that have local administrative rights for all computers on which you want to deploy the DPM protection agent.
- **Manual installation**—This method can be used to install the DPM protection agent on computers that are not domain members or that do not belong to the same domain as the DPM server. It can also be used if a firewall blocks automatic deployment of the DPM protection agent from the DPM console. For more information, see Installing Protection Agents Manually.

Step 2: Make multiple servers visible to virtual machines

Use the **SetDPMServer** command with the *Add* parameter on the protected virtual machine to make multiple DPM servers visible to the protected virtual machine, as follows:

1. `Setdpmserver –add –dpmservername <name of second DPM server>`

Tip
If you do not use the *–Add* parameter, the previous DPM server is overwritten. Ensure that all servers that are running Hyper-V and virtual machines are discovered by the Virtual Machine Manager (VMM) server before you begin to create protection groups.

For more information about this command, see Using SetDPMServer.

Step 3: Add protection groups

After you attach all the DPM servers, you can add the virtual machine to a protection group on any of the DPM servers that the virtual machine can recognize.

If you do not have any existing protection groups, do the following:

1. Create protection groups and add the servers that are running Hyper-V to those groups. This action enables the backup and restore operations of the servers that are running Hyper-V,

and the virtual machines running on them. The configuration settings for a protection group specify backup and recovery settings for all servers that are running Hyper-V in the group. They include:

- The choice to perform backups by using tape or disk
- The duration to retain backups on the disk
- The recovery point settings to use
- The storage pool settings to assign to the protection group
- The choice to collocate data in the storage pool
- The choice to automatically increase the size of the volumes
- The choice to perform initial replication of virtual machines that are located on servers that are running Hyper-V in the group over the network or manually offline
- The choice of how consistency checks should be performed

Note

Depending on the number of virtual machines that you want to protect and depending on the backup policies for the different virtual machines, you should create virtual machines by using the New Protection Wizard from the DPM console, and keep virtual machines which have the same backup policy in the same group. You should create smaller groups of about 50-100 virtual machines per protection group, although this is not a fixed restriction. Use collocation while you create the protection groups to optimize the replica volume, and to avoid reaching the maximum number of volumes that are supported in a Windows Server deployment.

2. If you have existing protection groups, after you attach all the DPM servers, add the virtual machine to a protection group on any of the DPM servers that the virtual machine recognizes. After you add the virtual machine to a group, the virtual machine is always backed up on that DPM server. If you want the virtual machine to be backed up on a different server, you must stop protection for it and add it to a protection group on the new server. This flexibility means that virtual machines from a single node can be protected by different DPM servers.

For more information, see Create a protection group.

Step 4: Configure new nodes for protection

If you want to add a new node to the cluster, you must install the DPM protection agent on that node, and then configure it for protection, as follows:

1. Install the DPM protection agent on the server that is running Hyper-V.
2. Attach the DPM protection agent to all DPM servers in the network.
3. Run **Setdpmserver** on all nodes in the cluster.

Step 5: Add a new DPM server

If you want to add a new DPM server to the scaled-out deployment, it must be configured with all the nodes in the cluster to prepare it for protection, as follows:

1. Attach a new node for protection.
2. Run **Setdpmserver** on all nodes in the cluster.

Optimizing virtual machine protection

You can perform a number of actions to optimize the performance of System Center 2012 - Data Protection Manager (DPM) backups for Hyper-V virtual machines. The actions include:

1. Enable caching—When you protect over 200 virtual machines that use Cluster Shared Volumes (CSV), it can take more than 15 minutes to populate the **Inquiry** page in the **Create New Protection Group Wizard**. You can avoid this time latency if you enable caching on the primary DPM server. After you enable caching, when you expand the data source on the **Inquiry** page, DPM refreshes the resource groups under that node, but the virtual machines under each resource group are populated from the cache. The default time-out for the cache is 48 hours.
2. Exclude page file churns—To improve the performance of your Hyper-V backups, you can decide not to back up the entire churn in your page file. This exclusion gives you the benefit of reduced storage requirement and improvement in backup performance. When the page file is excluded, DPM does not affect replica creation and consistency checking. The only change is that when the page file is excluded, DPM does not perform incremental backups on the page file.
3. Automatically add new virtual machines to a protection group—After you deploy the DPM protection agent on a server that is running Hyper-V, you must add the server that is running Hyper-V manually to the required protection groups. You can automate the process by running a script.

Enable caching

Enable caching as follows:

Create a new registry key, called **CacheInquiryResults** at **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Configuration**. Under this key, create the DWORD InquiryResultsTimeoutInterval.

After you create the registry key, on the **Inquiry** page of the **Create New Protection Group Wizard**, click **Clear Cache** when you want to force DPM to refresh the list of virtual machines.

Note

When you click **Clear Cache**, DPM refreshes the entire cache, and not just the cache of the selected resource group.

Exclude page file churns

Exclude page files as follows:

1. Move the page file for a virtual machine to a different virtual hard disk (VHD).
2. Exclude page files by using the **Set-DPMGlobalProperty** cmdlet. For more information about how to use this cmdlet, see Set-DPMGlobalProperty.

Automatically add new virtual machines to a protection group

Automate the process to add new virtual machines to a protection group as follows:

- Automatically add stand-alone virtual machines
- Automatically add virtual machines to a cluster deployment

Automatically add stand-alone virtual machines

The AddNewStandAloneVM.ps1 script does the following:

- Takes the fully qualified domain name (FQDN) of the protected server and the name of the protection group as input.
- Searches for the protected server and the protection group.
- Runs an inquiry on the server that is running Hyper-V and obtains the list of unprotected virtual machines.
- Adds this list of virtual machines to the protection group.
- Saves the changes to the protection group and exits the procedure.

The script takes the following two parameters.

Parameter	Description	Example
Server name	FQDN of the server that is running Hyper-V	hyperv01.contoso.com
Protection group	Name of the existing protection group to which you add the new virtual machines	Protection Group 3

Automatically add virtual machines to a cluster deployment

The AddNewClusteredVM.ps1 script does the following:

- Takes the FQDN of the protected cluster and the name of the protection group as input.

- Searches for the protected cluster and the protection group.
- Runs an inquiry on the cluster to get the list of resource groups.
- Runs a parallel inquiry for each resource group and obtains the list of unprotected virtual machines under them.
- Adds the unprotected virtual machines to the protection group.
- Saves the changes to the protection group and exits the procedure.

The script takes the following two parameters.

Parameter	Description	Example
Server name	FQDN of the server that is running Hyper-V	hyperv01.contoso.com
Protection group	Name of the existing protection group to which you add the new virtual machines	Protection Group 3

Recovering virtual machines

After backing up Hyper-V virtual machines, System Center 2012 - Data Protection Manager (DPM) supports the following recovery scenarios.

Scenario	Description
Recovery of a virtual machine to the original location	The original virtual hard disk (VHD) is deleted. DPM recovers the VHD and other configuration files on the original location by using the Hyper-V VSS writer. At the end of the recovery process, the virtual machine is still highly available. **Warning** The resource group must be present to enable the recovery. If the resource group is not available, recover the VHD to an alternate location, and then make the virtual machine highly available.
Recovery of a virtual machine to an alternate location	DPM supports alternate location recovery (ALR), which provides a seamless recovery of a protected Hyper-V virtual machine to a different

Scenario	Description
	server that runs Hyper-V, independent of the processor architecture. Hyper-V virtual machines that are recovered to a cluster node are not highly available. For more information about how to make a virtual machine highly available, see To make a virtual machine highly available.
Item-level recovery (ILR) of Hyper-V virtual machines	DPM supports item-level recovery (ILR), which allows you to perform a specific recovery of files, folders, volumes, and virtual hard disks (VHDs) from a host-level backup of Hyper-V virtual machines to a network share or a volume on a DPM protected server.  **Tip** The DPM protection agent does not have to be installed on the guest machine to perform item-level recovery.

The following tables show the types of data recovery that you can perform that is based on the type of your deployment.

Deployment	Recovery to original location	Recovery to alternate location	Item-level recovery
Stand-alone host	Yes	Yes	Yes
Clustered host	Yes	Yes	Yes
Using server message block (SMB) share	Yes	Yes	Yes
Using live migration	Yes	Yes	Yes

The following table shows the supported and unsupported scenarios to recover files, folders, volumes, and VHDs by using ILR on a Hyper-V virtual machine.

Scenario	Volumes or files/folders recovery	Virtual hard disk (VHD) recovery
Recovery from a virtual machine that has snapshots	Yes	Yes

Scenario	Volumes or files/folders recovery	Virtual hard disk (VHD) recovery
Recovery from a secondary DPM server	Yes	Yes
Recovery from tape backups	No	Yes
Recovery from NTFS file system volumes only	Yes	Not applicable
Recovery from non-NTFS file system volumes	No	Entire VHD only
Recovery from a VHD that is partitioned by using dynamic disk partitioning	No	Entire VHD only

Important
You cannot traverse or browse the mount points when you explore a VHD for item-level recovery.

- To recover a Hyper-V virtual machine in a non-CSV environment
- To recover a virtual machine to an alternate stand-alone server that runs Hyper-V
- Item-level recovery for Hyper-V
- To recover a Hyper-V virtual machine that uses live migration

To recover a Hyper-V virtual machine in a non-CSV environment

1. Select the recovery point that you want to recover from the Recovery work area.
2. Use the **Recovery** wizard to select and recover the virtual machine.

Note

- If you select the virtual machine on the left pane, the **Recoverable Item** list shows you the list of VHDs. If you perform a recovery at this point, you recover a VHD and not the virtual machine.
- In a non-CSV environment, the destination is a volume in available storage in the cluster.

To recover a virtual machine to an alternate stand-alone server that runs Hyper-V

1. Select the recovery point that you want to recover from the Recovery work area.
2. Use the **Recovery** wizard to select and recover the virtual machine.

Note

- If the recovered virtual machine was backed up in an online state, and it is saved state after recovery, delete the saved state of that virtual machine from the Hyper-V Manager console and start it.
- Always check whether the virtual machine's network configuration is correct after the alternate location recovery.

Item-level recovery for Hyper-V

DPM provides both host-based and guest-based protection for Hyper-V virtual machines.

DPM supports item-level recovery (ILR), which enables you to recover specific files, folders, volumes, and virtual hard disks (VHDs) from a host-level backup of Hyper-V virtual machines to a network share or a volume on a DPM protected server.

If you use a version of Windows Server before Windows Server 2008, you must have the Hyper-V role enabled on the DPM server to perform item-level recoveries. During item-level recovery, DPM has to mount the VHDs of the protected virtual machines.

Important

- Item-level recovery does not support recovery of an item to its original location.
- Item-level recovery is not supported if the Diff VHD and Base VHD are on different volumes.

To perform item-level recovery of files and folders

1. Select the recovery point that you want to recover from the Recovery work area.
2. To view the list of files and folders, in the **Recoverable Items** list, do the following:
   - Double-click the item **(VHD)** that you want to recover.
   - Double-click the items **(volumes in VHD)** that you want to recover.
3. Use the **Recovery** wizard to select and recover the virtual machine.

Note

DPM saves files and folders in a custom directory structure in the following format: <Recovery destination that is selected by the user>\<Virtual machine name>_<Backup time stamp> with the exact file system hierarchy that is used on a protected computer with the DPM protection agent installed.

To perform item-level recovery of volumes

1. Search for the virtual machine name that you want to recover, and then in the details pane, select the item **(VHD)**.
2. To view the list of volumes, in the **Recoverable Items** list, do the following:
   - Double-click the item **(VHD)** that you want to recover.
   - Select the item **(volume in VHD)** that you want to recover.

   Note
   - The **List** pane displays the volume label or "Virtual Machine Volume" if no volume label is available.
   - You cannot select and recover multiple volumes at the same time.
3. Use the **Recovery** wizard to select and recover the virtual machine.

To perform item-level recovery of VHD

1. Search for the name of the virtual machine that you want to recover, and then in the details pane, select the item **(VHD)**.
2. Use the **Recovery** wizard to select and recover the virtual machine.

Note

- The path of the VHD file on the protected computer is displayed in the **Recoverable Items** list.
- You cannot select and recover multiple VHDs at the same time.
- When you recover a VHD of a virtual machine that has Hyper-V snapshots, .avhd files are not displayed in the **Recoverable Items** pane, but DPM recovers the parent VHD and all the associated .avhd files.
- DPM saves VHDs in a custom directory structure in the following format: DPM_<backup-time>\DPM_Recovered_At_<RecoveryTime>\<Path of the VHD on the protected computer> with the exact file system hierarchy that is used on a protected computer with the DPM protection agent installed.

To recover a Hyper-V virtual machine that uses live migration

1. Browse to or search for the name of the virtual machine that you want to recover, and then in the details pane, select the item **(VHD).**
2. Use the **Recovery** wizard to select and recover the virtual machine.

Note

Recovery of a virtual machine to its original location is possible only if there is a replica from that location. For example, recovery is possible if a virtual machine is hosted on Host A and during this time 10 replicas are taken, and then the virtual machine is migrated to Host B, where two replicas are taken. Original location recovery means that the virtual machine is recovered to Host B if the latest replicas are used. If you want to recover the virtual machine to Host A, it uses an alternate location recovery flow.

Protecting virtual machines in clusters with CSV storage

Data Protection Manager (DPM) in System Center 2012 can back up virtual machines that are using Cluster Shared Volume (CSV) storage.

- CSV overview
- Using VSS
- Configure CSV backups
- Configure concurrent backups for hardware VSS providers

CSV overview

CSV is a feature of failover clustering that was introduced in Windows Server 2008 R2. CSV allows you to store multiple virtual machines running on multiple hosts in a cluster on a single storage volume. A CSV is a shared single disk that contains an NTFS volume. Multiple virtual machines can be stored on a CSV, and the CSV can be accessed by multiple Hyper-V host servers installed on failover cluster nodes. You can have multiple CSVs in a Hyper-V cluster. Typically, all of the virtual hard disks (VHDs) of virtual machines in the cluster are stored on a common CSV, so that any node in the cluster can access the VHDs.

Direct and Redirect I/O

Each Hyper-V host has a direct path (direct I/O) to the CSV storage Logical Unit Number (LUN). However, in Windows Server 2008 R2 there are a couple of limitations:

- For some actions, including DPM backup, the CSV coordinator takes control of the volume and uses redirected instead of direct I/O. With redirection, storage operations are no longer through a host's direct SAN connection, but are instead routed through the CSV coordinator. This has a direct impact on performance.
- CSV backup is serialized, so that only one virtual machine on a CSV is backed up at a time.

In Windows Server 2012, these limitations were removed:

- Redirection is no longer used.
- CSV backup is now parallel and not serialized.

You can learn more about CSV changes in the TechEd presentation: Windows Server 2012 in Cluster Shared Volumes Reborn in Windows Server 2012: Deep Dive.

Using VSS

DPM works seamlessly with Volume Shadow Copy Services (VSS) to ensure that consistent versions of virtual machines are backed up without affecting virtual machine availability and access. Using VSS you can u to back up entire virtual machines at the host or storage level, so that their contents are backed up in a consistent state. VSS pauses the virtual machines, takes a snapshot, and enables backup of the file system and VSS-aware applications.

You can back up CSVs with a hardware VSS provider or with software VSS integrated in the Windows operating system.

- Prior to Windows Server 2012, using software VSS entailed the use of redirected I/O from the time the backup starts to the time it finishes, and used serialization, thus impacting performance. This limitation is removed in Windows Server 2012.
- Hardware VSS does not require serialization and redirected I/O is only used when the snapshot is created. If you are running Windows Server 2008 R2 then using hardware VSS is recommended. After the snapshot is created, DPM starts to replicate the data from the snapshot to the DPM server. After the replication is completed, the DPM protection agent deletes the hardware snapshot.

Configure concurrent backups for hardware VSS providers

If you use a hardware Volume Shadow Copy Services (VSS) provider to back up Hyper-V virtual machines in a cluster that uses Cluster Shared Volumes (CSV) storage, you can back up multiple virtual machines System Center 2012 - Data Protection Manager (DPM) using from the same CSV and node in the cluster. To specify the number of concurrent backups that can run from a node, do the following:

1. Open the Registry Editor.
2. Navigate to HKLM\Software\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBackups.
3. Set the following values:
    - Value: Microsoft Hyper-V
    - Data: 3
    - Type: DWORD

This setting enables a maximum of three backups to run concurrently on each node. For optimal performance, we recommend that you do not use a value greater than 3.

Configure CSV backups

This section describes the required steps to back up Hyper-V virtual machines in a cluster that uses Cluster Shared Volumes (CSV) storage:

- Read Before you start
- Step 1: Deploy the DPM protection agent
- Step 2: Plan DPM storage requirements
- Step 3: Create protection groups

Before you start

Note the following before you start:

- A single node shutdown in a CSV cluster causes all virtual machines in the cluster to be marked as inconsistent. This action starts consistency checks for all virtual machines.
- If BitLocker Drive Encryption is enabled on the CSV cluster, to restart a server that is running Hyper-V, you must run a consistency check for Hyper-V virtual machines.
- If you are running Hyper-V on Windows Server 2008 R2 and you're backing up multiple clusters with DPM, you need to ensure that only one backup uses the same CSV at any one time. To do this, follow the instructions in Serialize virtual machine backups.
- If you're currently using the integrated software VSS and you want to move to a hardware VSS, follow the instructions in Migrate to a hardware VSS provider.

Step 1: Deploy the DPM protection agent

The DPM protection agent is software that you install on a computer to provide protection with Data Protection Manager (DPM) for the computer. For clusters that use CSV storage, you must deploy the DPM protection agent on each server that is running Hyper-V in the cluster. For more information, see Installing and Configuring Protection Agents

DPM protection agents can be installed as follows:

- **Automatic installation using the DPM console**—The DPM console automatically detects a list of available computers in the same domain as the DPM server, so that you can select the computer on which you want to install the DPM protection agent. The use of this method enables you to install DPM protection agents on these computers in a synchronous fashion. This method can be used for computers that belong to the DPM server domain and do not have a firewall that blocks the installation of the DPM protection agent. For more information, see Installing Protection Agents on Computers Outside of a Firewall. Note that you must have domain credentials that have local administrative rights for all computers on which you want to deploy the DPM protection agent.
- **Manual installation**—This method can be used to install the DPM protection agent on computers that are not domain members or that do not belong to the same domain as the DPM server. It can also be used if a firewall blocks automatic deployment of the DPM

protection agent from the DPM console. For more information, see Installing Protection Agents Manually.

Step 2: Plan DPM storage requirements

It is essential to plan for DPM storage requirements to back up CSV storage. 800 virtual machines can be provisioned to each DPM server.

Average virtual machine size	100 gigabytes (GB)
Number of virtual machines per DPM server	800
Total size of 800 virtual machines	80 terabytes (TB)
Required space for backup storage	80 terabytes (TB)

For example, if your fully scaled Hyper-V cluster contains 1600 virtual machines, you must have two DPM servers, and double the provisioning that is summarized in the table. The total storage requirement for 1600 virtual machines is greater than 160 TB.

To optimize the space that is used for backup storage, you can exclude the page file to prevent that incremental changes in the page file are transferred. For more information, see the following resources:

- Scaling out protection for virtual machines
- Exclude page file churns
- Plan for DPM storage

Step 3: Create protection groups

After the DPM protection agent is deployed to the servers that are running Hyper-V, you create protection groups and add the servers that are running Hyper-V to those groups. This action enables the backup and restore operations of the servers that are running Hyper-V, and the virtual machines that are running on these servers. The configuration settings for a protection group specify backup and recovery settings for all servers that are running Hyper-V in the group. They include:

- The choice to perform backups by using tape or disk
- The duration to retain backups on disk
- The recovery point settings to use
- The storage pool settings to assign to the protection group
- The choice to collocate data in the storage pool
- The choice to automatically increase the size of the volumes
- The choice to perform initial replication of virtual machines that are located on servers that are running Hyper-V in the group over the network or manually offline
- The choice of how consistency checks should be performed

Depending on the number of virtual machines that you want to protect and the backup policies for the different virtual machines, the user should create virtual machines by using the New Protection Wizard from the DPM console and keep the virtual machines that have same backup policy in the same group. The user should create smaller groups of 50-100 virtual machines per protection group, but this is not a restriction. Use collocation while you create the protection groups to optimize the replica volume and to avoid reaching the maximum number of volumes that are supported in a Windows Server.

For more information, see **Creating Protection Groups**.

Serialize virtual machine backups

If you're using software VSS with Hyper-V on Windows Server 2008 R2, do the following

- Serialize virtual machine backups per node
- **Serialize virtual machine backups per CSV LUN**

If you are protecting multiple Hyper-V clusters in Windows Server 2008 R2 with DPM, you can use the DPM merging and serialization tool to remove many of the manual steps associated with the scripts in this section. Download the tool from System Center Data Protection Manager CSV Serialization Tool on the Microsoft Download Center.

Serialize virtual machine backups per node

To serialize virtual machine backups per cluster node, on the DPM server navigate to HKLM\Software\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBackups and create a registry key with value: "Microsoft Hyper-V", Data:1, and Type:DWORD.

This registry key setting ensures that only one backup job runs at a time on a server that is running Hyper-V.

Serialize virtual machine backups per CSV LUN

This form of serialization limits the number of virtual machine backups that occur on a single Cluster Shared Volumes (CSV) logical unit number (LUN). The serialization is performed as follows:

1. **Create the DataSourceGroups.xml file**—This file provides DPM with information about the CSV virtual machine deployment configuration and distribution on the various CSV LUN for serialization of backups per CSV LUN.
2. Generate the DataSourceGroups.xml file on a CSV cluster.
3. **Merge the DataSourceGroups.xml file from all CSV clusters**—If you have multiple clusters, merge all the DataSourceGroups.xml files into a single file on the DPM server. Place the DataSourceGroups.xml file on the DPM server. You can skip this step and copy the file directly to %PROGRAMFILES%\Microsoft DPM\DPM\Config if the DPM server protects only one cluster.
4. If a protection group has already been created for the virtual machines, perform the steps in the Modify Protection Group Wizard. If a protection group has not been created, create a new

protection group, and the job serialization that is described in the previous section takes effect.

Create the DataSourceGroups.xml file

1. Generate the DataSourceGroups.xml file by running the DSConfig.ps1 script on each node in a cluster that contains CSV. Repeat this step for each cluster that is protected by a DPM server.

Note the following:

- The DataSourceGroups.xml file must be updated only when virtual machines are added, deleted, or modified in the cluster and when protection is configured for them.
- Regenerate the DataSourceGroups.xml file from the CSV cluster and update the DataSourceGroups.xml file by replacing the existing groups for that cluster with the new groups.

DSConfig.ps1

The following DSConfig.ps1 script creates the DataSourceGroups.xml file by listing all the virtual machines that run on CSV in groups. Each group has the list of all virtual machines that are hosted on one CSV LUN. DPM permits only one backup from one such group at a time.

```
# DSConfig.ps1


$infoText = "This script will generate the DatasourceGroups.xml file in the current path.
After this file is created, merge it with the same file name under
%programfiles%\Microsoft DPM\DPM\Config directory on the DPM server. Read the
documentation for more details."
echo $infoText


$header = "<?xml version=`"1.0`" encoding=`"utf-16`"?> `n <DatasourceGroup
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"
xmlns:xsd=`"http://www.w3.org/2001/XMLSchema`"
xmlns=`"http://schemas.microsoft.com/2003/dls/GroupDatasourceByDisk.xsd`">"
$footer = "</DatasourceGroup>"


import-module -name FailoverClusters


$dir = [guid]::NewGuid()
md $dir


$cluster = get-Cluster
```

```
$FQDN = $cluster.Name + "." + $cluster.Domain
$res = get-clusterresource | where-object { $_.ResourceType.Name -eq "Virtual Machine Configuration"}
foreach ($r in $res)
{
$VmObj = Get-ClusterParameter -inputobject $r | where {$_.Name -eq "VmStoreRootPath"} # Identifies the CSV volume on which the VM is hosted.
$VmName = Get-ClusterParameter -inputobject $r | where {$_.Name -eq "VmId"}
$vol = $vmobj.Value.Split("\")[2] # $vol will return to us the Volume<number> of the CSV on which the VM resides.
$line = "<Datasource DatasourceName=`"" + $VmName.Value +"`"" + " ProtectedServerName=`"" + $r.OwnerGroup.Name + "."+ $FQDN +"`"" + " WriterId=`"66841cd4-6ded-4f4b-8f17-fd23f8ddc3de`" />"
echo $line >> $dir\$vol # File VolumeX will contain entries for all VMs hosted on CSV VolumeX
}

echo $header > DataSourceGroups.xml
$filelist = dir $dir\Volume*
$GroupEndString = "</Group>"
foreach ($file in $filelist)
{
   $GroupBeginString = "<Group GroupName=`"" + $file.Name + "-" + $FQDN + "`">" # Group name is kept VolumeX itself
   echo $GroupBeginString >> DataSourceGroups.xml
   type $file >> DataSourceGroups.xml # Consolidating groups pertaining to all the volumes.
   echo $GroupEndString >> DataSourceGroups.xml
}

Remove-Item -Force -Recurse $dir

echo $footer >> DataSourceGroups.xml
```

Generate the DataSourceGroups.xml file on a CSV cluster

1. Copy the DSConfig.ps1 file to any one node of a CSV cluster.
2. Run this script in a Windows PowerShell session with elevated privileges and locate the DataSourceGroups.xml file that is generated in the same folder `C:\MyFolder\>DSConfig.ps1`
3. This script generates the DataSourceGroups.xml file in the current path. After this file is created, copy it to the `%programfiles%\Microsoft DPM\DPM\Config` directory on the DPM server.

   Tip
   If you upgraded from DPM 2010, copy the file to the %PROGRAMFILES%\Microsoft DPM\DPM\Config folder. If you install DPM as a new installation, copy the file to %PROGRAMFILES%\System Center 2012\DPM\DPM\Config.
4. You can verify the groupings by opening the XML file that is generated. The following code shows the expected format:

```
<?xml version="1.0" encoding="utf-16"?>
<DatasourceGroup xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.microsoft.com/2003/dls/GroupDatasourceByDisk.xsd">
<Group GroupName="Group1">
<Datasource DatasourceName="EA24071A-7B7B-42CF-AB1D-BBAE49F50632" ProtectedServerName="SCVMM VM-Vol7-03 Resources.CSVSCALE.SCALEDPM01.LAB" WriterId="66841cd4-6ded-4f4b-8f17-fd23f8ddc3de" />
</Group>
</DatasourceGroup>
```

Merge the DataSourceGroups.xml files from all CSV clusters

Note
You can skip this step if the DPM server protects only one CSV cluster. The generated DataSourceGroups.xml file can be used directly on the DPM server.

1. Copy any one of the DataSourceGroups.xml files that was generated to the folder `%Programfiles%\Microsoft DPM\DPM\Config` on the DPM server.
2. Open the file to edit it.

```
<?xml version="1.0" encoding="utf-16"?>
<DatasourceGroup xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
xmlns="http://schemas.microsoft.com/2003/dls/GroupDatasourceByDisk.xsd">
<Group GroupName="Group1">
<Datasource DatasourceName="EA24071A-7B7B-42CF-AB1D-BBAE49F50632" ProtectedServerName="SCVMM VM-Vol7-03 Resources.CSVSCALE.SCALEDPM01.LAB" WriterId="66841cd4-6ded-4f4b-8f17-fd23f8ddc3de" />
</Group>
</DatasourceGroup>
```

3. Copy the <Group> tags from all the DataSourceGroup.xml files that were generated and add the text between the <DataSourceGroup> tags. The DataSourceGroups.xml file now contains one <header> tag, one <DataSourceGroup> tag, and <Group> tags from all CSV clusters.
4. Close the DataSourceGroups.xml file on the DPM server. It is now ready to use.

Migrate to a hardware VSS provider

If you use the default system VSS provider and want to start using the hardware VSS provider, you must do the following:

1. Install the hardware VSS provider on the host computer and ensure that your Storage Area Network (SAN) is configured for hardware snapshots.
2. Delete the %Programfiles%\Microsoft DPM\DPM\Config\DataSourceGroups.xml file from the DPM server.
3. Open the Registry Editor and navigate to HKLM\Software\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBackups.
4. Set the following values:
   - Value: Microsoft Hyper-V
   - Data: 3
   - Value: DWORD
5. To complete this process, you must run the Modify Protection Group Wizard for each protection group that protects the virtual machines on this cluster.

Configure settings for the system VSS provider

If you do not use a hardware Volume Shadow Copy Services (VSS) provider from your storage area network (SAN) vendor to back up Hyper-V virtual machines with Cluster Shared Volumes (CSV) storage, you can use software snapshots to back up your virtual machines. We

recommend that virtual machines that are deployed on CSV should be backed up serially by the following actions:

- Serialize virtual machine backups per node
- Serialize virtual machine backups per CSV LUN

If you use the default system VSS provider and want to start using the hardware VSS provider, see Migrate from the system software VSS provider to a hardware VSS provider.

Serialize virtual machine backups per node

To serialize virtual machine backups per cluster node, create the following registry key on the System Center 2012 – Data Protection Manager (DPM) server:

Key	HKLM\Software\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBackups
Value	Microsoft Hyper-V
Data	1
Type	DWORD

This registry key setting ensures that only one backup job runs at a time on a server that is running Hyper-V.

Serialize virtual machine backups per CSV LUN

This form of serialization limits the number of virtual machine backups that occur on a single Cluster Shared Volumes (CSV) logical unit number (LUN). The serialization is performed as follows:

1. Create the DataSourceGroups.xml file—This file provides DPM with information about the CSV virtual machine deployment configuration and distribution on the various CSV LUN for serialization of backups per CSV LUN.
2. Generate the DataSourceGroups.xml file on a CSV cluster.
3. Merge the DataSourceGroups.xml files from all CSV clusters—If you have multiple clusters, merge all the DataSourceGroups.xml files into a single file on the DPM server. Place the DataSourceGroups.xml file on the DPM server. You can skip this step and copy the file directly to %PROGRAMFILES%\Microsoft DPM\DPM\Config if the DPM server protects only one cluster.
4. If a protection group has already been created for the virtual machines, perform the steps in the Modify Protection Group Wizard. If a protection group has not been created, create a new protection group, and the job serialization that is described in the previous section takes effect.

Create the DataSourceGroups.xml file

1. Generate the DataSourceGroups.xml file by running the DSConfig.ps1 script on each node in a cluster that contains CSV. Repeat this step for each cluster that is protected by a DPM server.

Note the following:

- The DataSourceGroups.xml file must be updated only when virtual machines are added, deleted, or modified in the cluster and when protection is configured for them.
- Regenerate the DataSourceGroups.xml file from the CSV cluster and update the DataSourceGroups.xml file by replacing the existing groups for that cluster with the new groups.

DSConfig.ps1

The following DSConfig.ps1 script creates the DataSourceGroups.xml file by listing all the virtual machines that run on CSV in groups. Each group has the list of all virtual machines that are hosted on one CSV LUN. DPM permits only one backup from one such group at a time.

```
# DSConfig.ps1


$infoText = "This script will generate the DatasourceGroups.xml file in the current path.
After this file is created, merge it with the same file name under
%programfiles%\Microsoft DPM\DPM\Config directory on the DPM server. Read the
documentation for more details."
echo $infoText


$header = "<?xml version=`"1.0`" encoding=`"utf-16`"?> `n <DatasourceGroup
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"
xmlns:xsd=`"http://www.w3.org/2001/XMLSchema`"
xmlns=`"http://schemas.microsoft.com/2003/dls/GroupDatasourceByDisk.xsd`">"
$footer = "</DatasourceGroup>"


import-module -name FailoverClusters


$dir = [guid]::NewGuid()
md $dir


$cluster = get-Cluster
$FQDN = $cluster.Name + "." + $cluster.Domain
```

```
$res = get-clusterresource | where-object { $_.ResourceType.Name -eq "Virtual Machine Configuration"}
foreach ($r in $res)
{
$VmObj = Get-ClusterParameter -inputobject $r | where {$_.Name -eq "VmStoreRootPath"} # Identifies the CSV volume on which the VM is hosted.
$VmName = Get-ClusterParameter -inputobject $r | where {$_.Name -eq "VmId"}
$vol = $vmobj.Value.Split("\")[2] # $vol will return to us the Volume<number> of the CSV on which the VM resides.
$line = "<Datasource DatasourceName=`"" + $VmName.Value +"`"" + " ProtectedServerName=`"" + $r.OwnerGroup.Name + "."+ $FQDN +"`"" + " WriterId=`"66841cd4-6ded-4f4b-8f17-fd23f8ddc3de`" />"
echo $line >> $dir\$vol # File VolumeX will contain entries for all VMs hosted on CSV VolumeX
}

echo $header > DataSourceGroups.xml
$filelist = dir $dir\Volume*
$GroupEndString = "</Group>"
foreach ($file in $filelist)
{
   $GroupBeginString = "<Group GroupName=`"" + $file.Name + "-" + $FQDN + "`">" # Group name is kept VolumeX itself
   echo $GroupBeginString >> DataSourceGroups.xml
   type $file >> DataSourceGroups.xml # Consolidating groups pertaining to all the volumes.
   echo $GroupEndString >> DataSourceGroups.xml
}

Remove-Item -Force -Recurse $dir

echo $footer >> DataSourceGroups.xml
```

Generate the DataSourceGroups.xml file on a CSV cluster

1. Copy the DSConfig.ps1 file to any one node of a CSV cluster.
2. Run this script in a Windows PowerShell session with elevated privileges and locate the DataSourceGroups.xml file that is generated in the same folder `C:\MyFolder\>DSConfig.ps1`
3. This script generates the DataSourceGroups.xml file in the current path. After this file is created, copy it to the `%programfiles%\Microsoft DPM\DPM\Config` directory on the DPM server.

   Tip
   If you upgraded from DPM 2010, copy the file to the %PROGRAMFILES%\Microsoft DPM\DPM\Config folder. If you install DPM as a new installation, copy the file to %PROGRAMFILES%\System Center 2012\DPM\DPM\Config.
4. You can verify the groupings by opening the XML file that is generated. The following code shows the expected format:

```
<?xml version="1.0" encoding="utf-16"?>
<DatasourceGroup xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.microsoft.com/2003/dls/GroupDatasourceByDisk.xsd">
<Group GroupName="Group1">
<Datasource DatasourceName="EA24071A-7B7B-42CF-AB1D-BBAE49F50632" ProtectedServerName="SCVMM VM-Vol7-03 Resources.CSVSCALE.SCALEDPM01.LAB" WriterId="66841cd4-6ded-4f4b-8f17-fd23f8ddc3de" />
</Group>
</DatasourceGroup>
```

Merge the DataSourceGroups.xml files from all CSV clusters

Note
You can skip this step if the DPM server protects only one CSV cluster. The generated DataSourceGroups.xml file can be used directly on the DPM server.

1. Copy any one of the DataSourceGroups.xml files that was generated to the folder `%Programfiles%\Microsoft DPM\DPM\Config` on the DPM server.
2. Open the file to edit it.

```
<?xml version="1.0" encoding="utf-16"?>
<DatasourceGroup xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
xmlns="http://schemas.microsoft.com/2003/dls/GroupDatasourceByDisk.xsd">
<Group GroupName="Group1">
<Datasource DatasourceName="EA24071A-7B7B-42CF-AB1D-BBAE49F50632" ProtectedServerName="SCVMM VM-Vol7-03 Resources.CSVSCALE.SCALEDPM01.LAB" WriterId="66841cd4-6ded-4f4b-8f17-fd23f8ddc3de" />
</Group>
</DatasourceGroup>
```

3. Copy the <Group> tags from all the DataSourceGroup.xml files that were generated and add the text between the <DataSourceGroup> tags. The DataSourceGroups.xml file now contains one <header> tag, one <DataSourceGroup> tag, and <Group> tags from all CSV clusters.
4. Close the DataSourceGroups.xml file on the DPM server. It is now ready to use.

Migrate from the system software VSS provider to a hardware VSS provider

If you use the default system VSS provider and want to start using the hardware VSS provider, you must do the following:

1. Install the hardware VSS provider on the host computer and ensure that your Storage Area Network (SAN) is configured for hardware snapshots.
2. Delete the %Programfiles%\Microsoft DPM\DPM\Config\DataSourceGroups.xml file from the DPM server.
3. Open the Registry Editor and navigate to HKLM\Software\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBackups.
4. Set the following values:
   - Value: Microsoft Hyper-V
   - Data: 3
   - Value: DWORD
5. To complete this process, you must run the Modify Protection Group Wizard for each protection group that protects the virtual machines on this cluster.

Protecting VMM Hosts

Virtual Machine Manager (VMM) enables you to configure and manage your virtualization host, networking, and storage resources in order to create and deploy virtual machines and services to the private clouds that you created. System Center 2012 – Data Protection Manager (DPM) supports protection and recovery of System Center 2012 – Virtual Machine Manager (VMM).

Important

DPM does not protect earlier versions of VMM.

DPM protects both standalone and clustered configurations of VMM, irrespective of whether they use standalone or clustered versions of SQL Server. The following is a list of support configurations:

- Standalone VMM host + standalone SQL Server (default and named, local and remote)
- Standalone VMM host + clustered SQL Server (default and named, remote)
- Clustered VMM host + standalone SQL Server (default and named, local and remote)
- Clustered VMM host + clustered SQL Server (default and named, remote)

In case of a failover, DPM will continue protection only if the node comes back online. This allows you to perform scheduled failovers without losing protection. But if the node is lost, you have to specifically protect the new node.

Caution

DPM only protects the VMM database. Not all configuration files from the VMM library will be protected.

VMM allows you to use two types of encryption. The first type is the encryption where the key is stored on the VMM host, and the other type is where the key stored along with the Active Directory, called Distributed Key Management (DKM). You should use DKM to ensure high availability of your virtual machines. If you use the DKM method, DPM does not automatically protect the key. You have to protect the key as part of the Active Directory. If you store the key locally, it will be protected as part of the database.

Supported features

- DPM supports initial replication and express full backups for VMM hosts.
- DPM does not support incremental backups for VMM hosts.
- DPM supports recovery to original location and the Copy As File option for VMM hosts.
- DPM does not support recovery to alternate location for VMM hosts.

What is not supported

DPM does not support disaster recovery for VMM.

Known issues

- If VMM is installed by specifying a static IP for the SQL Server, DPM will not be able to protect it.
- If VMM is installed by specifying "localhost" for the SQL Server, DPM will not be able to protect it.
-

Protecting Computers in Workgroups and Untrusted Domains

System Center 2012 – Data Protection Manager (DPM) enables you to protect computers that are in untrusted domains or workgroups.

The security for a production computer in an untrusted domain or workgroup is provided by using a local user account. The DPM agent uses Windows Challenge/Response (NTLM) authentication by using the local user credentials that are specified following the installation of the DPM agent on the protected computer.

Computers in untrusted domains or workgroups require local installation of the DPM agent. They must then be added to DPM by using the Install Agent Wizard, and by providing the same credentials that were specified when configuring the DPM agent by using SetDpmServer with the –isNonDomainServer parameter after the agent is installed on the protected computer. Any updates to the DPM agent on computers in untrusted domains or workgroups require a manual agent upgrade.

Supported Scenarios

	Workgroup	**Untrusted Domain**
Files – Basic - All server and client SKUs	Supported	Supported
Files – Clustering	Not applicable	Not supported
System State – Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012	Supported	Supported
SQL Server– Basic – SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012	Supported	Supported
SQL Server - Mirroring	Not supported	Not supported
SQL Server - Clustering	Not applicable	Not supported
Hyper-V – Basic – Windows Server 2008, Windows 2008 R2	Supported	Supported
Hyper-V – Clustering	Not applicable	Not supported

	Workgroup	Untrusted Domain
Hyper-V – Cluster Shared Volume	Not applicable	Not supported
Exchange – Basic – Exchange Server 2003, Exchange Server 2007, Exchange Server 2010, Exchange Server 2013	Not applicable	Supported
Exchange Server – Clustering	Not applicable	Not supported
Exchange Server – CCR	Not applicable	Not supported
Exchange Server – LCR	Not applicable	Supported
Exchange Server – SCR	Not applicable	Not supported
Exchange Server – DAG	Not applicable	Not supported
Microsoft SharePoint Server	Not supported	Not supported
Laptop and desktop computers	Not supported	Not supported
Bare Metal Recovery	Not supported	Not supported
End User Recovery	Not supported	Not supported
Disaster Protection	Supported, if using certificate-based authentication	Supported, if using certificate-based authentication

In This Section

Security Considerations for Protecting Computers in Workgroups or Untrusted Domains

The following table lists the security considerations when protecting computers on a workgroup or on untrusted domains.

Security Settings	On protected computer in untrusted domain
Connection type: Control data	• Protocol: DCOM • Default Port: 135 • Authentication: NTLM, using credentials specified after DPM agent installation
Connection type: File transfers	• Protocol: WINSOCK • Default Port: 5718 for agent coordinator; 5719 for protection agent. • Authentication: NTLM, using credentials specified after DPM agent installation
DPM account requirements	Local account without administrative rights on the production server.
	Use NTLM v2 for secure communication between DPM and protected computer.
Agent installation	Requires local installation of the DPM agent on the protected computer and running SetDpmServer. After installing the agent, use the Install Agent Wizard to attach the production server to DPM.
Restrictions	• SharePoint and disconnected client protection is not supported in DPM. • DPM disaster recovery is not supported in DPM. • Clustering/mirroring for Files/SQL Server/Exchange Server is not supported in DPM. • Protection of perimeter network (DMZ) machines is not supported in DPM.

Important

Make sure IPSEC does not block communication between DPM server and workgroup machines.

Protecting Workgroup Computers

To protect a computer that is not joined to a domain, you must follow the steps outlined in this topic.

1. Installing Agents on Workgroup Computers
2. Attaching a Workgroup Computer to the System Center 2012 – Data Protection Manager (DPM) server

Important

To protect a computer that is running Windows XP, you must first disable the ForceGuest registry key otherwise NTLM authentication will fail while attaching the computer.

For more information about disabling the ForceGuest registry key, see How to Set Security in Windows XP Professional That Is Installed in a Workgroup.

Installing Agents on Workgroup Computers

You can install a DPM protection agent on a computer by using DPMAgentinstaller.exe (DPMAgentInstall_X64.exe) from the setup DVD.

After installing the agent, you need to run SetDpmServer and specify the local user credentials which would be used for authentication. A local user account will be created and the DPM protection agent would be configured to use this account for authentication.

Syntax: `SetDpmServer.exe -dpmServerName <serverName> -isNonDomainServer -userName <userName> [-productionServerDnsSuffix <DnsSuffix>]`

Parameter	Description
-IsNonDomainServer	Specifies that this server is in a workgroup or an untrusted domain.
-UserName	Creates an NT user account with the specified username for this server to communicate with DPM server. This option should be used along with -IsNonDomainServer.
-ProductionServerDnsSuffix	In case there are multiple DNS suffixes configured for this server, ProductionServerDnsSuffix represents the DNS suffix which DPM server will use to communicate with this server.
-DpmServerName	Name of the DPM server. FQDN if DPM server and protected computer are accessible to each other using FQDNs. NETBIOS if DPM server and protected computer are accessible to each

Parameter	Description
	other using NETBIOS names.

Attaching a Workgroup Computer to the DPM Server

The steps to attach a workgroup computer using DPM Administrator Console are as follows.

1. Start the Protection Agent Installation Wizard from the DPM Administrator Console.
2. Select **Attach** and click **Next**.
3. Enter the computer name, user name, and password for the computer that you want to attach to. This should be the same as the login credentials specified during agent installation on that computer. Click **Next**.
4. Review the information on the **Summary** page, and then, if the information is correct, click **Install**. After the attach action is completed successfully, click **Close**.

Attaching a Workgroup Computer by Using DPM Management Shell

You can also attach a workgroup computer by using the Attach-NonDomainServer script in DPM Management Shell.

Syntax: `Attach-NonDomainServer.ps1 -DPMServername [Name of DPM server] -PSName [Protected computer] -Username [username] -Password [Password]`

This script registers the specified workgroup computer to be protected with this DPM server, creates a local user account using the specified credentials, and configures DPM to use these credentials to authenticate the workgroup computer.

Important
Before attaching the workgroup computer to the DPM server by using the DPM Administrator Console or DPM Management Shell, you must install the DPM agent and run SetDpmServer.exe on the workgroup computer.

Important
If you use the NetBIOS name of the DPM server in the SetDPMServer command, you also must use the NetBIOS for the protected computer when you attach the computer. This also applies if you use the fully qualified domain name (FQDN) of the DPM server.

Examples

Example 1

Configuring a workgroup computer for protection after agent is installed.

On the workgroup computer, run `SetDpmServer.exe -DpmServerName Server01 -isNonDomainServer -UserName mark`.

On the DPM server, run `Attach-NonDomainServer.ps1 –DpmServername Server01 -PSName Finance01 -Username mark`.

Important

Because the workgroup computers are typically accessible only by using NetBIOS name, the value for DPMServerName must be the NetBIOS name.

Example 2

Configuring a workgroup computer with conflicting NetBIOS names for protection after agent is installed.

On the workgroup computer, run `SetDpmServer.exe -dpmServerName Server01.corp.contoso.com -isNonDomainServer -userName mark -productionServerDnsSuffix widgets.corp.com`.

On the DPM server, run `Attach-NonDomainServer.ps1 -DPMServername Server01.corp.contoso.com -PSName Finance01.widgets.corp.com -Username mark`.

Protecting Computers on Untrusted Domains

Prerequisites

- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) on the protected computer
- Each machine (virtual machines included) must have its own certificate.

Certificate Requirements

- X.509 V3 certificates
- Enhance Key Usage should have client authentication and server authentication.
- Key length should be at least 1024 bits.
- Key type should be **exchange**.
- System Center 2012 – Data Protection Manager (DPM) does not support self-signed certificates.

Setting up DPM to Protect Computers Using Certificates

1. Generate a certificate from the certification authority for the DPM server
2. Import the certificate to the personal certificate store of Local Computer account and then run **Set-DPMCredentials** to configure the DPM server.

   This generates a metadata file that is required at the time of each agent install in untrusted domain.

Note

If this file is lost or deleted, you can recreate it by running Set-DPMCredentials -action regenerate.

The DPM server is now successfully configured for use with certificates.

3. Repeat these steps on every DPM server that will protect a computer in a workgroup or in an untrusted domain.

Installing Agents on Computers on Untrusted Domains

1. You can install a DPM protection agent on a computer using DPMAgentinstaller.exe (DPMAgentInstall_X64.exe) from the setup DVD.
2. After installing the agent, you need to run SetDpmServer and specify the local user credentials which would be used for authentication. A local user account will be created and the DPM protection agent would be configured to use this account for authentication.

   Syntax: `SetDpmServer.exe -dpmServerName <serverName> -isNonDomainServer -userName <userName>`

Parameter	Description
-IsNonDomainServer	Specifies that this server is in a workgroup or an untrusted domain.
-UserName	Creates a Windows NT user account with the specified username for this server to communicate with DPM server. This option should be used along with -IsNonDomainServer.
-ProductionServerDnsSuffix	In case there are multiple DNS suffixes configured for this server, ProductionServerDnsSuffix represents the DNS suffix which DPM server will use to communicate with this server.
-DpmServerName	Name of the DPM server. FQDN if DPM server and protected computer are accessible to each other using FQDNs. NETBIOS if DPM server and protected computer are accessible to each other using NETBIOS names.

Attaching a Computer on an Untrusted Domain to the DPM Server

The steps to attach a computer on an untrusted domain using DPM Administrator Console are as follows.

1. Start the Protection Agent Installation Wizard from the DPM Administrator Console.
2. Select **Attach** and click **Next**.
3. Enter the computer name, user name and password for the computer you want to attach to. This should be the same as the login credentials specified during agent installation on that computer. Click **Next**.
4. Review the information on the Summary page and click **Install** if the information is correct. Click **Close** once the attach action is successful.

Attaching Computers Using DPM Management Shell

You can also attach a computer on an untrusted domain through DPM Management shell using Attach-NonDomainServer script.

Syntax: `Attach-NonDomainServer.ps1 -DPMServername [Name of DPM server] -PSName [Protected computer] -Username [username]`

This script registers the specified computer to be protected with this DPM computer, creates a local user account using the specified credentials and configures DPM to use these credentials to authenticate to the computer.

Important
DPM agent must be installed and SetDpmServer.exe must be run on the computer, before attaching the computer to DPM server using the DPM Administrator Console or Management shell.

Important
If you use NetBIOS name of the DPM server in the SetDPMServer command, you must use the NetBIOS for the protected computer also during attach and vice versa if you are using FQDN.

Using Set-DPMCredentials

Syntax: `Set-DPMCredentials [-DPMServerName <String>] [-Type <AuthenticationType>] [Action <Action>] [-OutputFilePath <String>] [-Thumbprint <String>] [-AuthCAThumbprint <String>]`

Parameter	Description	Value
Type	Type of autentication	Certificate
Action	Intent for running the command	Regenerate, Configure

Parameter	Description	Value
OutputFilePath	Location of the output file (used in Set-DPMServer on the protected computer).	
Thumbprint	Thumbprint of the certificate (to be used on the DPM server).	
AuthCAThumbprint	Thumbprint of the certifying authority in the trust chain of the certificate. Optional. If not specified, Root will be used.	

Example 1

This cmdlet will generate a file in c:\CertMetaData\ with name CertificateConfiguration_<DPM SERVER FQDN>.bin

```
Set-DPMCredentials -DPMServerName dpmserver.contoso.com -Type Certificate -Action
Configure –OutputFilePath c:\CertMetaData\ –Thumbprint
"cf822d9ba1c801ef40d4b31de0cfcb200a8a2496"
```

Where dpmserver.contoso.com is the name of the DPM server and "cf822d9ba1c801ef40d4b31de0cfcb200a8a2496" is the thumbprint of the DPM server certificate.

Example 2

This cmdlet will regenerate the lost configuration file in the folder c:\CertMetaData\.

```
Set-DPMCredentials -DPMServerName dpmserver.contoso.com -Type Certificate "-
OutputFilePath c:\CertMetaData\ -Action Regenerate
```

Updating Password for Workgroup or Untrusted Computers

When you install an agent locally on a workgroup computer, you specify the credentials to SetDpmServer to generate a local account and System Center 2012 – Data Protection Manager (DPM) uses these credentials to communicate with the agent on the workgroup computer.

Procedure to update password

Follow these steps to update the password for the user account being used for workgroup computer protection.

1. On the protected computer, `SetDpmServer.exe -dpmServerName <serverName> -isNonDomainServer -updatePassword`

   Important
   You must use the same naming convention (FQDN or NetBIOS) as you did when configuring protection.
2. On the DPM server, run the Update-NonDomainServerInfo cmdlet and provide appropriate information along with new password.
3. Refresh the agent information for the protected computer.

Examples

Example 1

Changing the password when the computer was protected using NetBIOS name.

On the protected computer, run `SetDpmServer.exe -dpmServerName Server01 -isNonDomainServer –UpdatePassword`

On the DPM server, run `Update-NonDomainServerInfo –PSName Finance01 –dpmServerName Server01.`

When prompted, provide the same password as the one you provided in Step 1.

Example 2

Changing the password when the computer was protected using FQDN.

On the protected computer, run `SetDpmServer.exe -dpmServerName Server01.corp.contoso.com -isNonDomainServer –UpdatePassword`

On the DPM server, run `Update-NonDomainServerInfo –PSName  Finance01.worlwideimporters.com –dpmServerName Server01.contoso.com.`

When prompted, provide the same password as the one you provided in Step 1.

Certificate-Based Authentication for Computers in Untrusted Domains

System Center Data Protection Manager 2010 supports protection of computers in workgroups and untrusted domains using local accounts and NTLM. However, in scenarios where an organization does not allow creation of local accounts, this solution does not work.

System Center 2012 – Data Protection Manager (DPM) allows you to use certificates to authenticate computers in workgroups or untrusted domains.

Currently, DPM supports the following data sources for certificate-based authentication when they are not in trusted domains:

- File server
- Hyper-V

DPM also supports these data sources in clustered deployments.

The following data sources are not supported:

- DPM
- SQL Server
- Exchange Server
- Client computers
- SharePoint Server
- Bare Metal Recovery
- System State

DPM supports protecting DPM servers that are in untrusted domains if the primary and secondary DPM servers are in domains that trust each other or if they are in the same domain.

Note

DPM also supports using certificate-based authentication for computers in trusted domains.

Prerequisites

- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) on the protected computer
- Each machine (virtual machines included) must have their own certificate.

Certification Requirements

- X.509 V3 certificates
- Enhance Key Usage should have client authentication and server authentication.
- Key length should be at least 1024 bits.
- Key type should be **Client/Server Authentication**.
- DPM does not support self-signed certificates.

In This Section

- Setting Up Protection for Computers Using Certificates
- Using Set-DPMCredentials
- Using SetDPMServer
- Using Attach-ProductionServerWithCertificate

Setting Up Protection for Computers Using Certificates

Setting up DPM server to protect computers using certificates

Repeat these steps on every DPM server that will protect a computer in a workgroup or in an untrusted domain.

1. Generate a certificate from the certification authority for the DPM server.
2. Import the certificate to the personal certificate store of Local Computer account and then run Using Set-DPMCredentials to configure the DPM server.

   Note

   This generates a metadata file that is required at the time of each agent install in untrusted domain.

   Tip
   If this file is lost or deleted, you can recreate it by running `Set-DPMCredentials -action regenerate`.
3. The DPM server is now successfully configured for use with certificates.

Setting up a computer for protection by DPM

Repeat these steps on every computer you want to protect that is in a workgroup or in an untrusted domain.

1. Install the DPM protection agent on a computer and then attach it to the DPM server. For more information, see Installing and Configuring Protection Agents.
2. Generate a certificate from the certification authority for the computer you want to protect.
3. Import the certificate to the personal certificate store of Local Computer.
4. Run Using SetDPMServer to complete the setup.

   The program saves a file locally with the certificate metadata. Later, this file is used to attach this agent to the DPM server.

   Tip
   If this file is lost or deleted, you can recreate it by running SetDPMServer.exe.

5. Copy the generated Cert.xml file to the DPM server.

Attaching an untrusted computer to DPM

1. Run Using Attach-ProductionServerWithCertificate to attach an untrusted computer to the DPM server.
2. Repeat the step for every untrusted computer.

Using Set-DPMCredentials

Syntax

Set-DPMCredentials [–DPMServerName <String>] [–Type <AuthenticationType>] [Action <Action>] [–OutputFilePath <String>] [–Thumbprint <String>] [–AuthCAThumbprint <String>]

Parameter	Description	Value
Type	Type of authentication.	Certificate
Action	Intent for running the command	Regenerate, Configure
OutputFilePath	Location of the output file (used in Set-DPMServer on protected computer)	
Thumbprint	Thumbprint of the certificate (to be used on DPM server)	
AuthCAThumbprint	Thumbprint of the certifying authority in the trust chain of the certificate. Optional. If not specified, Root will be used.	

Example 1

Set-DPMCredentials -DPMServerName dpmserver.contoso.com -Type Certificate -Action Configure -OutputFilePath c:\CertMetaData\ –Thumbprint “cf822d9ba1c801ef40d4b31de0cfcb200a8a2496”

Where dpmserver.contoso.com is the name of the DPM server and “cf822d9ba1c801ef40d4b31de0cfcb200a8a2496” is the thumbprint of the DPM server certificate.

This cmdlet will generate a file in c:\CertMetaData\ with name CertificateConfiguration_<DPM SERVER FQDN>.bin

Example 2

Set-DPMCredentials -DPMServerName dpmserver.contoso.com -Type Certificate “-OutputFilePath c:\CertMetaData\ -Action Regenerate

This cmdlet will regenerate the lost configuration file in the folder c:\CertMetaData\.

Using SetDPMServer

Syntax

SetDPMServer.exe -dpmCredential CertificateConfiguration_<DPMServerFqdn>.bin -OutputFilePath <Output File Path> -Thumbprint <Certificate Thumbprint> [-AuthCAThumbprint <authorized CA thumbprint>]

Parameter	Description
DPMCredential	The credential file that was the output of Set-DPMCredentials.
OutputFilePath	The location of the output file that used in Attach-ProductionServerWithCertificate on DPM server
Thumbprint	The thumbprint of the certificate, which is to be used on a protected computer
AuthCAThumbprint	The thumbprint of the certifying authority in the trust chain of the certificate. This is an optional parameter. If it is not specified, Root will be used.

Example

C:\Program Files\Microsoft Data Protection Manager\DPM\bin>SetDpmServer.exe -dpmcredential CertificateConfiguration_dpmserver.contoso.com.bin -OutputFilePath c:\CertMetaData -Thumbprint 5b3db055d3f769bc58e2f6c0703bac4ea8fbd8da

CertificateConfiguration_dpmserver.contoso.com.bin is the DPMServerCertificateConfiguration file, which was generated on DPM server by running Set-DPMCredentials; and

5b3db055d3f769bc58e2f6c0703bac4ea8fbd8da is the CertificateThumbprint of the protected computer certificate.

This will generate PS certificate configuration file at C:\CertMetaData with name CertificateConfiguration_ <PSServerFqdn>.bin.

Using Attach-ProductionServerWithCertificate

Syntax

Attach-ProductionServerWithCertificate.ps1 [-DPMServerName <String>] [-PSCredential <String>] [<CommonParameters>]

Parameter	Description
PSCredential	The credential file that was the output of Set-DPMServer.

Example

Attach-ProductionServerWithCertificate.ps1 -DPMServerName dpmserver.contoso.com –PSCredential CertificateConfiguration_DocServer.fourthcoffee.com.bin

Administering DPM Servers

As a system administrator, you are accustomed to managing servers in different roles. You plan your maintenance routines to accommodate each server's role, and you take that role into account when making structural changes such as changing the server name or relocating the server. So what do you need to consider when the role of a server running System Center 2012 – Data Protection Manager (DPM) is added to your network structure?

This section discusses performing common maintenance tasks on DPM servers. It provides guidance on making changes to server configurations after DPM is set up and on how DPM manages time zones. This section provides information about configuring firewalls on both the DPM server and protected computers so that communication can be maintained. This section also provides recommendations for monitoring DPM and offers methods for monitoring.

In This Section

Performing General DPM Server Maintenance

Performing General DPM Server Maintenance

General maintenance includes tasks such as disk and file maintenance, updating operating systems and applications, and protecting data by using antivirus software and performing regular backups. Some special considerations apply when you are performing server maintenance on DPM servers.

In This Section

Using Windows Maintenance Tools on the DPM Server

In general, you can add the DPM server to your regular maintenance schedule and use the maintenance tools provided in Windows Server 2008. However, you need to be aware of some considerations that apply to a few specific tools when you use them with DPM. Those tools are listed in the following table.

Windows Maintenance Tools and DPM

Windows Tool	Considerations
Disk Cleanup: Use to remove temporary files, Internet cache files, and unnecessary program files.	Disk Cleanup is not available for replica volumes and recovery points volumes in the DPM storage pool.
Disk Defragmenter: Use to analyze volumes for the amount of fragmentation and to defragment volumes.	You should not run Disk Defragmenter on disks that are members of the storage pool on the DPM server. Knowledge Base article 312067 explains the issue with Disk Defragmenter as follows: "The System Shadow Copy provider uses a copy-on-write mechanism that operates at a 16-KB block level. This is independent of the

Windows Tool	Considerations
	file system's cluster allocation unit size. If the file system's cluster size is smaller than 16 KB, the System Shadow Copy provider cannot easily determine that disk defragmentation I/O is different from typical write I/O, and performs a copy-on-write operation. This might cause the Shadow Copy storage area to grow very quickly. If the storage area reaches its user-defined limit, the oldest shadow copies are deleted first." For more information about this issue, see the Microsoft Knowledge Base article Shadow copies may be lost when you defragment a volume.
Chkdsk.exe: Use to check the file system and file system metadata for errors and to display a status report of its findings.	Do not run chkdisk on DPM replica and recovery point volumes. Chkdsk causes the volumes to dismount, and if data is written to the replica volume while the recovery point volume is dismounted, it might cause a complete loss of recovery points.

Applying Operating System Updates to the DPM Server

An important part of computer maintenance is ensuring that operating systems and software are up to date. Updates—known as fixes, hotfixes, patches, service packs, and security rollup packages — help to protect computers and data.

You can use your preferred method for deploying software updates, such as Automatic Updates or Windows Server Update Services, both on DPM servers and on protected computers. Because some software updates require a computer restart, you should schedule or perform the updates at times that have the least impact on protection operations.

You should also check regularly for updates to DPM and pre-requisite software. For a list of the pre-requisite software, see **On the DPM server**.

Updates to DPM are available through Microsoft Update, which is a service from Microsoft that delivers required updates from the Microsoft Update Catalog. The Microsoft Update Catalog is a repository for Microsoft software updates and contains updates that address security and reliability issues. The Microsoft Update service queries the Microsoft Update Catalog to determine what updates are available for the computer on which Microsoft Update is installed.

You can subscribe to Microsoft Update at any time on the Microsoft Update Web site.

See Also

Running Antivirus Software on the DPM Server

Using Windows Maintenance Tools on the DPM Server

Running Antivirus Software on the DPM Server

To prevent file conflicts between DPM and antivirus software, on the DPM server, disable real-time monitoring by the antivirus software of the following directories in the DPM program files:

- \XSD
- \Temp\MTA

DPM is compatible with most popular antivirus software products. However, antivirus products can affect DPM performance and, if not configured properly, can cause data corruption of replicas and recovery points. To mitigate these issues, consider taking the following actions:

- **Disable real-time monitoring of dpmra.exe on the DPM server.**

  To minimize performance degradation, disable antivirus real-time monitoring of replicas and transfer logs for all protected volumes by disabling real-time monitoring of the DPM process dpmra.exe, which is located in the folder Program Files\Microsoft Data Protection Manager\DPM\bin.

  Real-time monitoring of replicas degrades performance because it causes the antivirus software to scan the replicas each time DPM synchronizes with the protected server and to scan all affected files each time DPM applies changes to the replicas. The problem is resolved when you disable the feature for the replicas. For information about configuring real-time monitoring based on process name, see your antivirus product documentation.

- **Disable real-time monitoring of csc.exe on the DPM server.**

  If you experience degraded performance while using DPM Administrator Console, disable real-time monitoring of the csc.exe process, which is located in the folder Windows\Microsoft.net\Framework\v2.0.50727\csc.exe. The csc.exe process is the C# compiler. Real-time monitoring of the csc.exe process can degrade performance because it causes the antivirus software to scan files that the csc.exe process emits when it generates XML messages. For information about configuring real-time monitoring based on process name, see your antivirus product documentation.

- **Delete infected files on protected servers and the DPM server.**

  To prevent data corruption of replicas and recovery points, configure the antivirus software to delete infected files rather than automatically cleaning or quarantining them. Automatic

cleaning and quarantining can result in data corruption because these processes cause the antivirus software to modify files, making changes that DPM cannot detect.

Whenever DPM attempts to synchronize a replica that has been modified by another program, data corruption of the replica and recovery points can result. Configuring the antivirus software to delete infected files resolves this problem. For information about configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

Important

You must run a manual synchronization with consistency check job each time that the antivirus software deletes a file from the replica, even though the replica will not be marked as inconsistent.

See Also

Applying Operating System Updates to the DPM Server

Using Windows Maintenance Tools on the DPM Server

Performing DPM Server Management Tasks

This section provides instructions and guidelines for managing the DPM server and making changes after the initial DPM configuration.

In this section

Managing the DPM Database Volume

Finding DPM Servers in Active Directory Domain Services

How to Migrate a DPM Server to New Hardware

Restarting the DPM Server

Moving the DPM Server to a New Domain

Renaming the DPM Server

Changing the SQL Server Instance Used by DPM

Coordinating Protection Across Time Zones

How to Change the Time Zone of the DPM Server

Using a Backup Network Address

Moving the DPM Server to a Different Computer

Removing a Protected Computer

Replacing the DPM System Disk

Managing the DPM Database Volume

The DPM database (DPMDB) location is specified during DPM installation. When you use the dedicated instance of SQL Server installed by DPM, the default location of DPMDB is C:\Program Files\Microsoft DPM\DPM\DPMDB. When you use an existing instance of SQL Server for DPM, the default location of DPMDB is the path on the SQL Server where the SQL databases are located.

To determine which instance of SQL Server is being used by DPM, in DPM Administrator Console, click the Information icon.

Space in the volume on which DPMDB is stored can be increased by the following methods:

- Deleting unneeded files from that volume (such as temporary files)
- Increasing the size of the volume

See Also

Performing DPM Server Management Tasks

Finding DPM Servers in Active Directory Domain Services

Active Directory Domain Services is designed to provide information about directory objects when queried by either users or programs. When you install DPM on a server that is a member of a domain, a service connection point is registered in Active Directory Domain Services. The information registered with the service connection point makes it possible for you to search Active Directory Domain Services to locate computers running DPM.

Note

If DPM is installed on a server that is not a member of a domain and the server is then added to a domain, the service connection point will not be registered in Active Directory Domain Services.

To locate DPM servers in Active Directory Domain Services, use a query tool such as Adsiedit to find all computers in the domain that have a “serviceClassName=MSDPM” service connection point.

Note

Adsiedit is a Microsoft Management Console (MMC) snap-in that is available when you install the Windows Server 2003 Support Tools. For more information about using Adsiedit, see ADSI Edit Overview on the Windows Server 2003 TechCenter.

To install Windows Server 2003 support tools

1. Insert the Windows Server 2003 CD.
2. Browse to the \support\tools directory.
3. Double-click the suptools.msi file name.

To locate DPM servers by using Adsiedit

1. Run adsiedit.msc.
2. Right-click the **Domain** node, point to **New**, and then click **Query**.
3. Enter a name for the query, such as “MSDPM Servers.”
4. Choose the **Machines** node as the root of the search.
5. In **Query String**, enter **serviceClassName=MSDPM**.
6. Click **OK** to display a query node under the **Domain** node.
7. Select the query node; the servers on which DPM is installed are displayed in the list pane.

See Also

Performing DPM Server Management Tasks

How to Migrate a DPM Server to New Hardware

To ensure data source protection and availability of recovery points across the process, you should create a plan for the DPM server migration process, including considerations of the following factors:

- The service level agreement (SLA) that you need to maintain for the period of the migration.
- The length of time that you can continue running the existing DPM server before retiring or repurposing it.
- Maintenance windows for the protected computers.

Important
You must be an administrator on the local computer to do migration.

To migrate a DPM server to new hardware

1. Install DPM on a new server. For more information, see Installing DPM.
2. Identify a protected computer to migrate and run `SetDPMServer.exe -DPMServerName <Name of new DPM server>` on the protected computer.
3. Run the PowerShell script `Attach-ProductionServer.ps1` from the DPM Management Shell on the DPM server.

Note

For more information about using the Attach-ProductionServer script, see Installing Protection Agents Manually.

4. Create protection groups on the new DPM server for the protected computers. For more information, see Configuring DPM.
5. Maintain the previous DPM server until the recovery points from inactive replicas on it are no longer required.

See Also

Performing DPM Server Management Tasks

Restarting the DPM Server

If you need to restart the DPM server for any reason, check the **Monitoring** task area in DPM Administrator Console for jobs currently running, and then follow these guidelines:

- If there are no jobs currently running or scheduled to run during the time required for the restart, restart the DPM server.
- If a synchronization with consistency check job is running, restart the DPM server. Synchronization with consistency check will resume at the next scheduled time or you can retry the job manually.
- If a replica creation job is running, postpone the restart until the job is completed. If the restart cannot be postponed, you must run synchronization with consistency check manually for the replica after you restart the DPM server.
- If any synchronizations or express full backups are scheduled to run during the restart, either postpone the restart until the recovery points are created or re-run the synchronizations and create the recovery points manually after you restart the DPM server.
- If any jobs that use the tape library are running, postpone the restart until the jobs are complete. If the restart cannot be postponed, the following job types will be canceled by the restart and must be re-run after the restart:
  - Back up to tape
  - Copy to tape
  - Recovery from tape
  - Tape verification
- If you are erasing a tape, postpone the restart until the current job is complete. Cancel any pending tape erase jobs, restart the computer, and then reschedule the canceled tape erase jobs.

See Also

Performing DPM Server Management Tasks

Moving the DPM Server to a New Domain

You cannot change the domain of the DPM server.

See Also

Performing DPM Server Management Tasks

Renaming the DPM Server

You cannot rename a DPM server.

See Also

Performing DPM Server Management Tasks

Changing the SQL Server Instance Used by DPM

DPM uses a specified instance of SQL Server to stores its database. You specify the instance of SQL Server that DPM will use during the DPM installation process. It is possible to change the instance of SQL Server that a DPM server uses only by uninstalling and reinstalling DPM.

If you need to change the instance of SQL Server for a DPM server, use the following process:

1. Ensure that you have a recent backup of the DPM database (DPMDB).
2. Uninstall DPM and choose to retain data.
3. Install DPM and specify a new instance of SQL Server. For more information, see Installing DPM.
4. Restore DPMDB to the new instance of SQL Server, run DpmSync, and then run a consistency check for the data sources protected by the DPM server.

This process depends on the availability of a backup of the DPM database. For more information about backing up and restoring the DPM database, see Setting Up Disaster Recovery.

See Also

Performing DPM Server Management Tasks

Coordinating Protection Across Time Zones

In an Active Directory domain, the system times on servers are synchronized according to the time zone configuration of each server. However, when a DPM server is protecting computers that are in a different time zone from the DPM server, you must consider the time differences when scheduling jobs, reviewing reports, managing alerts, and performing data recovery.

How DPM Displays Times

DPM automatically schedules synchronization and recovery point jobs in the time zone of the protected computer. In all other areas of DPM Administrator Console, system times are displayed in the time zone of the DPM server. Although you schedule jobs to run in the time zone of the protected computer, the start times and recovery point times of the jobs are displayed in the time zone of the DPM server.

For example, suppose that your DPM server is located in Berlin and a protected file server is located in Reykjavik, which is two hours earlier than Berlin. When you schedule synchronization and the recovery point for 6:00 P.M., the jobs run at 6:00 P.M. in Reykjavik time, the time on the file server. However, if a user in Reykjavik requests to have data recovered to its state as of 6:00 P.M. yesterday, you must search for the recovery point that represents 8:00 P.M. Berlin time, because the DPM recovery user interface represents recovery point times in the time zone of the DPM server.

In DPM Administrator Console, in the Recovery task area, the **Last Modified** column displays the date and time of the most recent changes to the file, which could be either changes to the contents or changes to the metadata.

Work hours for network bandwidth usage throttling use the time zone of the protected computer.

Scheduling Initial Replica Creation

Initial replica creation jobs are scheduled by using the time of the DPM server; you cannot schedule a job to run at a time that is already in the past for the DPM server, even if that time is still in the future for the protected computer. In our example of a DPM server in Berlin that is protecting a file server in Reykjavik, there is a two hour difference between the times of the two servers. At 9:00 P.M. Berlin time, you cannot schedule an initial replica creation job for the file server in Reykjavik at 8:00 P.M. on the same day, even though it is not yet 8:00 P.M. in Reykjavik, because that time is in the past for the DPM server in Berlin.

Initial replica creation jobs occur by using the time of the protected computer. This means that if you schedule an initial replica creation job for the file server in Reykjavik to occur at 9:00 P.M. on a set date, the job will run at 9:00 P.M. Reykjavik time on that day.

Suppose the DPM server in Berlin is also protecting a file server in Sofia, which is an hour later than Berlin. At 8:00 P.M. in Berlin, you schedule an initial replica creation job for the file server in Sofia to begin at 8:30 P.M. You can schedule it for 8:30 P.M. because that time is in the future for

the DPM server. However, because it is already past 8:30 P.M. in Sofia, the initial replica creation will begin immediately.

How DPM Manages Daylight Saving Time

DPM automatically identifies the time zone of a protected computer during installation of the protection agent. Providing that both the DPM server and the protected computer reside in time zones that observe the same rules for daylight saving, DPM also automatically adjusts to accommodate the start and end of daylight saving time. However, if the DPM server and the protected computer reside in locations that observe different rules for daylight saving time—for example, if the DPM server resides in a location that observes daylight saving time and the protected server resides in a location that does not—the start of daylight saving time disrupts the time zone offsets between DPM and the protected computer.

To resolve this problem, you can force the DPM server to reset the time zone offset by removing the data sources from protection and then adding the data sources back to protection groups.

See Also

How to Change the Time Zone of a File Server or Workstation

How to Change the Time Zone of the DPM Server

Performing DPM Server Management Tasks

How to Change the Time Zone of the DPM Server

You can use the following procedure to change the time zone of the DPM server.

To change the time zone of the DPM server

1. Close DPM Administrator Console.
2. Stop the DPM service (MsDpm.exe).
3. Change the time zone on the DPM server in Control Panel by using the **Time Zone** tab in the **Date and Time Properties** dialog box.
4. Open DPM Administrator Console. This restarts the DPM service as well.
5. In DPM Administrator Console, click **Options** in the **Action** pane.
6. In the **Options** dialog box, on the **Auto Discovery** tab, change the time of day for auto discovery to run, and then click **OK**.

   Changing the schedule for auto discovery causes all DPM jobs to be regenerated with the new time zone of the DPM server.

See Also

How to Change the Time Zone of a File Server or Workstation

Coordinating Protection Across Time Zones

Performing DPM Server Management Tasks

Using a Backup Network Address

System Center 2012 – Data Protection Manager (DPM) allows you to configure a backup network address to ensure that DPM backups do not slow down your primary network. The backup network address is created when you put separate network adapters on the DPM server and the protected servers and connect them through a separate LAN. As a result, backup data traffic does not impact the primary network.

You can set up your backup network address using DPM Management Shell (PowerShell) cmdlets.

Setting up your network

Before you can set up a backup network address, you need to:

1. Ensure that the name resolution of the protected server on the DPM server can resolve the backup address of the protected server and vice versa.
2. Configure the backup subnet and the corresponding subnet mask using Add-DPMBackupNetworkAddress.

   Note
   The subnet should cover the entire range of network addresses for the DPM server and the servers you intend to protect.
3. Restart the DPM agent on the DPM server and the protected computers. It may cause ongoing tasks to fail. Post a restart, watch out for alerts, and perform the recommended actions, if needed.

Example

This example details the process of setting up a backup network address for a DPM server protecting another server. All names and addresses are hypothetical and for illustration only.

The existing backup setup consists of dpm.x.y.com protecting ps.x.y.com. Name lookup using “nslookup” on either server returns the following IPs (that is, each IP address is visible to each node):

Note
The name lookups must be performed on the FQDNs; for example, “nslookup ps.x.y.com”.

Server	NIC address
DPM server (dpm.x.y.com)	10.10.12.89
Protected computer (ps.x.y.com)	10.10.12.90

Now, to set up a backup network, another NIC is added to each of the above servers and connected to another network such as 192.168.1.0/24 with a corresponding subnet mask 255.255.255.0. When the network and NICs are configured, the name lookup using “nslookup” returns two addresses per server as given below.

Server	Primary NIC address	Backup NIC address
DPM server	10.10.12.89	192.168.1.23
Protected computer	10.10.12.90	192.168.1.24

We recommend that you verify whether the DPM server is able to ping the protected computer’s backup network address (192.168.1.24). Similarly, the protected computer should be able to ping the DPM server’s backup network address (192.168.1.23).

At this stage, backup LAN configuration information is added to the DPM server as follows:

Add-DPMBackupNetworkAddress -DpmServername DPM -Address 192.168.1.0/24 -SequenceNumber 1

Note

The “Address” parameter specifies the backup network/subnet.

The DPM agents on TestingServer and the protected server are restarted (“net stop dpmra” followed by “net start dpmra” on each server).

Finally, a backup task is triggered and the NIC used for backup data transfer verified using taskmgr->networking. The backup task must correspond to a data source on the protected server.

Note

Add-DPMBackupNetworkAddress enables you to configure more than one backup network. You can also use the primary network as a fallback network while using the backup network. In the above example, the primary network could also have been added with SequenceNumber 2. As a result, if the primary network is removed and the name lookup of servers no longer returns 192.168.1.0/24 addresses, DPM can automatically start using the primary network for backup data traffic.

Moving the DPM Server to a Different Computer

This topic describes the steps that you must take to move a DPM server to a different computer. If you have a DPM server that is running on a server (for example, Server1) and you decide to move it to a different server (for example, Server2), then you must perform the following procedure.

On Server1, follow these steps:

1. Back up the DPM database.
2. Note the updates installed on DPM by using the **Add or Remove Programs** item in Control Panel.

On Server2, follow these steps:

1. Remove Server1 from the network. Ensure that the fully qualified domain name (FQDN) of Server1 and Server2 is the same.
2. Install DPM.
3. Install all the DPM updates that were previously installed on Server1.
4. Restore the DPM database.

Note
The FQDN and version of DPM on both Server1 and Server2 must be the same.

To back up the DPM database

1. At the command prompt, run DPMBackup.exe -db, located at **Microsoft Data Protection Manager\DPM\bin**.
2. In the console tree of the backup program, browse to **Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\Database Backups**. The file name of the DPM database backup is **DPMDB.bak**.
3. Select the media to which you want to back up the database.
4. Start the backup.

To install DPM

For information about how to install DPM, see Installing DPM.

To restore the DPM database

1. At the command prompt, **type DpmSync –restoredb –dbloc** <DPMDB location>, and then press ENTER.

   Note
   The default location of DPMDB is C:\Program Files\Microsoft DPM\DPM\DPMDB. When you use an existing instance of SQL Server for DPM, the default location of DPMDB is the path on the instance of SQL Server where the SQL databases are located.
2. At the command prompt, type **DpmSync -sync**.
3. After the new installation is complete and the database is restored, in DPM Administrator Console, in the **Monitoring** task area, check for protection jobs that failed. Manually restart any failed jobs.
4. After you restart the failed jobs, you must perform a consistency check for all data sources. For more information about how to perform a manual consistency check, see "How to synchronize a replica" in DPM Help.

Removing a Protected Computer

If you don't want to continue protection of a protected computer, you can remove the protected computer from DPM by using the Remove-ProductionServer.ps1. This will not uninstall the DPM protection agent from the protected computer. You must uninstall the agent manually.

Running this script will remove the protected computer from the DPM database (DPMDB) and from the trusted groups DCOMTrustedMachines and DPMRADMTrustedMachines.

Remove-ProductionServer.PS1

Syntax: `Remove-ProductionServer.ps1 -DPMServername [DPMServerName] -PSName [ProtectedComputerName]`

Parameter	Description
-DPMServername	Name of the DPM server.
-PSName	Name of the protected computer that must be removed. If the computer was protected using an FQDN or NETBIOS name, you must use that name here.

Important

There should be no actively protected data sources on the computer you are trying to remove.

Replacing the DPM System Disk

The following procedure helps you replace the system disk on your DPM server or replace the DPM server with a new computer.

To replace the DPM system disk

1. Cancel and stop all running jobs.
2. Back up the DPM database.
3. Using Windows Server Backup, back up the operating system along with the critical volumes.
4. Install the new disk and perform a bare metal recovery (BMR) of the operating system by using Windows Server Backup.

   Note
   If you are installing on a new computer, ensure that machine name is the same as the previous one.
5. Use DPMSync to restore the DPM database and its replicas.

   Note
   The new computer should be part of the same domain as the previous computer.
6. Run a consistency check to bring all the replicas to a consistent state.

See Also

Using DPMSync

How to Migrate a DPM Server to New Hardware

Managing the Storage Pool

The storage pool is a set of disks on which the DPM server stores the replicas and recovery points for the protected data. DPM can use any of the following for the storage pool:

- Direct attached storage (DAS)
- Fiber Channel storage area network (SAN)
- iSCSI storage device or SAN

The storage pool supports most disk types, including Integrated Drive Electronics (IDE), Serial Advanced Technology Attachment (SATA), and SCSI, and it supports both the master boot record (MBR) and GUID partition table (GPT) partition styles.

You cannot add USB/1394 disks to the DPM storage pool.

DPM cannot use space in any pre-existing volumes on disks added to the storage pool. Although a pre-existing volume on a storage pool disk might have free space, DPM can use space only in volumes that it creates. To make the entire disk space available to the storage pool, delete any existing volumes on the disk and then add the disk to the storage pool.

Important
Some original equipment manufacturers (OEMs) include a diagnostic partition that is installed from media that they provide. The diagnostic partition might also be named the OEM partition, or the EISA partition. EISA partitions must be removed from disks before you can add the disk to the DPM storage pool.

In This Section

Adding Disks to the Storage Pool

How to Replace a Disk in the Storage Pool

Removing a Disk from the Storage Pool

See Also

Monitoring DPM Server

Performing DPM Server Management Tasks

Performing General DPM Server Maintenance

Adding Disks to the Storage Pool

DPM cannot use space in any pre-existing volumes on disks added to the storage pool. Although a pre-existing volume on a storage pool disk might have free space, DPM can use space only in volumes that it creates. To make the entire disk space available to the storage pool, delete any existing volumes on the disk and then add the disk to the storage pool.

DPM regularly rescans the disks and volumes in the storage pool and updates the storage pool space. If you add a disk that contains a volume to the storage pool and later delete that volume, when DPM rescans the disk, it will add the new unallocated space to the available storage pool.

If the name of a disk is listed as “Unknown” on the **Disks** tab in the **Management** task area of DPM Administrator Console, you cannot add the disk to the storage pool until the disk name is corrected. To resolve this issue, perform the following procedure.

To correct a disk name

1. In **Device Manager**, expand **Disk drives**.
2. Right-click each disk listed as "Disk drive", and select **Uninstall**.

Note
All disks without a friendly name are listed as “Disk Drive.” An example of a friendly name is “HITACHI_DK23EB-40”.

3. On the **Action** menu, click **Scan for hardware changes** to reinstall the disk.

See Also

How to Replace a Disk in the Storage Pool

Removing a Disk from the Storage Pool

How to Replace a Disk in the Storage Pool

You can use the following procedure to replace a disk in the storage pool if a disk fails.

To replace a disk in the storage pool

1. In the **Disk Management** console, identify the replica volumes and recovery point volumes that are stored on the failed disk.
2. Remove protection from the data sources that have replica volumes and recovery point volumes on the failed disk, and select **Delete protected data**.
3. Physically remove the disk that needs to be replaced.
4. Physically add the replacement disk.
5. In DPM Administrator Console, click **Management** on the navigation bar, and then click the **Disks** tab.
6. Select the disk that you removed, and in the **Actions** pane, click **Remove**.
7. In the **Actions** pane, click **Add**.
8. In the **Available disks** section, select the replacement disk, click **Add**, and then click **OK**.
9. Add the data sources from step 2 to an existing protection group, or create a new protection group for these data sources.
   a. If you create a new protection group and have tape backup of the data sources, create the replicas manually by using the tape backup.
   b. If you create a new protection group and do not have tape backup of the data sources, allow DPM to create the replicas across the network.
   c. If you add the data sources to an existing protection group, DPM will start an immediate consistency check, which will re-create the replicas.

Note
For more information, see Configuring DPM.

See Also

Adding Disks to the Storage Pool

Removing a Disk from the Storage Pool

Removing a Disk from the Storage Pool

A storage pool disk is both physically attached to the DPM server and programmatically attached by DPM to the storage pool.

When a disk that belongs to the storage pool is physically removed or fails, DPM sends an alert that there is a missing volume. The missing volume also displays on the **Disks** tab in the **Management** task area.

In the missing volume alert **Details** pane, you will see that there is a link to remove the disk from the storage pool. When you click this link, you remove the programmatic attachment.

If you remove the disk from the storage pool and later bring the disk online again, DPM cannot access the existing data on it. If DPM labels a disk as "missing volume" and you do not remove the disk from the storage pool, when you bring the disk online again, DPM will remap the volumes on the disk and can access the existing data on it.

See Also

Adding Disks to the Storage Pool

How to Replace a Disk in the Storage Pool

Monitoring DPM Server

After you set up data protection, you should monitor DPM activity to verify that everything is working correctly and to troubleshoot any problems that occur. Monitoring is essential to give you an overview of what has already happened, what is currently happening, and what is scheduled to happen. By monitoring DPM, you will know that data protection activities are working as expected, and you will have confidence that errors and warnings will be brought to your attention when they occur.

Note

For information about monitoring server performance, see Managing Performance.

In This Section

Establishing a Monitoring Schedule

Locating Information

Establishing a Monitoring Schedule

After you begin protecting your data, DPM operations require little intervention from you. When a situation does require action, you will be informed by an alert. For information about responding to alerts, see Resolving Alerts. We recommend that you establish a monitoring schedule and follow it routinely so that you are aware of trends and troubleshooting issues, and so that you can respond quickly to any problems that require your attention. The following table lists suggestions for a monitoring schedule.

Suggested Monitoring Schedule

At this interval	Check these sources	And look for this information
Daily	• Critical and warning alerts • Email notifications (if they are configured) • Status report	Replica issues, synchronization and recovery point creation issues, agent issues, jobs waiting for tape, backup failures
Monthly	Reports: • Status • Tape Management • Disk Utilization	Trends and patterns that might indicate problems or potential issues
On Demand	Recovery job status	Recovery job failures

See Also

Locating Information

Managing Performance

Methods for Monitoring DPM

Locating Information

After you implement your monitoring schedule, you will observe certain trends and notice various alerts. You might want to investigate the issues underlying the alerts, troubleshoot problems, or analyze some of the trends. DPM provides a number of resources to help you with your research. The following table lists a number of references that you can use to locate information that will help you answer many common questions.

Information Locations

What do you want to know?	Look here:
Does anything need my attention? Are there any changes on the protected computers that affect data protection?	• Email notifications of alerts, if you subscribe to them • **Monitoring** task area, **Alerts** tab
Did all the backups that were supposed to happen yesterday happen correctly? Is there an issue that keeps coming up? Are recovery goals being met?	• Status report • Protection report
Do I need to add disk space to the storage pool?	• **Management** task area, **Disks** tab • Disk Utilization report
When will a job run? How long did the last consistency check take? How much data was transferred by the most recent synchronization job?	**Monitoring** task area, **Jobs** tab
How many recovery points are available for a data source? Are all replicas consistent?	• **Protection** task area, **Details** pane • **Recovery** task area
What tapes are available in the library? What data is on each tape?	**Management** task area, **Libraries** tab
Did a recovery job complete successfully?	• **Monitoring** task area, **Alerts** tab • **Monitoring** task area, **Jobs** tab • Email notification (if you subscribe to email notification when you initiate a recovery)
Is the DPM server able to contact each protected computer?	**Management** task area, **Agents** tab
What is the status of the DPM service?	• Microsoft Management Console (MMC) Services snap-in • Event log, in case of service failures
What problems have occurred over the past month?	• Status report • **Monitoring** task area, **Alerts** tab, with **Show inactive alerts** selected
What is the status of each of my DPM servers and the computers that they protect?	MOM Operator console, **State** view
Why is recovery point creation failing for a	Status report

What do you want to know?	Look here:
protection group member?	

See Also

Establishing a Monitoring Schedule

Managing Performance

Methods for Monitoring DPM

Methods for Monitoring DPM

To monitor protection activities in System Center 2012 – Data Protection Manager (DPM), you can use the following methods:

- Use DPM Administrator Console to view DPM operations running on a specific DPM server.
- Configure DPM to provide reports and notifications of alerts by email.
- Monitor operations for multiple DPM servers by using the Management Pack for DPM.
- Monitor the instance of SQL Server that DPM installs by using the Management Pack for System Center SQL Server.

In This Section

Monitoring with DPM Administrator Console

Monitoring with Reports and Alert Notifications

Monitoring with DPM Management Packs

Monitoring with DPM Administrator Console

To use DPM Administrator Console, you must be logged on to a DPM server with an account that has Administrator rights on that server.

This section explains each of the following task areas of DPM Administrator Console and describes the information that each provides:

- Monitoring Task Area
- Protection Task Area
- Management Task Area
- Reporting Task Area

Note

You do not need to monitor each task area in DPM Administrator Console. For more information, see Establishing a Monitoring Schedule.

Monitoring Task Area

The **Monitoring** task area contains two tabs: **Jobs** and **Alerts**.

For monitoring purposes, the **Alerts** tab provides the more critical information. You should check the **Alerts** tab daily to provide timely resolution of issues that might be preventing successful protection of data.

Monitoring Task Area: Alerts

What do you look for on the **Alerts** tab?

- Current problems (critical alerts)
- Potential problems (warning alerts)
- Important activity (informational alerts)
- Recommended actions

The **Alerts** tab displays errors, warnings, and informational messages. You can group alerts by protection group, computer, or severity. You can also choose to display active alerts exclusively or to display both active alerts and inactive alerts (alerts that have been resolved). You can also subscribe to notifications to receive alerts sent by e-mail.

DPM ensures that the **Alerts** tab reflects the set of issues that are currently active in the system. When the issue that generated an alert is corrected, the alert becomes inactive. In fact, many issues reported as alerts never require your intervention at all, either because they reflect temporary conditions or because they are self-correcting. For example, an alert that indicates that the DPM server is unable to contact a protected computer might result from a transient network issue; the subsequent attempt might be successful. In some cases, DPM automatically designates an informational alert as inactive after a predefined period of time. A "Recovery collection completed successfully" alert, for example, becomes inactive three days after the recovery is completed.

DPM enables you to mark alerts as inactive. Marking alerts as inactive can be done for a variety of reasons, such as when the alert is no longer meaningful or if you do not plan to resolve the alert. For example, you see failure alerts for the past three days for a data source that is configured for daily backups to tape. You decide to rerun only the latest failed backup job. In this situation, you might want to mark the alerts for the previous failures as inactive.

When you mark an alert as inactive, the protection status for the protection group will change to **OK** in DPM Administrator Console and in the Management Pack for DPM.

For more information, see **Resolving Alerts** in DPM Help.

As a general guideline, we recommend that you do the following:

- View active alerts when you want to focus on active, current issues.

- Use inactive alerts as a source of information when you want to identify trends or analyze issues.
- Mark alerts as inactive only when you are sure that you need not address the issue.

  Note
  Marking an alert as inactive should be evaluated on a case-by-case basis and should not be done except when absolutely necessary.

Monitoring Task Area: Jobs

What do you look for on the **Jobs** tab?

- When jobs ran
- When jobs are scheduled to run
- Which jobs of a specific type are scheduled
- Which jobs are scheduled for a protected computer
- Which jobs are scheduled for a protection group
- Which jobs did not complete successfully and why
- How long jobs took to run
- The amount of data transferred for a job
- Number of files scanned during a consistency check
- Which tape and library resources were used

The **Jobs** tab displays the status of jobs. You can group jobs by protection group, computer, status, or type. You can also create filters to customize the view of jobs according to any combination of job parameters.

Detailed information for each job is available only on the **Jobs** tab in the **Details** pane. Detailed information about job failures can be useful for advanced troubleshooting.

You can choose to include regularly scheduled synchronization operations in the list of jobs. However, it is not necessary to monitor synchronization jobs regularly because any problems will be reported on the **Alerts** tab.

Protection Task Area

What do you look for in the **Protection** task area?

- Status of volumes and shares in each protection group
- Configuration of each protection group, such as recovery goals, disk allocation, and protection schedule

The **Protection** task area provides the status of each protected item.

Management Task Area

The **Management** task area contains three tabs: **Disks**, **Agents**, and **Libraries**.

Management Task Area: Disks

What do you look for on the **Disks** tab?

- Capacity of disks in the storage pool (used and free space)
- Status of disks in the storage pool
- Which protected volumes are contained on each disk

The **Disks** tab displays a list of disks included in the storage pool, and it enables you to add and remove disks from the pool.

Management Task Area: Agents

What do you look for on the **Agents** tab?

- Version of deployed agents
- Status of deployed agents
- Availability of agent licenses

The **Agents** tab displays a list of protection agents deployed on computers, and it enables you to install, uninstall, and update the agents and to update licenses.

Management Task Area: Libraries

What do you look for on the **Libraries** tab?

- State of the tape libraries and stand-alone tape drives
- Status of individual tapes

The **Libraries** tab displays a list of libraries and tape drives attached to the DPM server, and it enables you to inventory, add, and remove tapes.

Reporting Task Area

What can you do in the **Reporting** task area?

- Generate and view reports on DPM operations.
- Schedule automatic report generation.
- Manage Reporting Services settings.
- Subscribe to reports by e-mail.

DPM uses Microsoft SQL Server Reporting Services as the basis for its reporting functionality. SQL Server Reporting Services includes a Report Manager tool that is not installed during DPM installation. Because settings made through Report Manager can create conflicts with DPM settings, we recommend that you do not install the Report Manager tool that is included with SQL Server Reporting Services.

You can enable the DPM reporting feature at any time after installing and configuring DPM. However, to ensure that DPM has enough information to generate meaningful report data, we recommend that you wait at least a day after starting data protection activities to begin viewing reports. For instructions to help you enable DPM reporting, see Using Reports in DPM Help.

Note
When a DPM server is protecting a large number of computers, you should stagger the delivery schedule for reports sent by e-mail. If you schedule all reports to be sent at the same time, the memory limitations of SQL Server Reporting Services might prevent some reports from being sent.

The following table summarizes the available reports and indicates how you should use them. For information about interpreting the data in reports, see Report Types in DPM Help.

DPM Reports

Report name	Summary of contents
Status	The Status report provides the status of all recovery points for a specified time period, lists recovery jobs, and shows the total number of successes and failures for recovery points and disk-based and tape-based recovery point creations. This report shows trends in the frequency of errors that occur and lists the number of alerts. Use this report to answer questions such as the following: • What happened yesterday? Last week? Last month? • What succeeded and what failed? • What is the trend of errors? Which errors occur most frequently? • Are we achieving the recovery point objective (RPO) established in our service level agreement (SLA)? **Note** The Status report includes the error codes for any alerts recorded during the report period.
Tape Management	The Tape Management report provides details for tape rotation and decommissioning, and it verifies that the free media threshold is not exceeded. Use this report to manage tape circulation between the library and your offsite location.
Tape Utilization	The Tape Utilization report provides trending of

Report name	Summary of contents
	resource (disk/tape) usage over time to assist capacity planning. Use this report to make decisions about tape allocations and purchases.
Protection	The Protection report provides the commonly used metrics for backup success rolled up over long periods of time to track how backups are doing. Use this report to identify which computers or protection groups have been backed up successfully.
Recovery	The Recovery report provides the commonly used metrics for recovery success rolled up over long periods of time to track how recoveries are doing. Use this report to identify how well you performed against your service level agreements for recovery time objectives and recovery success guarantees.
Disk Utilization	Summarizes disk capacity, disk allocation, and disk usage in the DPM storage pool. Use this report to do the following: • Identify trends in disk usage • Make decisions about modifying space allocations for protection groups and adding disks to the storage pool • Identifying how much disk resource each computer is using on DPM.

See Also

Managing Performance

Monitoring DPM Server

Monitoring with DPM Management Packs

Monitoring with Reports and Alert Notifications

Monitoring with Reports and Alert Notifications

Notifications increase the ease of your routine monitoring. Rather than connecting to DPM Administrator Console to find out whether any alerts require your attention, you can subscribe to receive the following by e-mail:

- Any or all DPM reports, in the format that you select and on a schedule that you establish.
- Individual notification for each alert of the type to which you subscribe, and a notification when the alert has been resolved.

If you enable notifications or subscribe to reports, consider setting up a rule in Microsoft Office Outlook to filter notification and report mail into one or more dedicated mailbox folders. You can filter these e-mail notifications by using the **From** address or subject line. The **From** address of e-mail messages that contain notifications or reports will be the address that you specify when you configure the SMTP server.

The **Subject Lines Contained in E-Mail Notifications** table provides a list of subject lines that are used in each type of alert notification and each type of DPM report. You can use the text in these subject lines when you set up rules in Outlook to filter reports and alert notifications into specific folders. You can customize your e-mail notifications by using Operations Manager.

Subject Lines Contained in E-Mail Notifications

Email type	Subject line
Notification of an alert	• DPM: Information (Protected computer name) • DPM: Warning (Protected computer name) • DPM: Critical (Protected computer name) • DPM: Recovery (Protected computer name)
Notification of a resolved alert	• DPM: Resolved (Protected computer name)
Report	• Status Report from specified server • Media Management Report from specified server • Protection Report from specified server • Recovery Report from specified server • Tape Utilization Report from specified server • Disk Utilization Report from specified server

See Also

Managing Performance

Monitoring DPM Server

Monitoring with DPM Administrator Console

Monitoring with DPM Management Packs

Monitoring with DPM Management Packs

The Management Packs for DPM enable an administrator to use an Operations Manager Server to centrally monitor data protection, state, health, and performance of multiple DPM servers and the computers that they protect.

From the Operations Manager Operator console, the administrator can monitor DPM and network infrastructure simultaneously, analyzing issues with data protection in the context of other factors in system and network performance. From the same console, the administrator can monitor other mission-critical applications, such as Microsoft SQL Server and Microsoft Exchange Server.

From the Operations Manager server, administrators can perform the following monitoring tasks for managed DPM servers and the computers that they protect:

- Centrally monitor the health and status of data protection and critical performance indicators of multiple DPM servers and the computers that they protect.
- View the state of all roles on DPM servers and computers servers.
- Monitor actionable DPM alerts relating to replica creation, synchronization, and recovery point creation. The Management Pack for DPM filters out alerts that do not require an action, such as a synchronization job in progress.
- Through Operations Manager alerts, monitor the status of memory, CPU, and disk resources on DPM servers, and be alerted to DPM database failures.
- Monitor resource usage and performance trends on DPM servers.
- Diagnose and resolve problems on a remote DPM server.

The Management Packs for DPM are not included with the DPM product. You can download management packs at the DPM Management Pack download site.

See Also

Managing Performance

Monitoring DPM Server

Monitoring with DPM Administrator Console

Monitoring with Reports and Alert Notifications

Troubleshooting DPM Servers

This topic documents the following known issues and resolutions relating to System Center 2012 – Data Protection Manager (DPM) servers.

Data sources cannot be protected because prerequisite software is missing

Error 31008 appears because the DPM prerequisite software requirements are not met. For a complete list of all prerequisite software requirements and the required hotfixes and updates, see Software Requirements.

DPM changes destination folder attributes when recovering a file under the root volume

If you perform a recovery of a file or a file and a folder to an alternate location and the file is under the root of the protected volume, DPM changes the attributes of the destination folder to the attributes of the protected volume. For example, in the following scenario, if you recover **File1**, or **File1** and **Folder1**, to an alternate destination folder named **Test**, the **Test** folder acquires the attributes of **Volume X**.

VolumeRoot (X:)

\Folder1

\Folder2

File2

File1

After performing the recovery, set the appropriate permissions for **Folder1**.

DPM does not support protecting encrypted data in a file path that exceeds 5120 characters

If the file path of a protected data source on a volume that uses the Encrypting File System (EFS) exceeds 5120 characters, data protection will fail. You must ensure that the file path of the protected data source uses fewer than 5120 characters.

DPM does not support reprotecting a data source and then recovering it to an alternate location

You cannot recover a recently protected data source to an alternate location. For example, you protect a database that contains a full text catalog. You recover the database, and then protect

the recovered instance of the database. If you then try to recover the newly protected instance of the database to an alternate location, the recovery will fail.

DPM does not support protection of data sources if the data is on nested mount points

DPM does not support protection of a data source if the data is located on a nested mount point. For example, if you create a SQL Server database on nested mount points as shown in the scenario outlined in the following table, protection will fail for the SQL Server database located on volume V3.

Mount point	Volume
C:\	V1
D:\mnt1 (MP)	V2
D:\mnt1\mnt2 (MP)	V3

DPM Setup fails if a pre-release version of .NET Framework 2.0 is already installed

If a pre-release version of .NET Framework 2.0 is already installed on the computer on which you are installing DPM, Setup fails with an "unhandled exception" when installing .NET Framework 2.0.

Before running DPM Setup, uninstall the pre-release version of .NET Framework 2.0 by using **Add or Remove Programs** from Control Panel. Then reinstall DPM, and DPM Setup will install the current version of .NET Framework 2.0.

DPM does not automatically restart computers running Windows XP or Windows Vista

In the Protection Agent Installation Wizard, on the **Choose Restart Method** page, if you select the **Yes. Restart the selected computers after installing the protection agents.** option, DPM will not automatically restart computers running Windows XP or Windows Vista. You must manually restart the computers before you can start protecting data.

Alerts for different data sources in a protected server do not appear in System Center Operations Manager 2007

After an alert is generated and then additional alerts that have the same ID are generated for different data sources within the same protected server, System Center Operations Manager 2007 automatically suppresses the additional alerts. This is because the System Center Operations Manager 2007 Console takes time to refresh the view.

DPM Management Shell stops responding when specific cmdlets are running on a remote instance of DPM server

The following cmdlets cause the remote DPM Management Shell to stop responding. The cmdlets run successfully when they are run in DPM Management Shell on a local DPM server.

- Set-MaintenanceJobStartTime
- Get-BackupNetworkAddress
- Add-BackupNetworkAddress
- Remove-BackupNetworkAddress

DPM always defaults to port 25 when sending alerts through the SMTP server

In DPM, if you specify any port number in the SMTP server settings other than 25, DPM will continue to default to port 25 to communicate with the SMTP server.

Protection of DPMDB fails

If you try to protect the DPMDB before you deploy the DPM protection agent on at least one computer you will see the following error - "This item cannot be protected because some prerequisite software is missing. Ensure that all prerequisite software is installed and then protect this item (ID: 31008)". To resolve this issue, deploy a protection agent on a computer you want to protect before trying to protect DPMDB.

Uninstalling DPM does not remove reports

When DPM is using a remote instance of SQL Server, uninstalling DPM does not remove the reports that were generated by DPM. To remove these reports, navigate to Reports$<*InstanceName*> under Default Web Site using Internet Information Services (IIS) Manager, and delete the DpmReports directory.

Formatting custom volumes on which BitLocker is enabled

If you add a custom volume that has BitLocker enabled to a protection group, and then select the option to format the volume, DPM will format the volume.

BitLocker locks volumes on reboot

If you have enabled BitLocker on the DPM server, replicas and shadow copy volumes get locked and become inaccessible. This leads to failure of DPM jobs. The administrator needs to unlock the volumes so DPM jobs can run.

SetSharedDPMDatabase.exe tool fails on Windows Server 2008

Add exceptions for SQL Browser service, SQL Server and Windows Management Instrumentation to the global SQL Server to which you are trying to connect.

Administering DPM with the Central Console

It can be time-consuming to manage multiple servers in Microsoft System Center Data Protection Manager 2010. You must move from one server to another to perform various management and maintenance tasks. However, with Data Protection Manager (DPM), you can manage all your DPM servers from a single location.

After you have installed the Central Console, open the Operations Manager console, and click the **Monitoring** tab. Expand the **Data Protection Manager** folder to begin monitoring and managing your DPM servers. You can track servers for DPM 2010, System Center 2012 DPM and System Center 2012 SP1 DPM in the Central Console.

The important features of the Central Console are:

- Centralized monitoring of DPM servers across different versions of DPM
- Remote administration
- Role-based access control
- Remote recovery
- Remote corrective actions
- Service level agreement (SLA)-based alerting: Alerts are generated only when an SLA is broken
- Alert consolidation
- Support for scripting repetitive DPM jobs

Centralized Monitoring

When you use the centralized management solution, you can monitor all your DPM servers from a single location. In the Central Console, you can monitor the health of the various DPM resources like DPM server, protected computers, tape libraries, available disk space, and more. The Central Console also tracks the various tasks inDPM, like whether recovery points are being taken at the scheduled times, or whether a server is still on the network.

Remote Administration

If you have a smaller setup with about five to ten DPM servers, you can use Remote Administration to manage your DPM server centrally. Remote administration is basically the DPM Administrator Console on your computer. Use the remote Administrator Console to connect to and work on any DPM server.

You do not have to be a DPM administrator to use the Remote Administrator Console, just as long as your account is configured on Operations Manager for System Center 2012.

Caution

You cannot set end-user recovery options from the remote Administrator Console. This must be done on the DPM Administrator Console.

Alert Consolidation

Alert consolidation helps unclutter your **Alerts** tab and work on high priority items. DPM Central Console consolidates alerts in three cases:

- If the alert occurs repeatedly, only one alert is generated on the Central Console. If a job is scheduled to run hourly and hasn't run for the last ten hours, only one alert for the failed job is displayed in the Central Console instead of ten. On the DPM Administrator Console, the behavior is unchanged.
- If the root cause for multiple alerts is the same, or if multiple backups for the same data source have failed, only the alert informing you of the failure is generated.
- If you are using a ticketing system, consolidation of similar alerts means that only one ticket is generated.

You can resolve the alerts in different ways depending on the type of alert.

- Resume backups: If your backups are failing due to a cause that you have fixed or resolved, click **Resume backups**. The backup will start, and the alert will be resolved.
- Take recommended action: If there is a clear recommended action that can resolve your issue, click this option, and Central Console will trigger the action.
- Troubleshooting: For more complicated issues, you can use the scoped Administrator Console.

Caution

The time of creation of a recovery point is stored in the Operations Manager Data Warehouse in UTC time. When you create a report, you must convert the time to your time zone to get the right time. For example, if a recovery point was created at 01:00 P.M. 7/19/2011 on the protected computer, DPM pushes this as 1AM 7/19 to Operations Manager. Assuming that the Operations Manager server is in the Pacific Time zone, this will be store as 9AM 7/19. During report creation, you must convert the time back to get the actual time.

Scoped Administrator Console

The scoped Administrator Console is the administrator's best friend. The scoped console is based on the DPM Administrator Console with a few very noticeable changes:

- The title bar provides you with information such as ticket number, alert, and DPM server for which the alert is generated.
- The context bar gives you more details about the alert and where it is generated.
- The console is scoped to only show those objects for which the alert is generated.

Note

The scoped console also displays tasks that are not associated with any protection group or server because the jobs are common across all objects.

Using Central Console

In this section, we discuss how to use Central Console to manage multiple servers for System Center 2012 – Data Protection Manager (DPM).

Using Central Console

View jobs

The **View Jobs** dialog box gives you are list of all the jobs currently running on DPM servers that are monitored by the DPM Central Console.

To view jobs

1. Go to the Tasks view.
2. Select an object.
3. In the **Actions** pane, click **View Jobs**.

   The **View Jobs** dialog box will always display a list of all jobs that are currently running. If you want to filter the list, use the options in the **Filter by** section.

To cancel jobs

1. Select the job you want to cancel from the list.

   You can select more than one job by pressing the Ctrl key while you select from the list.
2. Click **Cancel Jobs**.

To view progress

1. Select the job whose progress details you want to see.
2. Click **View Progress**.

   This launches a scoped DPM Administrator Console where you can monitor the progress of the task.

View alerts

The Central Console gives you two views of DPM data:

- Alert view: A list of all DPM alerts that are generated and that require action.
- State view: The state of the various DPM objects, including data sources.

The right side of the console gives you a list of DPM tasks that you can perform based on the DPM object for which the alert was generated.

View the state of DPM objects

1. Expand the **DPM** folder on the left pane.
2. Expand the **State Views** folder.
3. Click the DPM object group you want to view.

   The main pane will show you the list of DPM objects and their current health.

To view an alert

1. Right-click the object, click **Open**, and then click **Alert View**.

   This opens the Operations Manager alerts view, and lists all the alerts generated on the object.
2. You can view the alerts and also check what steps are required to resolve the alert.

To resolve alerts

1. Expand the **DPM** folder on the left pane.
2. Expand the **Alerts Views** folder.

   The alerts are grouped under the Alerts Views folder by object. The groups are:
   - Data source alerts
   - DPM disk alerts
   - DPM tape alerts
   - DPM tape drive alerts
   - DPM tape library alerts
   - Protected computer alerts
   - Protection groups alerts
   - Replica volume alerts

   Note

   See DPM alerts for a list of alerts in each group.
3. Click the alert group you want to view.
4. Select the alert.

   The **Alert Details** pane displays all relevant details about the alert. Check the **Corrective action** in this section to learn what you need to do next.

   The **Alert Tasks** section of the **Actions** pane shows the actions to take to resolve the alert.
5. Select the action from the **Alert Tasks** section of the **Actions** pane.

   The **Alert Task** section has the following options:
   - **Get more information**: Takes you to a page where you can get more information about the alert and possible solutions.
   - **Resume backups**: Resumes the backups that were stopped. For a consolidated alert, this option resumes backups for all stalled backups.

     Note

     After you click **Resume backups** for a consolidated alert and start the scoped DPM Administrator Console, you cannot see all the jobs that were started because DPM will have already marked some alerts as resolved. To see a complete list of jobs, open the scoped DPM Administrator Console for

the consolidated alert's source, rather than the alert.

- **Take recommended action**: If there is a recommended action associated with the alert, this option runs the recommended action.
- **Troubleshoot**: Opens the scoped DPM Administrator Console for the alert.

View affected items

You can use the **View Affected Items** dialog box to view all the items that an alert was generated for.

To view an affected item

1. Select the alert.
2. Click **View Affected Items** in the **Actions** pane.

   This brings up the **View Affected Items** dialog box, with the following options.

   - **Resume backups** in the **Alert Details** section: Resumes the backups that were stopped. For a consolidated alert, this option resumes backups for all stalled backups.

     Note
     After you click **Resume backups** for a consolidated alert and start the scoped DPM Administrator Console, you cannot see all the jobs that were started because DPM will have already marked some alerts as resolved. To see a complete list of jobs, open the scoped DPM Administrator Console for the consolidated alert's source, rather than the alert.

   - **Take recommended action**: If there is a recommended action associated with the alert, this option runs the recommended action.
3. You can also use the following buttons to resolve the alert if without drilling down to the affected object.
   - **Troubleshoot**: Opens the scoped DPM Administrator Console for the alert.
   - **Resume backups** in **Affected Items** section: Resumes the backup for the selected item only.

Modify disk allocation

Use the **Modify Disk Allocation** dialog box to increase the amount of disk space allocated to recovery point volumes and replica volumes.

To modify disk space allocation

1. Select a data source.
2. Click **Modify Disk Allocation** in the **Actions** pane.

   This brings up the **Modify Disk Allocation** dialog box. You can modify the space allocated for recovery point volumes and replica volumes.

Create recovery points

The **Create Recovery Point** dialog box allows you to create a recovery point for a data source.

To create a recovery point

1. Select a data source.
2. Click **Create Recovery Point**.

   This opens the **Create Recovery Point** dialog box. Depending on the data source and the type of protection, you will be prompted with more options.

Manage users

In System Center 2012 – Data Protection Manager (DPM), you can use the Central Console to modify roles and tasks that users have permissions to work on. Because the Central Console is built on Operations Manager for System Center, you use the Operations Manager console to manage users. For more information about security roles in Operations Manager, see How to Administer Security Roles, Accounts, and Profiles in Operations Manager.

To restrict the tasks that a user has permissions for, use the Tasks page of the Create User Role Wizard, or the **Tasks** tab if you are editing an existing role. The DPM tasks are grouped under System Center Management Pack for Data Protection Manager. All the tasks are named Reserved, but the actual action is displayed in parentheses ().

Users see only the tasks they have permissions to perform. The permissions also extend to the scoped Administrator Console and to cmdlets.

Important

To add a DPM administrator, you must add the user to the Administrators group on the DPM server and to DPMDBAdministrators group on the SQL Server.

The following table displays the various preconfigured roles and the tasks each role can perform.

Task	Read-Only Operator	Reporting Operator	Tier-1 Support (Helpdesk)	Recovery Operator	Tier-2 Support (Escalation)	Tape Operator	Tape Admin	DPM Admin
Infrastructure management					Y			Y
Protection intent management					Y		Y	Y
Recovery related				Y				Y
Access to logs					Y			Y
Basic corrective actions					Y	Y	Y	
Modify disk allocation					Y			Y
Perform consistency check					Y			Y
Create recovery point for disk					Y			Y
Create recovery point for tape					Y		Y	Y
Agent management					Y		Y	Y
Cancel scheduled					Y		Y	Y

Task	Read-Only Operator	Reporting Operator	Tier-1 Support (Helpdesk)	Recovery Operator	Tier-2 Support (Escalation)	Tape Operator	Tape Admin	DPM Admin
jobs								
Retry jobs			Y	Y	Y		Y	Y
Tape library operations					Y	Y	Y	Y
Tape operations	Y						Y	Y
Allow recovery				Y				Y
Reporting operations		Y						Y
Monitoring operations			Y		Y	Y	Y	Y
Advanced tape library operations					Y	Y	Y	Y
Resume backups			Y		Y			Y

Infrastructure management

- Modify disk allocation
- Clear the Replica Inconsistent alert
- Allocate more disk space

Protection intent management

- Run the Tape Erase job again
- Run the Stop Protection job again
- Modify the Catalog Alert threshold size
- Claim ownership of the computer
- Modify protection group for this data source

Basic corrective actions

- Run the Tape Inventory job
- Run the Catalog Reload job
- Run the Verification job
- Run the Drive Cleaning job
- Run the Configure Protection job again
- Retrigger backup with verification

Tape library operations

- Allow a detailed inventory
- Open the library door
- Enable or disable a drive
- Clean a drive
- Remove a tape

Advanced tape library operations

- Rescan a library
- Rename a library
- Refresh a library
- Add tape (I/E port)

Tape operations

- Erase a tape
- Mark or unmark a tape as free

Working with protection groups

In System Center 2012 – Data Protection Manager (DPM), you can create and maintain protection groups, maintain recovery points and replicas for protection groups, and recover data for protection groups.

To create a protection group

1. Expand the **Data Protection Manager 2012** folder in the **Monitoring** view.
2. Expand **State Views**.
3. Click **DPM Server**.
4. From the **DPM Server Tasks** in the **Action** pane, click **Manage DPM server**.

   This opens the DPM Administrator console, where you can create the protection group.

To modify a protection group

1. Expand the **Data Protection Manager 2012** folder in the **Monitoring** view.
2. Expand **State Views**.
3. Click **Protection Groups**.
4. From the main window, select the protection group you want to modify.
5. From **Protection Group Tasks** in the **Actions** pane, click **Manage Protection**.

   This opens the DPM Administrator console to the **Protection** tab with the protection group you selected already highlighted.

To create a recovery point

1. Expand **Data Protection Manager 2012** folder in the **Monitoring** view.
2. Expand **State Views**.
3. Expand **Datasources**, and then click the data source type.
4. From the main window, select the data source for which you want to create a recovery point.

   This opens the **Create Recovery Point** dialog box where you can specify what kind of recovery point you want to create. Click **OK** to create the recovery point.

To recover data

1. Expand **Data Protection Manager 2012** folder in the **Monitoring** view.
2. Expand **State Views**.
3. Expand **Data Sources**, and then click the data source type.
4. From the main window, select the data source you want to recover.
5. From **DPM Data Source Tasks** in the **Actions** pane, click **Recover Data Source**.

   This opens the DPM Administrator console to the **Recovery** tab with the data source you selected already highlighted.

Troubleshooting with Central Console

Sometimes, it is not enough to resume a backup or perform the recommended action. If you want to drill down to the reason for an alert, use the **Troubleshoot** option. The **Troubleshoot** option opens the scoped Administrator Console. This console resembles the DPM Administrator Console, but is scoped to only display the object you are working with.

Using the console, you can drill down to see all the constituent alerts of a consolidated alert. You can also check to see if there is a pattern to when the alert is generated so you can find a long-term solution to the problem.

Apart from the available scoped options, the Central Console differs from the DPM Administrator Console with:

- A more informative title bar. The title bar of the scoped Administrator Console provides the ticket number (if a ticketing system is in use) and the alert from where the console was started.
- A context bar that gives you details about the object that is affected by the alert.

DPM alerts

This is a comprehensive list of alerts for System Center 2012 – Data Protection Manager (DPM), grouped by the object for which they are generated.

DPM Alerts

Protected computer

- Agent is incompatible (3121)
- Agent not reachable (3122)
- Agent ownership required (3107)
- Backup to tape failed - VSS data source is unavailable
- Configure protection failed - Agent not responding
- End-user recovery permissions update failed (3123)
- Recovery point creation failed - Access denied on protected server
- Recovery point creation failed - Active node not found
- Recovery point creation failed - Agent not responding
- Recovery point creation failed - Exchange log chain is broken
- Recovery point creation failed - Host unreachable
- Recovery point creation failed - Prepare CSV failed
- Recovery point creation failed - Snapshot is out of resource
- Recovery point creation failed - SQL command failure
- Recovery point creation failed - SQL database is missing
- Recovery point creation failed - SQL log chain is broken
- Recovery point creation failed - SQL Server is refusing connection
- Recovery point creation failed - VSS data source is unavailable
- Recovery point creation failed - VSS infrastructure error

- Recovery point creation failed - VSS retryable error
- Replica is inconsistent - Bit map file is corrupted
- Replica is inconsistent - Prepare CSV failed
- Replica is inconsistent - Protected server failed
- Synchronization failed - Access denied
- Synchronization failed - Host unreachable

DPM server

- DPM server availability
- Global DPMDB database not accessible - Alert notification (24091)
- No agent on cluster node (369)
- Tape encryption certificate has expired (24059)
- Database auto-protection failed (32511)
- Database size threshold exceeded (3168)

Microsoft Office SharePoint Server

- Backup metadata enumeration failed (3134)
- Backup to tape failed (3311)
- Cannot verify tape data (3309)
- Consolidation of recovery points of the replica failed (3178)
- Recovery point creation failed (3114)
- Replica is inconsistent (3106)
- SharePoint item-level catalog failed (3133)
- Tape copy failed (3310)
- Tape data integrity issues found (3317)
- Unable to configure protection for application data source (3170)

Data source

- Backup to tape failed (3311)
- Cannot verify tape data (3309)
- Recovery point creation failed (3114)
- Replica is inconsistent (3106)
- Tape copy failed (3310)
- Tape data integrity issues found (3317)

Protection group

- Backup to tape failed - Archive critical I/O error

- Backup to tape failed - Cancelled on restart
- Backup to tape failed - No dataset found on shadow copy for archive
- Recovery point creation failed - Cancelled on restart
- Recovery point creation failed - Replica is inconsistent
- Replica is inconsistent - Cancelled on timeout
- Replica is inconsistent - Replica is in invalid state
- Replica is inconsistent - VSS diff area I/O error

DPM library

- Backup to tape failed - Drive resource not online
- Backup to tape failed - Tape may be marked as cleaner
- Backup to tape failed - Tape library not online
- Free tape threshold reached (3305)
- Job waiting for tape (3315)
- Library devices were disabled (32572)
- Library not available (3301)
- Library not functioning efficiently (3302)

Application data source

- Backup to tape failed (3311)
- Cannot verify tape data (3309)
- Consolidation of recovery points of the replica failed (3178)
- Recovery point creation failed (3114)
- Replica is inconsistent (3106)
- Tape copy failed (3310)
- Tape data integrity issues found (3317)
- Unable to configure protection for application data source (3170)

DPM disk

Disk is missing (3120)

Tape drive

Library drive is not functioning (3303)

Replica volume

- Recovery point creation failed - Not enough space on replica
- Recovery point creation failed - Shadow copy area full

- Recovery point creation failed - Shadow copy storage insufficient
- Recovery point volume threshold exceeded (3169)
- Replica disk threshold exceeded (3100)
- Replica is inconsistent - Shadow copy area full
- Synchronization failed - Shadow copy area full
- Volume is missing (3101)

File system data source

- Backup to tape failed (3311)
- Cannot verify tape data (3309)
- Recovery point creation failed (3114)
- Replica is inconsistent (3106)
- Synchronization failures (3115)
- Tape copy failed (3310)
- Tape data integrity issues found (3317)

Backing up DPM

You can use System Center 2012 – Data Protection Manager (DPM) in your organization to protect file and application data, and to provide fast and efficient recovery of that data when the original data is lost or corrupted or mistakenly deleted on the protected computer.

In addition to configuring DPM to protect data on file and application servers, you should also deploy a backup and recovery option for DPM servers themselves. Ensuring that the DPMservers are properly backed up helps you to perform proactive maintenance, and to perform disaster recovery in the case of failure due to natural or technical causes.

This section explains how to prepare for disaster recovery and how to rebuild protected servers and the DPM server when server failure occurs.

DPM provides a number of methods for backup and recovery of DPM servers and protected data:

- Backup to disk.
- Backup to tape.
- Backup to secondary DPM server.
- Backup to the cloud using Windows Azure Recovery Services.

These methods are summarized in the following table.

Details	Backup to Disk	Backup to Tape	Backup to secondary DPM server	Backup to Windows Azure
Short-term	Yes	Yes	Yes	Yes

Details	Backup to Disk	Backup to Tape	Backup to secondary DPM server	Backup to Windows Azure
protection				
Long-term protection	No	Yes	No	No
Offsite protection	No	Yes	Yes	Yes
Application protection support	Files, SQL Server, Exchange, SharePoint, Hyper-V, System State, Clients	Files, SQL Server, Exchange, SharePoint, Hyper-V, System State, Clients	Files, SQL Server, Exchange, SharePoint, Hyper-V, System State, Clients	Files, SQL Server, Hyper-V

See the following topics for information about planning and deploying a backup and recovery process for DPM servers:

- Preparing DPM for backup
- Setting up secondary servers
- Backing up DPM using a secondary server
- Backing up the DPM database to tape
- Recovering DPM
- Using pre-backup and post-backup scripts

Preparing DPM for backup

The options available to you when the System Center 2012 – Data Protection Manager (DPM) server fails, or servers protected by the DPM server fail, will depend on the proactive planning steps you have taken to mitigate unexpected failures and disasters. For example:

1. If DPM is configured to protect file and application data, but no proactive measures for failure are in place, DPM can recover data after a protected computer is damaged or fails. However, you must first rebuild the protected computer manually by reinstalling the operating system, applications, and server configuration.
2. If the DPM server is damaged or fails without proactive backup and recovery processes in place, you must rebuild the DPM server manually and then reconfigure protection. Disk-based recovery points will not be recoverable, but you can import existing tapes for data recovery.
3. If both the protected computer and the DPM server are damaged or fail without proactive backup and recovery processes in place, all servers will need to be rebuild and reinstalled. Then the latest backup can be imported by existing tapes for data recovery. If no tapes are available, and only short-term disk protection is in place, all data might be lost.

To avoid this scenario, a number of proactive steps can be performed in preparation for backup and recovery in the case of unexpected failures:

1. **Verify data integrity**—Data backups rely on the integrity of the data being protected. To minimize the risk of data corruption, we recommend the following:
   - Run tools that check application integrity regularly, such as DBCC in SQL Server.
   - Monitor event logs on the protected computers and DPM server for hardware and file system errors.
   - Perform regular test recoveries of protected data.
   - Perform frequent consistency checks on critical data.
2. **Back up the system state of protected computer**—You can back up the system state of protected computers in a protection group by using DPM. System state backup enables you to restore a computer configuration after you reinstall the operating system and applications.
3. **Back up critical data to both disk and tape**—A thorough disaster recovery plan will include offsite storage of critical information; however, you want to be able to recover your organization's data should your facility be damaged or destroyed. Tape is a popular medium for offsite storage.
4. **Add a secondary DPM server**—A secondary server can protect and restore a primary server, which is a DPM server directly protecting file and application data sources. The secondary server can protect the databases of the primary server, as well as the data source replicas that are stored on the primary server. If the primary server fails, you can restore the databases and replicas to the rebuilt primary server from the secondary server. You can restore data to protected computers directly from the secondary server when the primary server is unavailable. The secondary server can also protect servers until the primary server is available.
5. **Back up DPM databases to tape**—You can use a DPM server to back up its own databases to its tape library, or you can use non-Microsoft software to back up the databases to tape or removable media. Backup of the DPM databases enables you to recover the configuration of protection groups after you reinstall DPM.
6. **Script file settings**—DPM uses a number of scripts. A pre-backup script resides on a protected computer, and is run before each DPM backup job. It prepares the protected data source for backup. A post-backup script runs after the DPM backup job to do any post-backup processing, such as bringing a virtual machine back online. When you install the DPM protection agent on a computer, a ScriptingConfig.xml file is added to the installpath\Microsoft Data Protection Manager\DPM\Scripting folder on the protected computer. For each protected data source on a computer, you can specify a pre-backup script and post-backup script in this XML file. When DPM runs a protection job, the ScriptingConfig.xml file is checked, and the pre-backup and post-backup files are run as indicated in the .xml file.

   DPM runs the pre-backup and post-backup scripts by using the local system account. As a best practice, ensure that the scripts have Read and Execute permissions for the administrator and local system accounts only. This level of permissions helps to prevent unauthorized users from modifying the scripts. In addition, on each protected computer you should back up the scripting file, ScriptingConfig.xml, at C:\Program Files\Microsoft System Center 2012\DPM\DPM\Scripting, and all pre-backup and post-backup scripts.

Backing Up DPM using Windows Azure Backup

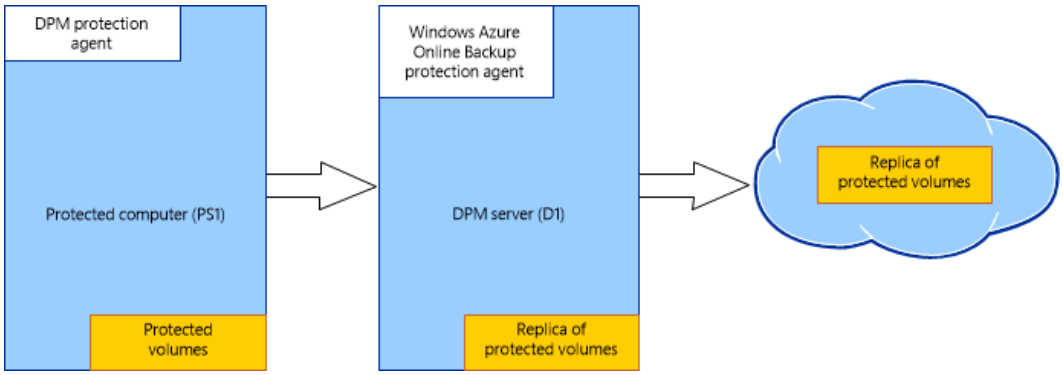
As an alternative to backing up System Center 2012 - Data Protection Manager (DPM) to disk or to a secondary on-premise DPM server, from System Center 2012 SP1 DPM onwards you can back up DPM servers and data protected by those servers to the cloud, using Windows Azure Backup.

This provides the following benefits:

- Reduced costs—The Windows Azure Backup service can help to reduce the total cost of ownership (TCO) for customers by providing scalability, elasticity, and simplified storage management.
- Peace of mind—The Windows Azure Backup service provides a reliable, secure, and a robust short-term offsite backup and restore solution that is highly available.
- Simplicity—The Windows Azure Backup workflows are seamlessly integrated into the existing DPM backup, recovery and monitoring workflows.

Overview

Windows Azure Backup works with the DPM disk-based protection feature. When you enable online protection, the disk-based replicas are backed up to an online location. The following diagram shows how DPM must be deployed with the Windows Azure Backup.



Configuring DPM backup to Windows Azure Backup consists of the following steps:

- Backing Up DPM using Windows Azure Backup
- Configuring backup vaults for Windows Azure Backup
- Registering DPM servers
- Managing online backups
- Recovering DPM data from Windows Azure Backup
- Manage and monitor backup vaults in Windows Azure Backup

Prerequisites for Windows Azure Backup

This topic outlines the deployment prerequisites required to back up Data Protection Manager (DPM) on servers running System Center 2012 Service Pack 1 (SP1) (or a later version) to Windows Azure Backup, and summarizes supported and non-supported scenarios.

Supported scenarios

The following scenarios are supported when protecting DPM data using backup vaults in Windows Azure Backup:

- Protection for file system
- Protection for virtual machines
- Protection for SQL Server databases
- Supported file types include:
  - Encrypted (Full backups only)
  - Compressed (Incremental backups supported)
  - Sparse (Incremental backups supported)
  - Compressed and sparse (Treated as Sparse)

Unsupported scenarios

The following scenarios are not supported when protecting data using Windows Azure Backup.

- DPM servers on case-sensitive file systems are not supported.
- Unsupported file types include:
  - Hard links (Skipped)
  - Reparse points (Skipped)
  - Encrypted and compressed (Skipped)
  - Encrypted and sparse (Skipped)
  - Compressed stream
  - Sparse stream

Deployment prerequisites

There are a number of deployment prerequisites required to deploy Windows Azure Backup for DPM:

- A server installed with Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 with SP1, and running DPM in System Center 2012 SP1 or System Center 2012 R2.
- You must have a Windows Azure account that has the Windows Azure Backup feature enabled. If you don't have an account, you can create a free trial account in just a couple of

minutes. For details, see Windows Azure Free Trial. Note that Windows Azure Backup uses the current pricing model at the time of writing (June 2013)

  - Charges are according to the amount of data stored in Windows Azure.
  - Up to 5 GB per month storage is free of charge.
  - Information about storage charges after 5 GB per month are available at Backup. While this feature is in preview there is a discount of 50% during the preview period.

- Using Windows Azure Backup requires the Windows Azure Backup Agent to be installed on DPM servers you want to back up. The DPM server must have at least 2.5 GB of local free storage space for cache location, although 15 GB of free local storage space to be used for the cache location is recommended.
- A management certificate that you will upload to the backup vault in Windows Azure Backup. Note the following:
  - To upload to the certificate to the vault, you must export it as a .cer format file that contains the public key.
  - The certificate should be an x.509 v3 certificate.
  - The key length should be at least 2048 bits.
  - The certificate must have a valid ClientAuthentication EKU.
  - The certificate should be currently valid with a validity period that does not exceed 3 years.
  - The certificate should reside in the Personal certificate store of your Local Computer.
  - The private key should be included during installation of the certificate.
  - You can create a self-signed certificate using the makecert tool, or use any valid SSL certificate issued by a Certification Authority (CA) trusted by Microsoft, whose root certificates are distributed via the Microsoft Root Certificate Program. For more information about this program, see Microsoft article Windows Root Certificate Program members.

To use makecert.exe note that:

- If you register the server you used to run makecert.exe, you can browse for the certificate using the Register Server Wizard (after installation of the agent).
- If you want to register a server that was not used to run makecert.exe, you must export the .pfx file (containing the private key) from that server, and copy it to the server you want to register, and import it into the Personal certificate store on that server. After the import, you can browse for the certificate using the Register Server Wizard (which runs as part of the agent installation application).

Configuring backup vaults for Windows Azure Backup

Windows Azure Backup is supported for Data Protection Manager (DPM) in System Center 2012 SP1 and System Center 2012 R2. Configuring Windows Azure Backup consists of the following steps:

1. Step 1 – Obtain a certificate—You can use either a valid existing management certificate for upload to the Backup vault, or obtain a certificate using makecert.exe.
2. Step 2 – Create a backup vault—In Windows Azure Backup, create a new Backup vault.
3. Step 3 – Upload a certificate—In Windows Azure Backup, upload the management certificate you created to the vault.
4. Step 4 – Download and install the Windows Azure Backup agent —From Windows Azure Backup, install the agent on each DPM server you want to backup online.

Step 1 – Obtain a certificate

You can use an existing management certificate, or obtain a self-signed certificate with the Makecert tool. If you run makecert.exe on the DPM server you register with the Backup vault, you can browse for the certificate using the Register Server Wizard (which runs as part of the agent installation), and the Windows Azure Backup agent is installed on the DPM server. If you want to register a server that was not used to run makecert.exe, you must export the .pfx file (containing the private key) from that server, copy it to the server you want to register, and import it to the Personal certificate store on that computer. Then after the import you can browse for the certificate using the Register Server Wizard. Use the following procedures to export and import the .pfx certificate.

To obtain a self-signed certificate using Makecert

1. Obtain the Makecert tool as described in MakeCert. Note that when installing the Windows SDK, you can install makecert.exe only by selecting the optionTools under.Net Development and leave everything else unchecked.
2. Open Command Prompt (cmd.exe) with Administrator privileges and run the following command, replacing CertificateNamewith the name of your certificate and specifying the actual expiration date of your certificate after -e: **makecert.exe -r -pe -n CN=CertificateName -ss my -sr localmachine -eku 1.3.6.1.5.5.7.3.2 -len 2048 -e 01/01/2016 CertificateName.cer**

Note that if you run makecert.exe on the DPM server you register with the Backup vault, you can browse for the certificate using the Register Server Wizard (which runs as part of the agent installation), and the Windows Azure Backup agent is installed on the DPM server. If you want to register a server that was not used to run makecert.exe, you must export the .pfx file (containing the private key) from that server, copy it to the server you want to register, and import it to the Personal certificate store on that computer. Then after the import you can browse for the

certificate using the Register Server Wizard. Use the following procedures to export and import the .pfx certificate.

To import the certificate (.PFX) to a different server

1. Copy the certificate .pfx file to a location on the local server.
2. In the Certificates MMC snap-in select **Computer account** and click **Next**.
3. Select **Local Computer** and click **Finish**. You are returned to the Add/Remove Snap-in dialog box. Click **OK**.
4. In the MMC, expand **Certificates**, right-click **Personal**, point to **All Tasks**, and then click Import to start the Certificate Import Wizard.
5. On the Certificate Import Wizard Welcome page, click **Next**.
6. On the File to Import page, click **Browse** and locate the folder that contains the .pfx certificate file that contains the certificate that you want to import. Select the appropriate file, and then click **Open**.
7. On the Password page, in **Password**, type the password for the private-key file that you specified in the previous procedure and then click **Next**.
8. On the Certificate Store page, select **Place all certificates in the following store**, click **Browse**, select the **Personal** store, click **OK**, and then click **Next**.
9. On the Completing the Certificate Import Wizard page, click **Finish**.

To export a certificate (.pfx) using the Certificates snap-in

1. From the Start screen type **mmc.exe** to start the Microsoft Management Console (MMC).
2. On the File menu, click **Add/Remove Snap-in**. The Add or Remove Snap-ins dialog box appears.
3. In **Available snap-ins**, click C**ertificates**, and then click **Add**.
4. Select **Computer account,** and then click **Next**.
5. Select **Local computer**, and then click **Finish**.
6. In the MMC, in the console tree, expand **Certificates**, and then expand Personal.
7. In the details pane, click the certificate you want to manage.
8. On the **Action** menu, point to **All Tasks**, and then click **Export**. The Certificate Export Wizard appears.
9. Click **Next**.
10. On the Export Private Key page, click **Yes**, export the private key. Click **Next**. Note that this is only required if you want to export the private key to other servers after the installation.
11. On the Export File Format page, select **Personal Information Exchange – PKCS #12 (.PFX)**. Click **Next**.
12. On the Password page, type and confirm the password that is used to encrypt the private key. Click **Next**.
13. Follow the pages of the wizard to export the certificate in PFX format.

Step 2 – Create a backup vault

To create a backup vault

1. Sign in to the Management Portal.

   To use this feature and other new Windows Azure capabilities, sign up for the free preview.
2. Click **Recovery Services**, then click **Create New**, point to **Backup Vault**, and then click **Quick Create**.
3. In **Name**, enter a friendly name to identify the backup vault.
4. In **Region**, select the geographic region for the backup vault.
5. In **Subscription**, enter the Windows Azure subscription that you want to use the backup vault with.
6. Click **Create Backup vault**.

   It can take a while for the backup vault to be created. To check the status, you can monitor the notifications at the bottom of the portal. After the backup vault has been created, a message will tell you that the vault has been successfully created and it will be listed in the resources for Recovery Services as **Online**.

Step 3 – Upload a certificate

To upload a certificate

1. Click **Recovery Services**, then click the name of backup vault to which you want to upload a certificate. On the backup vault page, click the **Quick Start** icon to open the **Quick Start** page.
2. On the **Quick Start** page, click **Manage Certificate**.
3. In the **Manage Certificate** dialog click **Browse Your Computer** to locate the .cer file to use with this backup vault.

You can also upload and manage certificates from the **Dashboard** tab for the vault. To do this, click **Recovery Services**, and click the vault name. On the **Dashboard** tab, click **Manage Certificate**.

Step 4 – Download and install the Windows Azure Backup agent

Prerequisites

If you will be using Windows Azure Backup with your DPM server, install the Update Roll up 2 for System Center Data Protection Manager SP1 before installing the Windows Azure Backup Agent..

Installation

Install the Windows Azure Backup provider agent on each DPM server you want to back up. Agents are accessed on the Windows Azure Download Center, and have their own setup process. When setup runs the agent is installed, and the DPM server is registered with the vault. Do the following from each DPM server you want to back up:

To install the backup agent

1. Open the Windows Azure Management portal, and log in.
2. On the Quick Start Page, click **Download Agent**.

   You will be presented with a dialog where you can choose which agent to download. Select Agent for Windows Server 2012 and System Center 2012 SP1 - Data Protection Manager. The application is downloaded from the Microsoft Download Center. Note the following:

   - Administrative permissions on the DPM server are required to install the agent
   - If you are installing the agent on multiple DPM servers you can place the installer file on a shared network resource, or use Group Policy or management products such as System Center Configuration Manager to install the agent.
   - A restart is not required in order to complete installation of the agent.
3. Run Setup to start the installation wizard.
4. On the Supplement Notice for the Service page, click **Accept the service agreement terms and conditions**, and then click **OK** to continue the installation.
5. The Prerequisites Check page is displayed and any missing prerequisite software is selected for installation. Click **Next** to approve the installation of the prerequisite software and continue the installation.
6. The Installation Settings page is displayed. On this page, you choose the **Installation Folder** and **Cache Location** for Windows Azure Backup.

   By default the installation folder will be <**system drive>:\Program Files\Windows Azure Backup Agent**. If you click **Browse** you can navigate and choose a new location in which to create the **Windows Azure Backup** folder.

   By default the cache location folder will be **<system drive>:\Program Files\Windows Azure Backup Agent**. In the cache location, the installation process will create a folder named Scratch within the **Windows Azure Backup Agent** folder. The cache location must have at least 2.5 GB of free space. Only local system administrators and members of the Administrators group have access to the cache directory to prevent denial-of-service attacks.

   Click **Install** when you have identified the folders that you want the Windows Azure Backup Agent to use. Note that if you are reinstalling Windows Azure Backup Agent, using the same cache location as the previous installation is recommended.
7. If you have not enabled automatic updates on your server, the **Microsoft Update Opt-In** page is displayed to give you the opportunity to enable Microsoft Update for Windows Server 2012. The Microsoft Update settings are for all Microsoft product updates, and they are not exclusive to the Windows Azure Backup Agent. Click **Next** to continue.

8. The **Installation** page is displayed. A progress indicator displays when the installation begins and shows the progress of the installation. When the installation is complete, you will receive a message that the Windows Azure Backup Agent was installed successfully. At this point, you can choose to check for updates. It is recommended that you allow the updates check to occur.
9. Click **Finish**. If you selected to check for updates, Internet Explorer will automatically start and the updates check will be performed. After any updates have been installed, you are ready to start configuring Windows Azure Backup Agent.

After the agent installation is complete, you can register the DPM server with the vault.

Registering DPM servers

After configuring backup vaults and deploying the Backup agent for System Center 2012 – Data Protection Manager (DPM), the servers must be registered with the vault.

To register DPM servers

1. In the DPM Administrator Console, click **Management** in the left-pane, and then click **Online**. Click **Register** on the tool ribbon. The Windows Azure Backup Registration Wizard starts, and backup vault information is retrieved from Windows Azure.
2. Enter your Azure login credentials, and then click **Next**.
3. On the Backup Vault page, select the certificate you uploaded to the vault, and then select the corresponding vault. Then click **Next**.
4. On the Proxy Configuration page, specify whether you want to use a specific proxy server to connect the backup service to Azure. Select **Use a proxy server for Windows Azure Backup**, and then type the URL to the proxy server. Use the FQDN or the IP address of the proxy server (for example, http://proxy.corp.contoso.com or http://10.186.173.132) and the port number on the server that is configured for Internet connections. If you do not specify a proxy server, the default Internet connection settings for the DPM server will be used, as displayed in the LAN settings. If the proxy server requires authentication before allowing connections, select **This proxy server requires authentication**, and then type the user name and password that Windows Azure Backup Agent should submit when it is queried for credentials. Click **Next** to continue.
5. On the Throttling Setting page, configure the settings for Internet bandwidth throttling. You can specific throttling settings for specific days, and for work hours and non-work hours. Note that this option is not available for Windows Server 2008 R2. Then click **Next**.
6. On the Recovery Folder Settings page, specify a folder location that will be used to temporarily hold recoverable items when a recovery occurs. Allocate enough space to hold the size of data you anticipate for recovery purposes. Then click **Next**.
7. On the Encryption Setting page, in **Enter Passphrase** and **Confirm Passphrase**, specify a passphrase that will be used to encrypt backups sent to Windows Azure, and to decrypt backups retrieved from Windows Azure. Click **Copy to clipboard** and then ensure that

you store the passphrase in a secure and safe location, preferably to a restricted access external location.

8. Click **Register** to complete the process. If successful, a registration confirmation message is displayed and you can close the wizard.

Managing online backups

You configure Windows Azure Backup for Data Protection Manager (DPM) in the same way you configure regular backup jobs. The only difference is that the backup destination is set as Windows Azure. The steps are as follows:

1. Step 1: Configure Windows Azure Backup for a new protection group—You can either configure an existing protection group, or create a new one.
2. Step 2: Configure Windows Azure Backup with an existing protection group
3. Step 3: Review online backup settings
4. Step 4: Run an on-demand online recovery point

Step 1: Configure Windows Azure Backup for a new protection group

1. In the **Protection** task area of the DPM Administrator Console, click **New** on the tool ribbon. The Create New Protection Group wizard opens.
2. On the Welcome page, click **Next**.
3. On the Select Protection Group Type, select **Servers**, and then click Next.
4. On the Select Group Members page, select the data sources and servers that will be members of the protection group, and thus backed up to Windows Azure. Then click **Next**.
5. On the Select Data Protection Method page, select **I want short-term protecting using: Disk**, and then select **I want online protection**. Note that online protection is only available for protection groups that use disk protection. Then click **Next**.
6. On the Specify Short-Term Goals page, specify the retention range and file recovery points. Note that these settings are not applicable for Windows Azure backups. Retention settings for online backup are set on the Specify Online Protection Goals page. Note that Windows Azure Backup will always keep the latest version of the backup.
7. In **File recovery** point, specify how recovery points for the backup should be created. Then click **Next**.
8. On the Review Disk Allocation page, accept the default settings, or modify the disk space allocated for new members of the protection group. Then click **Next**.

9. On the Choose Replica Creation Method page, specify how DPM creates a replica to copy the data from servers in the protection group to the DPM server.
10. On the Consistency Check Options page, specify how consistency checks should be run on replicas to ensure data integrity.
11. On the Specify Online Protection Data page, specify the data that you want to backup to Windows Azure for the protection group. Then click **Next**. The following types of data can currently be backed up from DPM using Windows Azure:
    - Files protected by DPM. Supported file types include:
        - Encrypted (Full backups only)
        - Compressed (Incremental backups supported)
        - Sparse (Incremental backups supported)
        - Compressed and sparse (Treated as Sparse)
    - Hyper-V virtual machines protected by DPM
    - SQL Server databases
12. On the Specify Online Protection Goals page, specify the following:
    a. In **Retention range in days**, specify how long backups should be kept in the Windows Azure cloud.
    b. In **Synchronization frequency**, specify if data for servers in the protection group should be synchronized with Windows Azure Backup daily or weekly
    c. In Synchronization Schedule, specify synchronization times. Then click Next.

    Note the following:
    - The maximum retention range for Windows Azure backups of DPM is 120 days.
    - You can synchronize to Windows Azure Backup at a maximum of twice per day.
    - The retention range depends on the synchronization settings. If you set to two backups per day then the retention range will be 60 days.
    - DPM creates an online recovery point using the latest DPM replica on disk. If you want to ensure that the latest data is backed up, create a new recovery point on disk before creating an online recovery point with this wizard. You can do this after completing the wizard, using the procedure below.
13. On the Summary page, review settings, and then click **Create Group**.

Step 2: Configure Windows Azure Backup with an existing protection group

1. In the DPM console, select the protection group containing the computers you want to back up to Windows Azure. Note that you can only use this type of backup for protection groups that are protected on disk.
2. On the tool ribbon, click **Add Online Protection**.

3. Complete the Modify Protection Group Wizard.

Step 3: Review online backup settings

1. After the protection group is created and the initial replication is complete, you can review settings and status as follows:
   a. In the protection group, you can verify that status is green for the protection group, and that Online Protection is set to Enabled. You can also review retention and scheduling settings for the online backup.
   b. On the **Monitoring** tab you can select **All Jobs in Progress** to view the backup type as “Online recovery point”.

Step 4: Run an on-demand online recovery point

1. To create an on-demand backup for a data source, click the **Protection** tab.
2. Right-click the data source and select **Create recovery point**.
3. In the **Create Recovery Point** dialog box, in **Create recovery point for**, select **Short term disk protection** to create a disk recovery point. Select **Online protection** to perform an on-demand online backup.

   Note that any on-demand online backup will count towards the maximum two online backups that can be performed each day.

See Also

New Protection Group Wizard

Recovering DPM data from Windows Azure Backup

Use the instructions in this topic to recover System Center 2012 - System Center 2012 – Data Protection Manager (DPM) data backed up using Windows Azure Backup.

1. In the DPM Administrator Console, click **Recovery** on the navigation bar.
2. Right-click the data source you want to recover, and click **Recover** in the **Actions** pane to start the Recovery Wizard.
3. On the Review Recovery Selection page, verify that the **Recover from:** setting is **Online**. Then click **Next**.

4. On the Select Recovery Type page, specify whether you want to recover to the original location, or to an alternate destination. Then click **Next**.
5. On the Specify Recovery Options page, specify whether you want DPM to mount databases after they are recovered, and whether you want to send an email notification when recovery is complete. Then click **Next**.
6. On the Summary page, review your selected settings, and then click **Recover**.

To view progress of the recovery job, go to the **Monitoring** tab in the DPM Administrator Console. The job type will be **Online Recovery**.After the recovery is complete, navigate to the recovery location to confirm that the data is located there as expected.

Manage and monitor backup vaults in Windows Azure Backup

You can manage and monitor backup vaults the Windows Azure portal.

Monitoring backup vaults

You use the Dashboard to get a quick overview of the state of your System Center 2012 - Data Protection Manager (DPM) backups in Windows Azure Backup. The Dashboard provides a centralized gateway to view servers protected by backup vaults, as follows:

- **Usage Overview** shows how you are using the backup vault. You can select a vault and see how much storage is being consumed by the vault, versus the amount of storage provided by your subscription. You can also see the number of servers registered to the vault.
- **Quick Glance** displays crucial configuration information about the backup vault. It tells you whether the vault is online, which certificate is assigned to it, when the certificate expires, the geographic location of the storage servers, and subscription details for the service.

From the dashboard you can download the Backup agent for installation on a server, modify settings for certificates uploaded to the vault, and delete a vault if required.

Managing backup vaults

You can perform the following actions on backup vaults and the DPM servers in those vaults:

- Delete a vault
- Update the certificate associated with the vault
- **View items backed up from DPM servers that are in the Backup vault**
- Reregister DPM servers with the vault
- Delete a server from a vault

Delete a vault

1. In the Windows Azure portal, click **Recovery Services**.

2. Click the name of the backup vault you want to delete, and then click **Delete**.

   You cannot delete a vault that currently contains protected servers. To do this, first remove the servers from the vault, and then delete the vault.

Update the certificate associated with the vault

1. In the Windows Azure portal, click **Recovery Services**.
2. Click the name of the backup vault you want to update, and then click **Manage certificate**.
3. In the **Manage Certificate** dialog box, update certificate settings.

Reregister DPM servers with the vault

1. In the Windows Azure portal, click **Recovery Services.**
2. Click the name of the relevant backup vault.
3. Click the **Servers** tab to view the servers registered with the vault
4. Select a server, and click **Allow Re-Register**. Then use the Registration Wizard available in the Agent installation application to reregister the server with the vault. This can be useful if you have experienced an error, or if a server was rebuilt. Reregistration is only allowed once per server name.

Delete a server from a vault

1. In the Windows Azure portal, click **Recovery Services**.
2. Click the name of the relevant backup vault.
3. Click the **Servers** tab to view the servers registered with the vault.
4. Select the server you want to delete, and then select **Delete**. All of the stored data associated with the server is deleted immediately, including all restore points, and all registered server settings.

Backing up DPM using a secondary server

You can back up a primary DPM server using a secondary DPM server as follows:

To back up a primary DPM server

1. On the secondary DPM server, install a protection agent on each primary DPM server that you want to protect. No restart is required.
2. You can use an existing protection group or create a new protection group for the primary DPM servers. The following items can be protected from a primary DPM server on which is protection agent is installed and which is configured for protection:
   - The databases in the instance of SQL Server on the primary DPM server

- All volumes on the primary DPM server (Shares will not be visible separately)
- All replicas on the primary DPM server.

Note the following:

1. Each of these data sources can be selected as a protection group member. At a minimum, you should select the databases, the \Program Files\Microsoft System Center 2012\DPM\DPM\Config folder, and the \Program Files\Microsoft System Center 2012\DPM\Scripting folder.

   Note
   You cannot exclude file name extensions from protection for a replica.
2. On the **Select Data Protection Method** page, you can select short-term disk-based protection and long-term tape-based protection, or just short-term disk-based protection. Selecting only short-term tape-based protection or only long-term tape-based protection is unavailable when a primary DPM server is a member of a protection group.
3. Complete the Create New Protection Group Wizard with the desired protection options.

   Note
   If a replica is selected as a member of the protection group and you select short-term disk-based protection, you must specify a synchronization frequency; the option to synchronize just before a recovery point will be unavailable. We recommend that you synchronize every 24 hours.

Setting up secondary servers

A DPM server can be used as a backup for other DPM servers. The main DPM server that protects data sources directly is known as the primary DPM server. A DPM server that protects other DPM servers is known as the secondary DPM server. The secondary DPM server can protect both the databases and the replicas on the primary DPM server, providing recovery if your primary DPM server fails. Note that a DPM server can act as both a primary server protecting data sources, and as a secondary server providing protection to a primary DPM server.

Deploying DPM servers for backup

You can configure DPM servers for DPM backup in different ways depending on your requirement. The most common scenarios are:

- **Single secondary server backing up a primary server**—In this configuration the secondary server continues to back up the protected servers on the primary server, in the event of the primary server failure. Since the primary server database and replicas will be available on the secondary server, you can use these to rebuild the primary DPM server by moving the backup of the protected servers back to the primary DPM server. Alternatively you can switch primary protection to the secondary DPM server, and restore to the protected computer directly from the secondary server.

- **DPM chaining**—DPM chaining creates a chain of DPM servers that protect one another. Each DPM server in the chain protects the next server in the chain. For example, in a chain of servers:
  - DPM1: primary server
  - DPM2: secondary server for DPM1 and/or primary DPM server
  - DPM3: secondary server for DPM2

  A secondary DPM server can protect the DPM database of its primary server along with replicas that the primary DPM server protects. Note that
  - Each DPM server can only be protected once.
  - A DPM server lower in the chain cannot protect higher in the chain. In other words, in our example DPM3 is protecting DPM1 but it cannot act as a secondary server for DPM1.
  - If a DPM server protects its own local data source the chain will be broken. For example if DPM1 protects its own DPMDB or System State, DPM2 will not be able to protect anything on DPM1.
- **Cyclic protection**—With this type of protection two DPM servers can protect each other. This is particularly useful in a branch office deployment. For example if you have two DPM servers — DPMa and DPMb, DPMa protects everything on DPMb and vice versa.

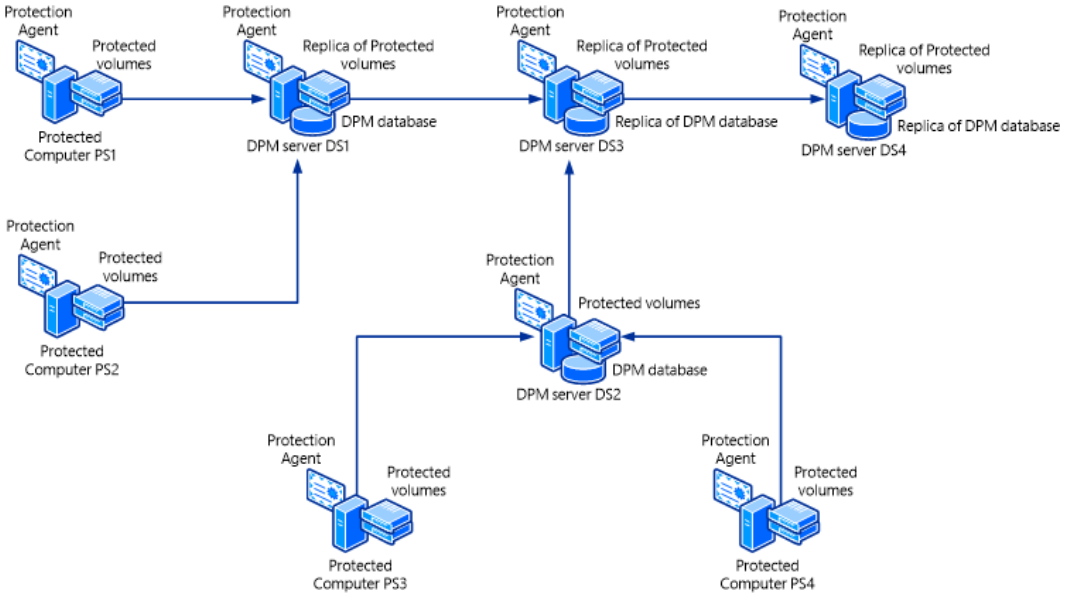
DPM chaining

The following graphics illustrate DPM chaining.

Scenario 1

Scenario 1 shows a scenario in which four DPM servers are chained:

- DS1 is a primary server protecting servers PS1 and PS2.
- DS2 is a primary server protecting PS3 and PS4.
- DS3 is a secondary server protecting DS1 and DS2.
- DS4 is a secondary server protecting DS3.



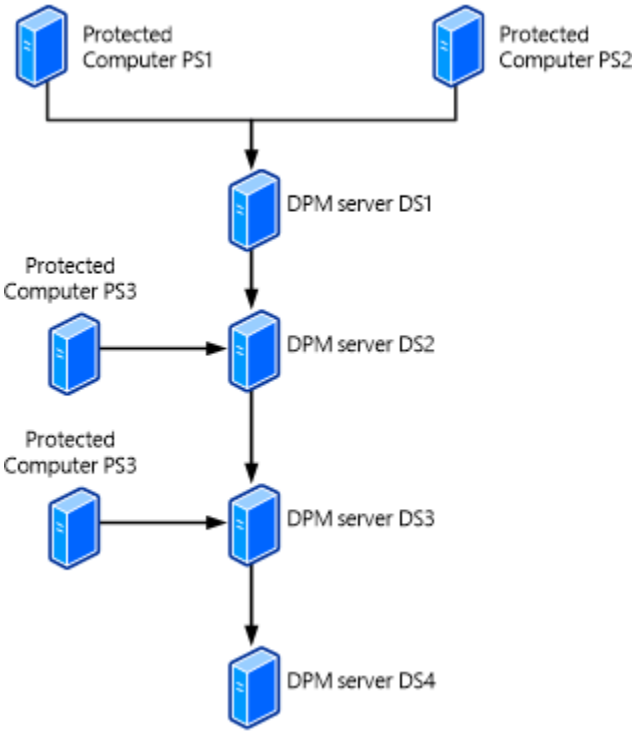
The table describes what each DPM server in the diagram protects.

	DS1	**DS2**	**DS3**	**DS4**
Protecting	PS1 PS2	PS3 PS4	DS1 DS2	DS3
Protected By	DS3	DS3	DS4	-

Scenario 2

Scenario 2 shows a scenario in which four DPM servers are chained:

- DS1 is a primary server protecting servers PS1 and PS2.
- DS2 is a primary server protecting PS3, and a secondary server protected DS1.
- DS3 is a primary server protecting PS4, and a secondary server protecting DS2.
- DS4 is a secondary server protecting DS3.



The following table describes what each DPM server in the diagram protects.

	DS1	**DS2**	**DS3**	**DS4**
Protecting	PS1 PS2	PS3 DS1	PS4 DS2	DS3
Protected By	DS2	DS3	DS4	-

Before you configure secondary protection for your servers, verify the following:

- The selected DPM servers are not protecting additional DPM servers.
- The DPM server or selected DPM servers are not being protected by other DPM servers.

Important
Before you can protect the database of the primary DPM server, you must start the SQL Server VSS Writer service on the primary DPM server. To start the SQL Server VSS Writer service, in the **Services** console, right-click **SQL Server VSS writer**, and then click **Start**.

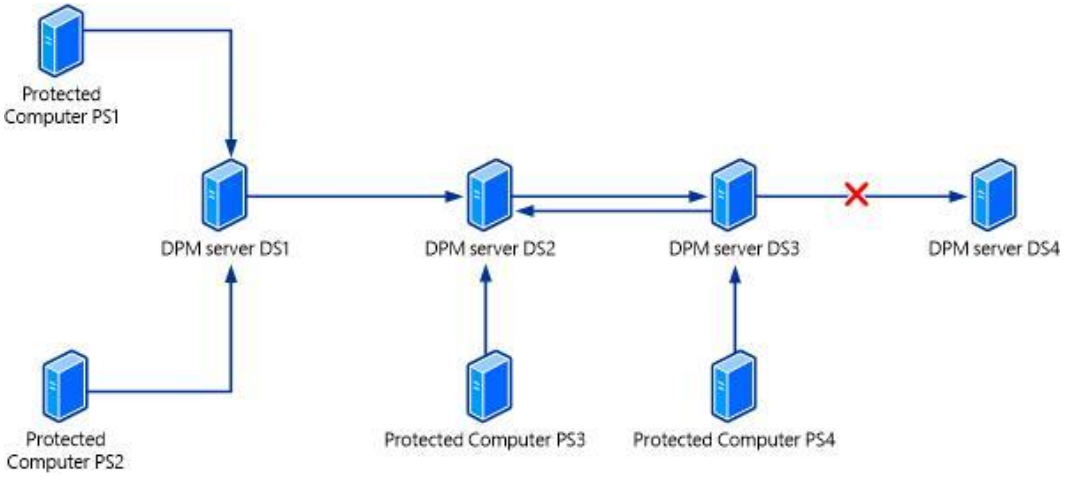
Cyclic protection

If you do not want to use a dedicated secondary server, you can have another primary DPM server double up as a secondary server. In this deployment, two DPM servers can protect each other.

Scenario 3

Scenario 3 shows a scenario using cyclic protection

- DS1 is a primary server protecting servers PS1 and PS2.
- DS2 is a primary server protecting PS3, and a secondary server protecting DS1 and DS3.
- DS3 is a primary server protecting PS4, and a secondary server protecting DS2.



The following table describes what each DPM server in the diagram protects.

	DS1	DS2	DS3	DS4
Protecting	PS1 PS2	PS3 DS1 DS3	PS4 DS2	-
Protected By	DS2	DS3	DS2	-

Backing up DPM using third-party software

The process for backing up DPM using third-party software is dependent on whether the backup software supports DPM and the Volume Shadow Copy Service (VSS). The principal advantages of software that supports DPM and VSS are:

- Software that supports VSS organizes the archived data in a way that makes restore operations intuitive and comparatively simple.
- The number of steps involved in archive and restore operations are minimized.

The following procedures provide general instructions for archiving DPM databases and replicas when using backup software that supports DPM. For instructions on using the backup software, see the documentation for the backup software.

Using software that supports VSS

If your backup software supports VSS, you can back up data directly from the replicas at \Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\Replica; however, you must ensure that the software does not modify data on the replica volumes. For example, if you are using Windows Backup to archive data, use only the “copy” backup type.

To verify that the backup types for that software that will not modify data on the replica volumes, consult the documentation for your backup software or contact the vendor.

You must back up the database for both the DPM database and the Report database. The following procedures provide general instructions for archiving DPM databases and replicas when using backup software that does not support DPM but does support VSS. For instructions on using the backup software, see the documentation for the backup software.

To back up databases by using backup software that supports VSS

1. In the console tree of the backup program, browse to Microsoft System Center 2012\DPM\DPM, and select the DPMDB folder.
2. Select the media to which you want to back up the databases.
3. Start the backup.

Note

Some VSS-enabled backup software does not have a SQL VSS Requester for backing up SQL Server databases through the VSS infrastructure and the MSDE VSS Writer. In that situation, use the procedure for backing up databases with non-VSS-enabled backup software.

To back up replicas by using VSS-enabled backup software

1. In the console tree of the backup program, browse to \Microsoft System Center 2012\DPM\DPM\Volumes\Replica\ on the DPM server.
2. Select the computer for the replicas you want to archive or the individual protected volumes.
3. Select the backup type.

   Important
   Consult your backup software documentation or contact the software vendor to determine which backup types will not modify the replica data.
4. Select the media to which you want to back up the files.
5. Start the backup.

Backing up using DPM-enabled backup software

To back up databases by using DPM-enabled backup software

1. In the console tree of the backup program, browse to \Program Files\Microsoft System Center 2012\DPM\DPM\DPMDB, and select the DPMDB folder.
2. Select the media to which you want to back up the database.
3. Start the backup.

To back up replicas by using DPM-enabled backup software

1. In the console tree of the backup program, expand DPM server.
2. Select the computer whose replicas you want to archive or the individual protected volumes.
3. Select the backup type.
4. Select the media to which you want to back up the files.
5. Start the backup.

Backing up using software that does not support VSS

If your backup software does not support VSS or DPM, you must use DPMBackup, a command-line tool, to create backup shadow copies of the replicas and database backups of the DPM database, and then use the backup software to archive the backup shadow copies and database backups to tape.

Use DPMBackup to prepare files for backup when using non-VSS-enabled backup software. DPMBackup is a command-line tool included with DPM that performs the following tasks:

- Creates and mounts backup shadow copies of each replica volume on the DPM server.
- Creates database backups of the DPM database.

DPM creates a mount point of the backup shadow copies of the replicas on the DPM server in the folder \Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\ShadowCopy\. The backup shadow copies of the replicas are organized by computer.

You can configure either your tape backup program or Windows Scheduler to run DPMBackup before the tape backup program runs. The amount of time that DPMBackup requires to create the backup shadow copies and database backups depends on factors such as disk and database activity, but as a guideline, you can expect the tool to take approximately 2 minutes per replica volume to complete the operation.

The DPMBackup.exe program is stored on the DPM server in the folder \Program Files\Microsoft System Center 2012\DPM\DPM\bin. DPMBackup requires Administrator rights on the DPM server.

The backup shadow copies created by DPMBackup are read-only copies of the replica volumes, and can be archived as you would archive a file system. Because the backup shadow copies of the replicas are mounted, you must configure your tape backup software to traverse mount points.

You must back up the database for the DPM database. The following procedures provide general instructions for archiving DPM databases and replicas when using backup software that does not support DPM or VSS. For instructions about using the backup software, see the documentation for the backup software.

To back up databases by using backup software that does not support DPM or VSS

1. Run DPMBackup.exe -db

   You can run the DPMBackup tool manually, or configure your backup program to run it automatically.
2. In the console tree of the backup program, browse to \Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\ShadowCopy\Database Backups. The file name of the DPM database backup is DPMDB.bak. The default file name of the Report database backup is ReportServer.bak.
3. Select the media to which you want to back up the databases.
4. Start the backup.

To back up replicas by using backup software that does not support DPM or VSS

1. Run DPMBackup.exe –replica. You can run the DPMBackup tool manually, or configure your backup program to run it automatically.
2. In the console tree of the backup program, browse to \Program Files\Microsoft System Center 2012\DPM\DPM\Volumes\ShadowCopy\. The backup shadow copies of the replicas are organized by computer.
3. Select the shadow copies that you want to back up.
4. Select the backup type.
5. Select the media to which you want to back up the files.
6. Start the backup.

Backing up the system state of protected computers

The system state is a collection of system-specific data maintained by the operating system that must be backed up as a unit. DPM can protect the system state for any computer on which a DPM protection agent can be installed, except computers running Windows Vista.

In order for DPM to back up the system state of a protected computer, the system state of the computer can be added to a protection group. DPM leverages the Windows Backup utility on the protected computer to back up the system state to a backup (.bkf) file, which is saved to the DPM medium you specify for that protection group (disk, tape, or both). Note the following:

- The backup of a computer's system state can be used when you need to return the computer to a known state, such as after an installation that puts the computer in an undesirable state. It is not a backup of the entire system.
- Because system state does not change frequently, consider placing system state in protection groups separate from file and application data so that you can specify the most efficient protection schedule for each data source.
- For complete protection on a Windows Server 2008 operating system, including system state protection, you must install Knowledge Base article 949779.

DPM backs up the system state of protected computers as follows:

- **Domain member system state**— When DPM backs up the system state of a computer that belongs to a domain, the following components are protected:
  - The boot files
  - The COM+ class registration database
  - The registry
- **Domain controller system state**— When DPM backs up the system state of a domain controller, the following components are protected:
  - Active Directory (NTDS)
  - The boot files
  - The COM+ class registration database
  - The registry
  - The system volume (SYSVOL)

  For more information about backing up and restoring system state for a domain controller, see Introduction to Administering Active Directory Backup and Restore.
- **Server running certificate services system state**— When DPM backs up the system state of a member server or domain controller with Certificate Services installed, Certificate Services is protected in addition to the member server or domain controller system state components.
- **Cluster server system state**— When DPM backs up the system state of a cluster server, the cluster service metadata is protected in addition to the member server system state components.

System state backup file and logs

The backup file of system state is created at %systemdrive%\DPM_SYSTEM_STATE.

The logs for system state backup are stored at C:\Document and Settings\Default User\Application Data\Microsoft\NTBackup. Log files will be named NTBackup0.log, NTBackup1.log, and so forth. You can view these logs to help resolve any issues that occur with the system state backup.

You can change the default location of the system state backup file as follows:

To change the location of the system state backup file

1. On the protected computer, open PSDatasourceConfig.xml in an XML or text editor. PSDatasourceConfig.xml is typically located at *install path*\Program Files\Microsoft Data Protection Manager\DPM\Datasources.
2. Change the **<FilesToProtect>** value from %systemdrive% to the desired location.
3. Save the file.
4. On the DPM server, run a consistency check if there is a protection group protecting the system state of the protected computer in step 1.
5. The consistency check will fail and generate an alert. Perform the recommended actions in the alert as follows:
    a. In the alert details, click the **Modify protection group** link, and then step through the wizard.
    b. Perform a consistency check.

Backing up the DPM database to tape

You can use a DPM server to protect its own database by backing up the database to tape. We recommend that you use a unique protection group to back up the DPM server database, make at least two copies of the backup tapes, and store each of the backup tapes in a different remote location. You should also consider subscribing to the DPM Status report, which will list the tape with the most recent database backup.

Important
If DPM uses a remote SQL Server installation, you must install the DPM protection agent on the remote SQL Server-based computer before you can protect the DPM databases on that server.

To back up DPM databases to tape by using the primary DPM server with a local SQL Server installation

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Create protection group**.
3. On the **Select group members** page, expand the DPM server item, and then select **DPMDB**.
4. On the **Select data protection method** page, select **I want short-term protection using tape**, and then click **Next**.
5. Specify the short-term protection policy options. We recommend a retention range of two weeks for DPM databases.
6. Complete the Create New Protection Group Wizard with the protection options you want to use.

To back up DPM databases to tape by using the primary DPM server with a remote SQL Server installation

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Create protection group**.
3. On the **Select group members** page, expand the SQL Server item for the remote SQL Server installation that DPM uses, and then select **DPM database**.
4. On the **Select data protection method** page, select **I want short-term protection using tape**, and then click **Next**.
5. Specify the short-term protection policy options. We recommend a retention range of two weeks for the DPM databases.
6. Complete the Create New Protection Group Wizard with the protection options you want to use.

Recovering DPM

This section provides instructions for recovery in case of a disaster, such as a DPM server failing or a protected server failing.

Recovering DPM servers topics

- Switching protection to a secondary server
- Recovering a protected computer
- Recovering DPM servers

Switching protection to a secondary server

If the primary DPM server fails, the secondary DPM server can continue protection of protected computers. To continue protection, you must switch protection of the protected computers to the secondary server. After you have switched protection to the secondary server, you can also use it to perform recovery functions.

Important

To recover Windows SharePoint Services data directly from the secondary server to the protected computer when Windows SharePoint Services uses an instance of SQL Server on another computer, you must switch protection for both the Windows SharePoint Services server and the SQL Server-based computer to the secondary server.

To switch protection to the secondary DPM server

Using the DPM Administrator Console

1. Go to the Protection work area.
2. Right-click the protection group for which you want to switch protection.
3. Select Switch Disaster Protection from the context menu.

After switching protection, the replica will be shown as inconsistent until DPM runs a consistency check.

Using the DPM Management Shell

- On the secondary server, open the DPM Management Shell and run the Start-DPMSwitchProtection cmdlet.

To switch protection back to the primary DPM server

1. Go to the Protection work area.
2. Right-click the protection group for which you want to switch protection.
3. Select Switch Disaster Protection from the context menu.
4. After switching protection, you will begin to see **Agent Ownership Required** alerts on the primary server. Click **Take Ownership** in the alert to give the primary server ownership of the protection agent.

Recovering a protected computer

This topic includes instructions to continue protection for a protected computer after a disaster, recover a protected computer and recover data to a protected computer from the secondary DPM server.

Continuing Protection for a Protected Computer After a Disaster

After you rebuild a computer following a disaster, consistency check will fail on the new computer because the volume GUID of the original computer differs from the new one. To enable protection

for the new computer, start the Modify Protection wizard for the protection group and run through the wizard by clicking **Next** on each screen.

1.

Recovering System State to Protected Computers

You can recover the system state to protected computers that are in a *working state*, meaning the operating system and necessary applications are installed.

When you protect a computer's system state, DPM uses the Windows Backup utility on the protected computer to back up the system state to a backup (.bkf) file, which is saved to the DPM medium you specify for that protection group (disk, tape, or both). The restore of the system state is a two-phase process:

1. Use the DPM Recovery Wizard to restore the .bkf file to the protected computer.
2. Use Backup to restore the system state from the .bkf file to the protected computer.

To recover the system state .bkf file

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
2. Browse or search for the protected computer, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the .bkf file to recover.
5. In the **Actions** pane, click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and then click **Next**.
7. Specify to recover the .bkf file to an alternate location on the protected computer.
8. Click **Next**.
9. Specify your recovery options:
   - **Existing version recovery behavior**. Select **Create copy**, **Skip**, or **Overwrite**.
   - **Restore security**. Select **Inherit security settings of target when overwriting or of parent folder when creating copy** or **Apply the security settings of the recovery point version**.
   - **Throttling**. Click **Modify** to enable throttling.
   - **Notification**. Click **Send an e-mail when the recovery completes** and specify the recipients that will receive the notification. Use commas to separate e-mail addresses.
10. Click **Next**.
11. Review your recovery settings, and then click **Recover**.

    Any synchronization job for the selected recovery item will be canceled while the

recovery is in progress.

To restore system state from the .bkf file

1. On the computer to which you recovered the system state .bkf, click **Start**, click **Run**, type **ntbackup**, and then click **OK**.
2. When the Backup or Restore Wizard starts, click **Next**.
3. On the **Backup or Restore** page, click **Restore files and settings**, and then click **Next**.
4. On the **What to Restore** page, click the items to expand their contents, locate and select the .bkf file that you recovered using DPM, and then click **Next**.
5. On the **Completing the Backup or Restore Wizard** page, if you want to change any of the advanced restore options, such as restoring security settings and junction point data, click **Advanced**. When you are done setting advanced restore options, click **OK**. Verify that all settings are correct, and then click **Finish**.

Recovering Protected Computers from a Secondary DPM Server

When the primary server is unavailable, you can recover data for protected computers from the secondary server. To recover data to an alternate location from a secondary server, you use the Recovery Wizard in DPM Administrator Console on the secondary server with no additional steps required. To recover data to the original location from a secondary server, you must first switch protection to the secondary server.

To recover data to its original location on protected servers from a secondary DPM server

1. Switch protection of the protected computer to the secondary server by using the Start-SwitchProductionServer cmdlet or the SwitchProtection.ps1 script. For instructions about switching protection, see **Switching Protection If the Primary DPM Server Fails**.
2. Use DPM Administrator Console on the secondary server to recover the data to the original location.

See Also

Backup of Protected Computer System State

Backing Up DPM by Using a Secondary DPM Server

Recovering DPM servers

When you recover a primary DPM server, you must reestablish protection for the computers that were previously protected by the DPM server.

Note
You cannot restore recovery points for data sources protected by the DPM server.

To recover the DPM database when the database is corrupt

When recovering the DPM database files, ensure that the location on the DPM computer where you restore the files is secure.

1. Uninstall DPM through the Add/Remove Programs.

   Important
   Remember to select **Retain disk-based recovery points**.
2. Restart the computer.
3. Delete the DPM database using SQL Server Management Studio.
4. Install DPM.
5. Restart the computer.
6. On the DPM server, create a folder to which you can restore the files.
7. Insert the tape with the latest backup of the DPM database into the tape library.
8. Open the **Libraries** tab on the **Management** tab of DPM Administrator Console.
9. Click **Rescan** on the **Actions** pane.

   Go to Updating Tape Library Information for more information on using the Rescan option.
10. Insert the tape with the latest backup of the DPM database in the tape drive/library. You can find the tape having the latest backup using the last tape management report.
11. Select the library from the list and click **Inventory libraries…** and perform a detailed inventory from the **Actions** pane.
12. Select the imported tape from the list and click **Recatalog imported tape** on the **Actions** pane.
13. Open the **Recovery** tab from DPM Administrator Console.
14. Select the DPM database by expanding the External Tapes node.
15. Click **Recover** on the **Actions** pane.
16. Using the Recovery wizard, recover the database to a network folder. This folder will be the recovery folder you created in Step 6.

    Go to How to Inventory Tapes for more information on the procedure to inventory tapes.
17. Use DPMSync to attach the database to DPM.

    DPMSync –RestoreDB –DBLoc *location of folder created in Step 6\name of DPMDB*

    DPMSync takes the DPM service offline and attaches the backed up database to SQL

Server.

18. Run **DpmSync -sync**

To recover replicas after the DPM database is recovered

To recover a DPM replica, you must first run DpmSync to reallocate it. DpmSync marks the replica as manual replica creation pending. You can only recover the replica when its status in DPM Administrator Console is manual replica creation pending. If a replica recovery fails, the replica status changes to inconsistent, which prevents repeated recovery attempts.

If a replica recovery fails, you must stop protection of the data source using the delete replica option, add the data source to a protection group again using the manual replica creation option, and then retry the replica recovery.

If the recovery fails, simply retrying the recovery will always fail, because the replica is now marked as Invalid and not in a waiting manual load state.

1. Run **DpmSync -reallocateReplica**. This command reformats any replicas that are missing and marks them as "manual replica creation pending." For instructions, see Using DpmSync.
2. Manually create the replica from either the secondary DPM server or a tape backup of the data source corresponding to each of the replicas.
   - When using a secondary DPM server, a **Restore to replica** option is enabled in the **Recovery task** area.
   - When using tape backups, use DPM Management Shell with the **RestoreToReplica** option.
3. Perform a consistency check to continue protection.

To reestablish protection after rebuilding the primary DPM server

After you rebuild a primary DPM server, you must reestablish protection of the computers that were protected by the primary server. Perform the following procedure on each computer that was protected by the primary server.

1. On the protected computer, at the command prompt, run the following command:

   Setdpmserver.exe <*primary DPM server name***>**
2. Open Computer Management and perform the following steps:
   a. Select **Local Users and Groups**.

b. Verify that the primary server, in the format of *Domain**Name*, is a member of the following groups:

   Distribute COM Users

   DPMRADCOMTrustedMachines

   DPMRADmTrustedMachines

c. If the primary server is not listed in any of the groups in step b, manually add the server as a member in the format of *Domain**Name*.

If protection fails after completing the steps in the previous procedure, perform the following steps:

1. In Administrative Tools, open Component Services.
2. Expand **Computers**, expand **My Computer**, and then click **DCOM Config**.
3. In the results pane, right-click **DPM RA Service**, and then click **Properties**.
4. In the **Properties** dialog box, click the **Security** tab.
5. In the **Launch and Activation Permissions** area, click **Edit**, and then do one of the following:
   - If the primary server is listed, the Access Control List (ACL) entry might be incorrect. Remove the entry, and then add the primary server with full permissions.
   - If the primary server is not listed, add the primary server with full permissions.

Using DPMSync

DpmSync is a command-line tool that enables you to synchronize the DPM database with the state of the disks in the storage pool and with the installed protection agents. The DpmSync tool restores the DPM database, synchronizes the DPM database with the replicas in the storage pool, restores the Report database, and reallocates missing replicas.

DpmSync Syntax

DpmSync **–RestoreDb –DbLoc location –InstanceName server\instance**]

DpmSync **-Sync**

DpmSync **-ReallocateReplica**

DpmSync **-DataCopied**

Parameters

Parameter	Description
-RestoreDb	Restores a DPM database from a specified location.
-Sync	Synchronizes restored databases.

Parameter	Description
	You must run DpmSync –Sync after you restore the databases. After you run DpmSync –Sync, some replicas may still be marked as missing.
-DbLoc *location*	Identifies the location of backup of DPM database.
-InstanceName *server\instance*	Instance to which DPMDB must be restored.
-ReallocateReplica	Reallocates all missing replica volumes without synchronization.
-DataCopied	Indicates that you have completed loading data into the newly allocated replica volumes. This is applicable for client computers only.

Example 1: To restore the DPM database from local backup media on the DPM server.
Run the following command:

DpmSync –RestoreDb -DbLoc G:\DPM\Backups\2005\November\DPMDB.bak

After you restore the DPM database, to synchronize the databases, you run the following command:

DpmSync -Sync

After you restore and synchronize the DPM database and before you restore the replica, you run the following command to reallocate disk space for the replica:

DpmSync -ReallocateReplica

Example 2: To restore the DPM database from a remote database.
Run the following command on the remote computer:

DpmSync –RestoreDb -DbLoc G:\DPM\Backups\2005\November\DPMDB.bak –InstanceName contoso\ms$dpm

After you restore the DPM database, to synchronize the databases, you run the following command on the DPM server:

DpmSync -Sync

After you restore and synchronize the DPM database and before you restore the replica, you run the following command on the DPM server to reallocate disk space for the replica:

DpmSync -ReallocateReplica

Example 3: To move a DPM database from the local DPM server to a remote SQL server.

The following steps illustrate the use of DPMSync in moving a DPM database (DPMDB) from the local DPM server (DPMServer1) to a remote SQL server (DPMRemoteSQL).

1.	Run the following command: **DPMBackup –db**. This will create the file DPMDB.bak at **\Program Files\Microsoft DPM\DPM\volumes\Shadowcopy\Database Backups**. Store this backup in a secure location.
2.	Uninstall DPM from DPMServer1 and choose to retain data.
3.	Delete DPMDB. You have to do this in order to reinstall DPM.
4.	Install DPM on DPMServer1 with the remote SQL Server instance installed on DPMRemoteSQL.
5.	Run the following command on DPMRemoteSQL **dpmsync –restoredb –dbloc** <*dbbackuplocation*> **–instancename** <*instancename*>, where dbbackuplocation is the location of the backup taken in step 1 and instancename is the name of the remote SQL Server instance.
6.	Now run the following command on DPMServer1 Dpmsync –sync

Improving Usage of WAN Latency

If your deployment of System Center 2012 – Data Protection Manager (DPM) for disaster recovery requires DPM to send large amounts of data over a WAN, you can improve DPM's use of your WAN latency by adjusting the following registry settings:

On the remote DPM server:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize
```

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts
```

On the DPM server:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts
```

For example, using the following settings over a 100 Mbps link with 40 ms latency produces the following results:

Settings	
On the remote DPM server: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize`	524288
On both DPM servers: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts`	3
Results	
One job running	3.45 MB/sec
Three jobs running	~3.00 MB/sec per job

Using pre-backup and post-backup scripts

A *pre-backup script* is a script that resides on the protected computer, is executed before each DPM backup job, and prepares the protected data source for backup.

A *post-backup script* is a script that runs after a DPM backup job to do any post-backup processing, such as bringing a virtual machine back online.

When you install a protection agent on a computer, a ScriptingConfig.xml file is added to the *install path*\Microsoft Data Protection Manager\DPM\Scripting folder on the protected computer. For each protected data source on the computer, you can specify a pre-backup script and a post-backup script in ScriptingConfig.xml.

Note
The pre-backup and post-backup scripts cannot be VBScripts. Instead, you must user a wrapper command around your script containing **cscript myscript.vbs**.

When DPM runs a protection job, ScriptingConfig.xml on the protected computer is checked. If a pre-backup script is specified, DPM runs the script and then completes the job. If a post-backup script is specified, DPM completes the job and then runs the script.

Note
Protection jobs include replica creation, express full backup, synchronization, and consistency check.

DPM runs the pre-backup and post-backup scripts by using the local system account. As a best practice, you should ensure that the scripts have Read and Execute permissions for the

administrator and local system accounts only. This level of permissions helps to prevent unauthorized users from modifying the scripts.

ScriptingConfig.xml

```
<?xml version="1.0" encoding="utf-8"?>

<ScriptConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns="http://schemas.microsoft.com/2003/dls/ScriptingConfig.xsd">

   <DatasourceScriptConfig DataSourceName="Data source">

     <PreBackupScript>"Path\Script Parameters" </PreBackupScript>

     <PostBackupScript>"Path\Script Parameters" </PostBackupScript>

     <TimeOut>30</TimeOut>

   </DatasourceScriptConfig>

</ScriptConfiguration>
```

To specify pre-backup and post-backup scripts

1. On the protected computer, open the ScriptingConfig.xml file in an XML or text editor.

   Note
   The DataSourceName attribute must be provided as **Drive:** (for example, D: if the data source is on the D drive).

2. For each data source, complete the DatasourceScriptConfig element as follows:
   a. For the DataSourceName attribute, enter the data source volume (for file data sources) or name (for all other data sources). The data source name for application data should be in the form of *Instance**Database* for SQL, *Storage group name* for Exchange, *Logical Path**Component Name* for Virtual Server, and *SharePoint Farm**SQL Server Name**SQL Instance Name**SharePoint Config DB* for Windows SharePoint Services.
   b. In the PreBackupScript tag, enter the path and script name.
   c. In the PreBackupCommandLine tag, enter command-line parameters to be passed to the scripts, separated by spaces.
   d. In the PostBackupScript tag, enter the path and script name.
   e. In the PostBackupCommandLine tag, enter command-line parameters to be passed to the scripts, separated by spaces.
   f. In the TimeOut tag, enter the amount of time in minutes that DPM should wait after invoking a script before timing out and marking the script as failed.
3. Save the ScriptingConfig.xml file.

Note

DPM will suffix an additional Boolean (true/false) parameter to the post-backup script command, indicating the status of the DPM backup job.

System Center 2012 – Data Protection Manager

System Center 2012 – Data Protection Manager (DPM) provides administrative tools for protecting and recovering file and application data on the computers in your network, including Microsoft Exchange Server, Microsoft SQL Server, and Windows SharePoint Services, as well as virtual servers and workstations. DPM Help provides a comprehensive set of topics that explain basic DPM concepts and how to perform tasks in DPM. Context-sensitive help is available on most screens and dialog boxes in DPM.

Using DPM Help

By choosing **Help Topics** on the **Help** menu or by clicking **Help** on the **Action** menu, you can open DPM Help, from which you can access a variety of resources to help you with the following tasks.

Working with Protection Groups

Protect Data

Manage Protection Agents

Recover Data

Monitoring Alerts

Monitoring Jobs

Using Reports

Setting System Options

Optimizing Performance

DPM Wizards

Accessibility for People with Disabilities

Viewing context-sensitive help

When you are working in DPM Administrator Console, context-sensitive help is available for the task that you are currently performing:

- From any dialog box, click **Help** or press **F1**.
- From any task area, press **F1**.

Working with Protection Groups

System Center 2012 – Data Protection Manager (DPM) uses protection groups to help you organize and manage the data you protect. A *protection group* is a collection of data sources (such as volumes and shares) that share the same protection configuration. To create and maintain protection groups, use the Protection task area in DPM Administrator Console.

In this section

What Is a protection group?

A *protection group* is a collection of data sources, such as volumes, shares, or Exchange Server storage groups, which have a common protection configuration. Data sources within a protection group are referred to as *protection group members* or simply members. The protection group configuration encapsulates the data backup targets (disk or tape), the protection schedule that specifies how often to synchronize the replica with the live data on the protected computer, and when to create recovery points of the replica and the performance options that you want to enable such as on-the-wire compression and daily consistency checks.

Some of the factors you should consider when deciding how to organize your data into protection groups are the business requirements of your organization, network performance, and the

characteristics of the data. Consider, for example, how often the data changes, how rapidly the data size increases, and how critical it is to be able to recover a very recent copy of lost data. You might also want to consider how frequently you need to back up the data to tape, which data needs to be encrypted or compressed, and the number of backup copies you need available. In most cases, you will want to group data with similar characteristics together.

To help you in designing a storage layout for System Center 2012 – Data Protection Manager (DPM), you can use a Storage Calculator that focuses on outlining the storage capacity requirements based on a set of input factors. For more information, see Storage Calculators for DPM.

The following table shows the data sources DPM protects and the level of data that you can recover using DPM.

Product	Protectable Data	Recoverable Data
• Exchange Server 2003 with Service Pack 2 (SP2) • Exchange Server 2007 SP2 • Exchange Server 2013	Storage group	• Storage group • Database • Mailbox
Exchange Server 2010	Exchange database	Database Mailbox
• SQL Server 2000 with Service Pack 4 (SP4) • SQL Server 2005 SP1, SP2, SP3 • SQL Server 2008 • SQL Server 2008 SP1 • SQL Server 2012	• Database	• Database
Microsoft Office SharePoint Server (MOSS) 2007	• Farm • Search Shared Services Provider (SSP)	• Farm • Database • Site Collection • Site • File • List or document library • List item • Search Shared Services Provider (SSP)
Windows SharePoint Services 3.0	Farm SharePoint Search	• Farm • Database • Site Collection

Product	Protectable Data	Recoverable Data
		• Site • File • List or document library • List item • SharePoint Search
Microsoft SharePoint Server 2010 Microsoft SharePoint Foundation 2010 SharePoint Server 2013	Farm	• Farm • Database • Site Collection • Site • File • List or document library • List item **Note** Item-level recoveries can be performed without a recovery farm.
• Windows Server 2003 • Windows Storage Server 2003 • Windows Server 2008 (Standard and Enterprise editions) • Windows Server 2008 R2 (Standard and Enterprise editions) • Windows Server 2012	• Volume • Share • Folder	• Volume • Share • Folder • File
Microsoft Virtual Server 2005 R2 SP1	• Virtual server host configuration • Virtual machines • Data for applications running in virtual machines	• Virtual server host configuration • Virtual machines • Data for applications running in virtual machines
• Microsoft Hyper-V in x64-bit versions of Windows Server 2008 R2 • Microsoft Hyper-V in x64-bit versions of Windows Server 2012 R2	Virtual machines on the following deployments of Hyper-V: Cluster Shared Volumes (CSV) Highly available virtual machines on a	Virtual machines Item level recovery (item-level recovery of files, folders, volumes, and virtual hard disks (VHDs) from a host-level backup of Hyper-

Product	Protectable Data	Recoverable Data
	failover cluster Stand-alone hosts Windows Server/Server Core and Microsoft Hyper-V Server & Local Data Source Protection	V virtual machines to a network share or a volume on a DPM protected server).
Microsoft Hyper-V in x64-bit versions of Windows Server 2008	Virtual machines on the following deployments of Hyper-V: Stand-alone hosts Windows Server/Server Core and Microsoft Hyper-V Server & Local Data Source Protection Shared disk cluster	Virtual machines Item level recovery (item-level recovery of files, folders, volumes, and virtual hard disks (VHDs) from a host-level backup of Hyper-V virtual machines to a network share or a volume on a DPM protected server).
Client computers –desktops and laptops running: • Windows XP Professional SP2 • Windows Vista editions except Home (must be member of a domain) • Windows 7	File data	File data
Bare Metal Recovery (BMR) for computers that are running Windows Server 2008 and Windows Server 2003 **Note** To perform BMR operations on computers that are running Windows Server 2003, install DPM System Recovery Tool (SRT)	BMR	BMR and System State
System State for computers that are running Windows Server 2008 and Windows Server 2003	System State	System State

After a data source is added to a protection group, the data source is described as a member of the group. Before you can start protecting data, you must create at least one protection group. For more information about protection groups, see Planning Protection Groups.

See Also

Consistency check

What Is a Recovery Point?

Understand replicas

Synchronization

Create a protection group

A *protection group* is a collection of data sources that share the same protection configuration. Data sources within a protection group are referred to as *protection group members*. For information about managing protection groups, see Deploying DPM.

Before you can create your first protection group, you must add a disk to the storage pool and install agents on the computers you plan to protect.

To create a protection group, use the New Protection Group Wizard.

You can use System Center 2012 – Data Protection Manager (DPM) to protect the following protection group members:

To view the table that shows the data sources that System Center 2012 – Data Protection Manager (DPM) protects and the level of data that you can recover using DPM, see What Is a protection group?

To start the Create New Protection Group Wizard

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Create protection group**. The Create New Protection Group Wizard appears.
3. Review the **Welcome** page, and then click **Next**.

   Note
   If you do not want the wizard to display the **Welcome** page when you create protection groups in the future, select **Skip this page next time**.

To create and save a protection group using DPM Management Shell

- Use the following syntax to create a virtual instance of a new protection group:

  New-ProtectionGroup [-DPMServerName] <*String*> **[[-Name]** <*String*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable**

<*String*>] **[-OutBuffer** <*Int32*>**]**

- Add data sources to the new protection group.
- Set exclusions and job start times if required.
- Set the protection type.
- Set the replica creation method.
- Set the policy objectives.
- Use the following syntax to save the new protection group:

  Set-ProtectionGroup [-ProtectionGroup] <*ProtectionGroup*> **[-Async] [-TranslateDSList** <*Datasource[]*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help New-ProtectionGroup -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help New-ProtectionGroup -full**" in DPM Management Shell.

See Also

New Protection Group Wizard

Delete a protection group

A *protection group* is a collection of data sources that share the same protection configuration. Data sources within a protection group are referred to as *protection group members*.

To delete a protection group, you must first stop protection of the group. You can use the following procedure to stop protection and enable deletion of a protection group.

To delete a protection group by stopping protection

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the protection group to stop protecting.
3. In the **Actions** pane, click **Stop protection of group**. The **Stop Protection** dialog box appears.
4. Choose whether to retain or delete protected data:
   a. Click **Retain protected data** to retain the replica on disk with associated recovery points and tapes for the retention range.
   b. Click **Delete protected data** to delete the replica on disk and expire the recovery points on tapes.
5. Click **Stop Protection**. Data sources within the protection group are no longer protected, and DPM deletes the protection group.

See Also

New Protection Group Wizard

What Is a protection group?

Co-Locating Data on Disk

Add members to a protection group

After you create a protection group, you might want to protect a data source on a protected volume that you did not select for protection when you created the group.

The following are guidelines for adding members to a protection group:

- When you select a data source that contains a reparse point (mount points and junction points are data sources that contain reparse points), System Center 2012 – Data Protection Manager (DPM) prompts you to specify whether you want to include the target of the reparse point in the protection group. The reparse point itself is not replicated; you must manually re-create the reparse point when you recover the data.
- We recommend that you exclude system volumes and program folders from protection as a volume or share. Protecting a volume that contains system files and program folders does not enable you to restore the operating system or state of a computer. To restore the state of a computer, you must select the computer's system state as the protected data source. For information about restoring a computer, see **Disaster Recovery**.
- All storage groups on a single computer running Exchange Server 2003 must be in the same protection group.

To add protection group members

1. In DPM Administrator Console, go to **Protection** view.
2. In the display pane, select the protection group to which you want to add members.
3. Click **Modify**.
4. In the Modify Protection Group Wizard, follow the instructions to add data sources to the protection group.

To add protection group members using DPM Management Shell

- Use the following syntax to add a member to a protection group:

  Add-ChildDatasource -ProtectionGroup <*ProtectionGroup*> **-ChildDatasource** <*ProtectableObject[]*> **[-PassThru]**

  For more information, type "**Get-Help Add-ChildDatasource -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Add-ChildDatasource-full**" in DPM Management Shell.

See Also

Remove protection group members

What Is a protection group?

Working with Protection Groups

Add a client computer to a protection group

You can add a client computer by modifying the protection group for the client computer.

1. Right-click an existing protection group for the client computer.
2. Select **Add client computers**.

   A page appears allowing you to select and add new client computers.
3. Click **Next** to add the client computers to the protection group.

See Also

Working with Protection Groups

Choose a replica creation method

To begin protection of selected data, System Center 2012 – Data Protection Manager (DPM) must create a replica of the data. To create the replica, you can let DPM replicate the data over the network, you can specify a date and time for the replication, or you can choose to manually copy the data. The manual option requires you to transfer the data using removable media.

Note

For large amounts of data, manually copying data to the DPM server might take less time than replication over the network.

To choose a replica creation method

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Create protection group**. The Create New Protection Group Wizard appears.
3. Review the **Welcome** page, and then click **Next**.

   Note

   If you do not want the wizard to display the **Welcome** page when you create

protection groups in the future, select **Skip this page next time**.

4. Select group members you want to protect, and click **Next**.
5. Select the data protection method, and click **Next**.
6. Select short-term protection objectives, and click **Next**.
7. Review disk allocation, and click **Next**.
8. Select the replication method. Click **Automatically** to let DPM replicate the data over the network.
9. To select when you want to have DPM replicate the data, click **Now** or **Later**. If you select **Later**, select the date and time for the replica creation from the drop-down menus.
10. Click **Manually** if you want to transfer the data using removable media.
11. Click **Next** to finish the Create New Protection Group Wizard.

Note

You can optimize performance of the protection group on the **Summary** page or you can choose to optimize the group later from the **Actions** pane.

To choose a replica creation method by using DPM Management Shell

- Use the following syntax to retrieve the replica creation method for a protection group:

  Get-DPMReplicaCreationMethod [-ProtectionGroup] <*ProtectionGroup*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

- Use the following syntax to set the replica creation method for a protection group to **Now**:

  Set-DPMReplicaCreationMethod [-ProtectionGroup] <*ProtectionGroup*> **-Now [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

- Use the following syntax to set the replica creation method for a protection group to the specified time:

  Set-DPMReplicaCreationMethod [-ProtectionGroup] <*ProtectionGroup*> **-Later** <*DateTime*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

- Use the following syntax to set the replica creation method for a protection group to **Manual**:

  Set-DPMReplicaCreationMethod [-ProtectionGroup] <*ProtectionGroup*> **-Manual [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Set-DPMReplicaCreationMethod -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Set-DPMReplicaCreationMethod -full**" in DPM Management Shell.

See Also

Working with Protection Groups

Work with replicas

Remove protection group members

After a protection group is created, you might determine that some or all of the data sources in the protection group no longer need to be protected. To stop protecting data, remove the members that you no longer want to protect from the protection group. When the member is removed, System Center 2012 – Data Protection Manager (DPM) displays its status as "Inactive protection."

To delete protected data of any data source, you must remove inactive protection, which you can do by deleting the replica or expiring the data on the associated tapes. This frees up disk space and tapes for use by other protection groups.

To delete a protection group altogether, you must remove all the members in the protection group. Removing all members automatically deletes the protection group.

To remove a protection group member from protection

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, select the protection group member that you want to remove.

   Note
   You can select multiple members and remove them at the same time.
3. Click **Stop protection** on the tool ribbon.
4. In the **Stop Protection** dialog box, choose whether you want to retain the protected data or delete it.

   Note
   To stop protection on co-located data sources, see Stopping Protection for Co-Located Data

   Click **Retain Protected Data** to retain the replica on disk with associated recovery points and tapes for the retention range. These can be deleted later.

   Click **Delete protected data** to delete the replica on disk and expire data on tapes. The tapes remain available for other protection groups.
5. Verify that you want to remove the members displayed on the **Replica on Disk** tab. If you decide not to remove the member, click **Cancel** at the bottom of the dialog box.
6. After you click **Stop Protection**, you cannot cancel this action. DPM displays "Inactive replica available" as the status of this member.

To remove inactive protection for a protection group member

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, select the protection group member for which you want to remove inactive protection.

   Note
   You can select multiple members and remove them at the same time.
3. Click **Remove inactive protection** from the tool ribbon.
4. To delete the replica on disk, in the **Delete Inactive Protection** dialog box, you must select **Delete replica on disk** check box.
5. Optionally select **Expire the data on the tapes**. The data for the selected inactive protection group members is marked for expiration. The tapes will not be marked as free until all other data has been expired.
6. Click **OK**.

To remove a protection group member by using DPM Management Shell

- Use the following syntax to remove a member from a protection group:

  Remove-ChildDatasource -ChildDatasource <*ProtectableObject[]*> **-ProtectionGroup** <*ProtectionGroup*> **[-PassThru] [-KeepDiskData]**

  For more information, type "**Get-Help Remove-ChildDatasource -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Remove-ChildDatasource-full**" in DPM Management Shell.

See Also

Add members to a protection group

Create a protection group

Delete a protection group

How to Install DPM Management Shell

What Is a protection group?

Co-Locating Data on Disk

Rename a protection group

You can use the following procedure to rename a protection group in System Center 2012 – Data Protection Manager (DPM). Changing the name of a protection group has no impact on your protection configuration.

To rename a protection group

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the protection group that you want to rename.
3. In the **Actions** pane, click **Modify protection group**. This starts the Modify Group Wizard.
4. Click **Next**.
5. On the **Select Data Protection Method** screen, in the **Protection group name** field, type the new name of the protection group.
6. Click **Next** until you exit the wizard.

   The name change takes effect immediately.

To rename a protection group using DPM Management Shell

- Use the following syntax to retrieve the protection group:

  Get-ProtectionGroup [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to make the protection group modifiable:

  Get-ModifiableProtectionGroup [-ProtectionGroup] <*ProtectionGroup*>**[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to rename the protection group:

  Rename-ProtectionGroup [-ProtectionGroup] <*ProtectionGroup*>**[-NewName]** <*String*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to save the changes to the protection group:

  Set-ProtectionGroup [-ProtectionGroup] <*ProtectionGroup*> **[-Async] [-TranslateDSList** <*Datasource[]*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Rename-ProtectionGroup -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Rename-ProtectionGroup -full**" in DPM Management Shell.

See Also

Create a protection group

Working with Protection Groups

Modify protection options

When you create a protection group, you set protection options or accept the default settings for synchronization, recovery points, consistency checks, and network performance. After you create a protection group, you can modify these settings, as needed, to better meet your data protection requirements and optimize network performance.

Note
You can set data co-location only one time through the Create New Protection Group Wizard. You cannot modify it in the **Review Disk Allocation** page of the Modify Group wizard.

Note
If you are modifying protection for Exchange Server Standby Continuous Replication (SCR), on the **Specify Short-Term Goals** page of the Modify Group wizard, you can only select **Express full backups**.

The following procedures provide steps to set synchronization options and to perform a consistency check. For information about how to optimize performance using network bandwidth usage throttling, on-the-wire compression, and specifying start times for synchronization jobs, see Optimizing Performance.

To set synchronization options

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the protection group for which you want to set synchronization options.
3. In the **Actions** pane, click **Modify protection group**. This starts the Modify Protection Wizard.
4. Select group members, and click **Next**.
5. Select the data protection method and click **Next**.
6. On the **Select Short-Term Objectives** page, select the synchronization frequency.

   Important
   If you are protecting computers in a time zone that is different from that of the DPM server, the times specified in the **Modify Protection Options** dialog box are protected computer times.
7. On the **Specify Long-Term Objectives** page, specify long-term recovery goals for protection.
8. On the **Select Library and Tape Details** page, specify tape and library details and click **Next**.
9. On the **Summary** page, click **Update Group**.
10. Click **Close** to exit the wizard.

Note
If DPM displays a **Replica inconsistent** error, you should perform a consistency check.

To perform a consistency check

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Display** pane, select the protection group member for which you want to perform a consistency check.
3. In the **Actions** pane, click **Perform consistency check**.
4. In the dialog that notifies you that a consistency check is a lengthy operation, click **OK**.

To make a protection group modifiable using DPM Management Shell

- Use the following syntax to retrieve a protection group:

  Get-ProtectionGroup [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to make the retrieved protection group modifiable:

  Get-ModifiableProtectionGroup [-ProtectionGroup] <*ProtectionGroup*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Get-ModifiableProtectionGroup -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Get-ModifiableProtectionGroup -full**" in DPM Management Shell.

To set synchronization options (policy schedule) using DPM Management Shell

- Use the following syntax to retrieve policy schedule:

  Get-PolicySchedule [-ProtectionGroup] <*ProtectionGroup*> **-OffsetSchedule [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  Get-PolicySchedule [-ProtectionGroup] <*ProtectionGroup*> **-ShortTerm [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  Get-PolicySchedule [-ProtectionGroup] <*ProtectionGroup*> **-LongTerm [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**][-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to set the policy schedule:

  Set-PolicySchedule [-ProtectionGroup] <*ProtectionGroup*> **[-Schedule]** <*Schedule*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable**

<*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

Set-PolicySchedule [-ProtectionGroup] <*ProtectionGroup*> **[-OffsetInMinutes]** <*Int32*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable** <*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

For more information, type "**Get-Help Set-PolicySchedule -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Set-PolicySchedule -full**" in DPM Management Shell.

To set synchronization options (policy objective) using DPM Management Shell

- Use the following syntax to retrieve the policy objective:

  Get-PolicyObjective [-ProtectionGroup] <*ProtectionGroup*> **-LongTerm [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable** <*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

  Get-PolicyObjective [-ProtectionGroup] <*ProtectionGroup*> **-ShortTerm [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable** <*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

- Use the following sybtax to set the policy objective:

  Set-PolicyObjective [-ProtectionGroup] <*ProtectionGroup*> **[-RetentionRangeInDays]** <*Int32*> **[[-SynchronizationFrequency]** <*Int32*>] **[-BeforeRecoveryPoint] [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable** <*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

  Set-PolicyObjective [-ProtectionGroup] <*ProtectionGroup*> **[-RetentionRangeInWeeks]** <*Int32*> **[-ShortTermBackupFrequency]** <*BackupFrequency*> **[-CreateIncrementals] [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable**<*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

  Set-PolicyObjective [-ProtectionGroup] <*ProtectionGroup*> **[-RetentionRange]** <*RetentionRange*> **[-LongTermBackupFrequency]** <*BackupFrequency*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable** <*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

  Set-PolicyObjective [-ProtectionGroup] <*ProtectionGroup*> **[-RetentionRangeList]** <*RetentionRange[]*> **[-FrequencyList]** <*Int32[]*> **[-GenerationList]** <*GenerationType[]*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>] **[-ErrorVariable** <*String*>] **[-OutVariable** <*String*>] **[-OutBuffer** <*Int32*>]

  For more information, type "**Get-Help Set-PolicyObjective -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Set-PolicyObjective -full**" in DPM Management Shell.

To perform a consistency check using DPM Management Shell

- Use the following syntax to perform a consistency check:

  Start-DatasourceConsistencyCheck [-Datasource] <*Datasource*>**[-HeavyWeight] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**][-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Start-DatasourceConsistencyCheck -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Start-DatasourceConsistencyCheck -full**" in DPM Management Shell.

See Also

Optimizing Performance

Consistency check

What Is a Recovery Point?

Synchronization

Working with Protection Groups

Co-Locating Data

Get a list of protection groups

System Center 2012 – Data Protection Manager (DPM) provides a way for you to list all protection groups and their status.

To list protection groups

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Display** pane, in the **Group by** field, select **Protection Group**.
3. DPM displays all protection groups and their status. To group by computer, in the Display pane, in the **Group by** field, select **Computer**.

To list protection groups by using DPM Management Shell

- Use the following syntax to list all the protection groups:

  Get-ProtectionGroup [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Get-ProtectionGroup -detailed**" in DPM

Management Shell.

For technical information, type "**Get-Help Get-ProtectionGroup -full**" in DPM Management Shell.

See Also

How to Install DPM Management Shell

What Is a protection group?

Working with Protection Groups

Protect clustered resources

Loosely defined, a *cluster* is a group of machines that collaborate to provide highly available services to clients. The machines that comprise the cluster maintain their identity, but some level of abstraction is provided to clients of the service.

For example, a clustered Windows file server enables access to clustered file shares through a Common Internet File System. When a node fails, another node takes over, providing continued shares' access to clients with some level of transparency.

System Center 2012 – Data Protection Manager (DPM) provides support for clustered resources on a network.

Important

You must install a protection agent on all nodes of a cluster to support cluster protection. When you enable or disable a protection agent for a node on a cluster, you must enable or disable the agents for all nodes of the cluster.

The following procedure shows you how to configure protection for clustered resources.

To protect clustered resources

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Create a protection group**.
3. In the **Create New Protection** dialog box, in the **Available members** pane, choose the data you want to protect by selecting the check boxes.

   Note

   Clusters are listed in the **Available members** pane. You might need to click the plus sign (+) to expand the cluster.
4. Click **Next**.
5. Complete the Create New Protection Group Wizard.
6. On the **Summary** page, click **Create Group**.

See Also

New Protection Group Wizard

Working with Protection Groups

View tapes associated with a protection group

If you are using tape-based protection, you can view the tapes associated with specific protection groups. The following procedures show you how to get a list of tapes.

To view tapes associated with a protection group

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the protection group for which you want to display associated tapes.
3. In the **Action** pane, click **View tape list**.

   DPM displays a **View Tape List** dialog box with the name of the protection group and tape details, including associated label, bar code, and library.
4. Click **Close** to close the **View Tape List** dialog box.

To view tapes associated with a protection group using DPM Management Shell

- Use the following syntax to view tapes associated with a protection group:

  Get-Tape [-ProtectionGroup] <*ProtectionGroup[]*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Get-Tape -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Get-Tape -full**" in DPM Management Shell.

See Also

Managing Tapes

Stop protection for a protection group

You might decide that you no longer need to protect a specific protection group in System Center 2012 – Data Protection Manager (DPM). When you stop protection of a protection group, DPM automatically deletes the group.

To stop protecting a protection group

1. In DPM Administrator Console, on the navigation bar click, **Protection**.
2. In the display pane, select the protection group to stop protecting.
3. In the **Actions** pane, click **Stop protection of group**. The **Stop Protection** dialog box appears.

   Note
   To stop protection on co-located data sources, see Stopping Protection for Co-Located Data.
4. Choose whether to retain or delete protected data.

   Click **Retain protected data** to retain the replica on disk with associated recovery points and tapes for the retention range.

   Click **Delete protected data** to delete the replica on disk and expire the data on tapes.

   Note
   When you select **Delete protected data,** tapes become free for use by other protection groups.
5. Clear the **Delete replica on disk** check box if you do not want to delete the replica.
6. Clear the **Expire all the datasets in the tapes** check box to mark the tapes as free when they are online.
7. Click **Stop Protection**.

See Also

Working with Protection Groups

Co-Locating Data on Disk

Exclude data sources from a protection group

System Center 2012 – Data Protection Manager (DPM) allows you to create a protection group for application or file data and exclude specific file data sources from protection. You can choose to exclude data sources that do not change or that are no longer current. The following procedures show you how to exclude data sources from a protection group.

To exclude data sources from a protection group

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. On the **Actions** menu, click **Create protection group**. This launches the Create New

Protection Group Wizard.

3. To choose the data to protect, on **the Select Group Members** page, in the **Available Members** pane, select the check boxes that correspond to the data.
4. To exclude a folder, expand the directory structure and clear the check box next to the folder.
5. To exclude specific file types from protection, in the **Selected Members** pane, click **Exclude Files**.
6. In the **Exclude File Types** dialog box, type the file name extensions you want to exclude and click **OK.**

   Note
   To separate multiple file types, use a comma with no space; for example, .mp3,.mpeg,.avi
7. When you complete the wizard, click **Create Group**.

   Note
   To exclude data sources or file types from a protection group after the protection group has been created, on the **Actions** menu, click **Modify protection group** to launch the wizard, and then exclude data sources and file types on the **Select Group Members** page.

To remove data sources using DPM Management Shell

- Use the following syntax to retrieve a data source from a protection group:

  Get-ChildDatasource [-ChildDatasource] <*ProtectableObject*> **[[-ProtectionGroup]** <*ProtectionGroup*>**] [-Inquire] [-Async] [-Tag** <*Object*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to remove a data source from a protection group:

  Remove-ChildDatasource [-ProtectionGroup] <*Protection Group*> **[-ChildDatasource]** <*ProtectableObject*> **[-KeepDiskData] [-PassThru] [<CommonParameters>]**

  For more information, type "**Get-Help Remove-ChildDatasource -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Remove-ChildDatasource-full**" in DPM Management Shell.

See Also

New Protection Group Wizard

Working with Protection Groups

Compress data in a protection group

Compressing data for tape can result in significant savings in time, hardware, and performance. By compressing data, you are able to put more data on tape and use fewer tape drives. System Center 2012 – Data Protection Manager (DPM) supports compressing data in protection groups on tape for long-term and short-term protection. The following procedure shows you how to compress data in a protection group.

Note
DPM does not support compression if you choose to encrypt data in a protection group.

To compress data in a protection group

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. On the **Actions** menu, click **Create protection group**. This starts the Create New Protection Group Wizard.
3. On the **Welcome to the New Protection Group Wizard** page, click **Next**.

   Note
   You can choose not to display the **Welcome** page by selecting the **Do not show this Welcome page again** check box.
4. Select the members of the protection group by selecting the check boxes in the **Available members** pane, and click **Next**.
5. Select the data protection method and click **Next**.
6. Select short-term objectives for the protection group, and click **Next**.
7. Review disk allocation and click **Next**. You can also modify the disk space allocated in protected computers by clicking **Modify**.
8. Select long-term protection goals and a backup schedule for the protection group, and click **Next**.
9. On the **Select Tape and Library Details** page, specify details about the library, drives allocated, and copy library you would like to use for backup.
10. In the **Tape options for long-term protection** pane, click **Compress data** and then click **Next**.
11. Choose a replica creation method for the protection group, and click **Next**.
12. On the **Summary** page, click **Create Group**.

    Note
    If you want to compress data in a protection group that has already been created, in DPM Administrator Console, click **Protection** on the navigation bar. Select a protection group. Then on the **Actions** menu, click **Modify protection group**. Follow the Modify Protection Group Wizard, and on the **Select Tape and Library Details** page, click **Compress data**.

See Also

New Protection Group Wizard

Working with Protection Groups

Remove inactive protection for group members

After you have removed a member from protection and chosen to retain or delete protected data, System Center 2012 – Data Protection Manager (DPM) displays the protection status as "Inactive Replica Available." You can remove inactive protection by deleting the replica and, if tape protection was available, by expiring the recovery points on the associated tapes. This frees up disk space and tapes for use by other protection groups. The following procedure shows you how to remove inactive protection for group members.

Note
For co-located data sources, see Co-Locating Data.

To remove inactive protection

1. In DPM Administrator Console, go to the **Protection** tab.
2. In the display pane, select the group member for which you want to remove inactive protection.
3. Click **Remove inactive protection** on the tool ribbon.
4. Select whether you want to delete the replica on disk or expire the recovery points on tape.

   Note
   The tapes are not marked free until all other data on the tapes is expired.
5. On the **Tasks** tab, click **Close**.

See Also

Create a protection group

Remove protection group members

Working with Protection Groups

Encrypt data in a protection group

One of the benefits of storing backups on tape is portability. However, if the tapes get in the wrong hands, data security could be compromised. System Center 2012 – Data Protection Manager (DPM) supports encrypting data on tape for long-term protection. The following procedure shows you how to encrypt data that will be backed up on tape.

To encrypt data in a protection group

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. On the **Actions** menu, click **Create protection group**. This starts the Create New Protection Group Wizard.
3. On the Welcome to the New Protection Group Wizard, click **Next**.

   Note
   You can choose not to display the **Welcome** screen by selecting the **Do not show this Welcome page again** check box.
4. Select the members of the protection group by selecting the check boxes in the **Available members** pane, and then click **Next**.
5. Select the data protection method, and then click **Next**.
6. Select short-term goals for the protection group, and then click **Next**.
7. Review the storage pool disk space allocated for this protection group. You can also modify the size of the replica volume and recovery point volume by clicking **Modify**.
8. Specify long-term goals and a backup schedule for the protection group, and then click **Next**.
9. On the **Select Tape and Library Details** page, specify details about the tape and library that you would like to use for backup.
10. In the **Tape options for long-term protection** pane, click **Encrypt data**.

    Note
    A valid encryption certificate must be available on the DPM server to support this long-term protection option.
11. Click **Next**.
12. Choose a replica creation method for the protection group, and then click **Next**.
13. On the **Summary** page, click **Optimize performance** to optimize performance for the protection group, and then click **Create Group**.

    Note
    If you want to encrypt data in a protection group that has already been created, in DPM Administrator Console, on the navigation bar, click **Protection**. Select a protection group. Then, on the **Actions** menu, click **Modify protection group**. Follow the Modify Protection Group Wizard, and on the **Select Tape and Library Details** page, click **Encrypt data**.

See Also

Create a protection group

Create self-signed certificates for successful encryptions

Import certificates into DPMBackupStore

Install/remove certificates from a certification authority

Managing Tapes

Optimizing Performance

What Are certificates?

What Are certificates?

Digital certificates are electronic credentials that are used to certify the online identities of individuals, computers, and other entities on a network. Digital certificates function similarly to identification cards such as passports and drivers' licenses. They are issued by certification authorities (CAs) that must validate the identity of the certificate holder, both before the certificate is issued and when the certificate is used. Common uses include business scenarios requiring authentication, encryption, and digital signing.

System Center 2012 – Data Protection Manager (DPM) supports the following types of certificates for media encryption:

- Self-signed certificates
- Imported certificates from certification authorities

In addition, DPM supports backup and recovery of certificates.

Self-signed certificates

Self-signed certificates are not signed by a certification authority. These certificates ensure that encrypted Web connections are in place; however, they do not guarantee the identity of the organization that generated the certificate. Self-signed certificates are useful if the ability to encrypt data is more important than the ability to identify the issuing organization.

Imported certificates

Certification authority (CA) certificates are certificates that are issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two CAs.

A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy.

After the trusted root has been established, it can be used to authorize subordinate CAs to issue certificates on its behalf.

Although the relationship between CAs is most commonly hierarchical, CA certificates can also be used to establish trust relationships between CAs in two different public key infrastructure (PKI) hierarchies.

In all of these cases, the CA certificate is critical to defining the certificate path and usage restrictions for all end entity certificates issued for use in the PKI.

See Also

Import certificates into DPMBackupStore

Install/remove certificates from a certification authority

Create self-signed certificates for successful encryptions

Create self-signed certificates for successful encryptions

System Center 2012 – Data Protection Manager (DPM) supports two types of certificates to successfully encrypt data at a protection group level: self-signed certificates and certificates imported from a certification authority (CA). You can create a self-signed certificate using *makecert.exe*.

Important
You should use a certificate store to securely store your certificates. The .snk files used by this tool store private keys in an unprotected manner. When you create or import a .snk file, you should be careful to secure it during use and remove it when you are done.

SSL server certificates for Internet Information Services (IIS) are stored in the "Personal" ("My") certificate store of the "computer account" ("localMachine"). The "Certificates" snap-in of the Microsoft Management Console (mmc.exe) must be used to manage these certificates. The certificate management window (accessible from "Internet Properties" / "Content" / "Certificates" or from "Control Panel" / "Users and Passwords" / "Advanced" / "Certificates") cannot be used.

To create a self-signed certificate

- See Internet Information Services (IIS) Server Certificate Installation Instructions.

To import self-signed certificates into DPMBackupStore Using Makecert.exe

- Type the following command

  Makecert.exe -r -n "CN=MyCertificate" -ss DPMBackupStore -sr localmachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 -e <*expiry date in mm/dd/yyformat*>

See Also

Import certificates into DPMBackupStore

What Are certificates?

Install/remove certificates from a certification authority

System Center 2012 – Data Protection Manager (DPM) supports two types of certificates to successfully encrypt data at a protection group level: self-signed certificates and certificates imported from a certification authority (CA). Click the link in the following procedure to get information about how to install and remove trusted certificates.

Note

SSL server certificates for Internet Information Services (IIS) are stored in the "Personal" ("My") certificate store of the "computer account" ("localMachine"). The "Certificates" snap-in of the Microsoft Management Console (mmc.exe) must be used to manage these certificates. The certificate management window (accessible from "Internet Properties" / "Content" / "Certificates" or from "Control Panel" / "Users and Passwords" / "Advanced" / "Certificates") cannot be used.

To install and remove trusted certificates

- See "Installing and Removing Trusted Certificates" in Chapter 6. Digital Certificates.

See Also

Create self-signed certificates for successful encryptions

Import certificates into DPMBackupStore

What Are certificates?

Import certificates into DPMBackupStore

Before you can use encryption in System Center 2012 – Data Protection Manager (DPM), you need to do the following:

- Import certificates from a CA or create a self-signed certificate
- Manage your account in Microsoft Management Console (MMC)
- Import certificates into DPMBackupStore

When you import a certificate, you copy the certificate from a file that uses a standard certificate storage format to a certificate store for your user account or your computer account.

The following procedures describe how to manage your account in MMC and import certificates into the DPM certificate store, DPMBackupStore.

To manage your account in MMC

- See Manage Certificates for Your User Account.

To import certificates into DPMBackupStore

1. In MMC, open the **Certificates** snap-in.
2. In the console tree, click **DPMBackupStore**.
3. On the **Action** menu, point to **All Tasks**, and then click **Import** to start the Certificate Import Wizard.
4. Click **Next**.
5. Type the name of the file that contains the certificate to be imported, or click **Browse** and navigate to the file.

   Certificates can be stored in several different file formats. The most secure format is Public-Key Cryptography Standard (PKCS) #12, an encryption format that requires a password to encrypt the private key. For optimum security, send certificates using this format.

   If the certificate file is in a format other than PKCS #12, skip to step 8.

   If the certificate file is in the PKCS #12 format, do the following:

   a. In the **Password** box, type the password used to encrypt the private key. You must have access to the password that was originally used to secure the file.

   b. (Optional) If you want to be able to use strong private key protection, select the **Enable strong private key protection** check box, if available.

   c. (Optional) If you want to back up or transport your keys at a later time, select the **Mark key as exportable** check box.
6. Click **Next**.
7. In the **Certificate Store** dialog box, select **Place all certificates in the following store**, click **Browse**, and select **DPMBackupStore**.
8. Click **Next**, and then click **Finish**.

   Note
   The file from which you import certificates remains intact after you have imported the certificates. You can use Windows Explorer to delete the file if it is no longer needed.

To import self-signed certificates into DPMBackupStore Using Makecert.exe

- Type the following command

  Makecert.exe -r -n "CN=MyCertificate" -ss DPMBackupStore -sr localmachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 -e <*expiry*

date in mm/dd/yyformat>

See Also

Install/remove certificates from a certification authority

What Are certificates?

Protect Data

One of the primary purposes of System Center 2012 – Data Protection Manager (DPM) is to protect valuable data assets from possible loss or corruption. With DPM, protecting data is easy and recovering protected data is intuitive and fast.

In this section

How does data protection work?

Types of backups DPM supports

Retention range

Protection policy

Express full backup

Auto discovery

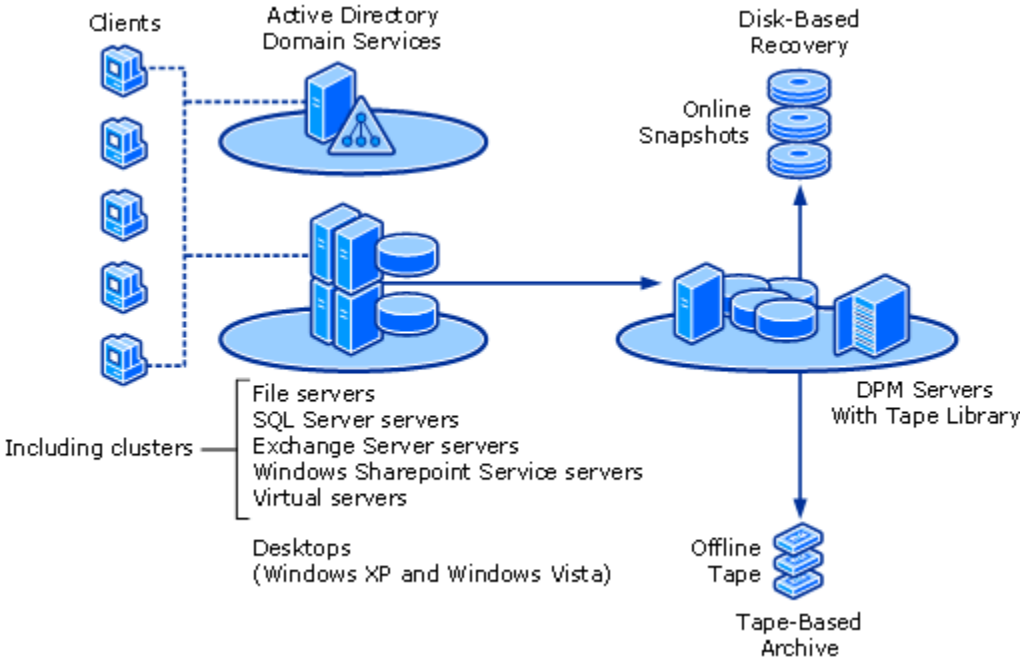
Work with replicas

How does data protection work?

System Center 2012 – Data Protection Manager (DPM) helps you manage the process of protecting and recovering data on the application servers, file servers, and workstations in your network. This topic describes the high-level steps you need to perform to successfully protect and recover data in the DPM environment.

Protecting data

The DPM protection process involves creating and maintaining a full replica of the protected data and regularly creating recovery points of the synchronized replica. The replica serves as a full backup of the protected data. The recovery points allow you to recover previous versions of the protected data. The following illustration shows the protection process.



Retention range is always capped at 64 days whether DPM is protecting a file server, a workstation, or an application server. The maximum number of recovery points for each data source type are provided in the following table.

Type of data source	Maximum number of disk-based recovery points
Files	64 spread over a maximum of 448 days.
Exchange Server	Maximum of 96 per day. Express full backups spread over a maximum of 448 days.
SQL Server	Maximum of 96 per day. 512 Express full backups spread over a maximum of 448 days.
Windows SharePoint Services	512 spread over a maximum of 448 days.
Virtual Server	512 spread over a maximum of 448 days.
Hyper-V	512 spread over a maximum of 448 days.

Recovering data

The DPM recovery process involves choosing a previous version of the data source from the stored recovery points on the DPM server, and then restoring a copy of the selected data to its point of origin or to an alternate location.

See Also

What Is a protection group?

What Is a Recovery Point?

Understand replicas

Synchronization

Types of backups DPM supports

System Center 2012 – Data Protection Manager (DPM) supports a variety of backup scenarios, including the following:

- Disk-based data protection and recovery.
- Tape-based backup and archive solutions.

To view the table that shows the data sources that DPM protects and the level of data that you can recover using DPM, see What Is a protection group?

Disk-based and tape-based support

With DPM data protection, you can use disk-based storage, tape-based storage, or both.

Disk-based storage, also called *D2D* (disk-to-disk), is a type of backup in which data from one computer is stored on the hard disk of another computer. This contrasts with the more traditional method of backing up data from one computer to a storage media such as tape, also called *D2T* (disk-to-tape). For extra protection, the two methods can be combined in a *D2D2T* (disk-to-disk-to-tape) configuration, which provides the rapid recovery benefits of disk-based storage in the short term and archive storage for critical data using tape-based storage in the long term.

See Also

Managing Disks

Managing Tapes

Retention range

A *retention range* is the duration of time for which the data is available for recovery.
System Center 2012 – Data Protection Manager (DPM) retains recovery points for the duration that is specified in the retention range. Any day that the replica is not consistent does not count toward the retention range.

When DPM protection is stopped temporarily because the replica is inconsistent, DPM does not delete expired recovery points until protection resumes. For example, if you specify a retention

range of 10 days, on day 1, recovery points are created. On day 2, the replica becomes inconsistent. On day 3, the scheduled consistency check runs and the replica is made consistent. Because the replica was inconsistent for one day, the recovery points from day 1 are not deleted until after day 11.

However, if disk co-location is enabled, then the recovery points of the data sources whose protection is stopped will be removed according to the retention range of its protection group. This is because the replica volume on which that data source resides is shared by other data sources. For example, if you specify a retention range of 10 days, on day 1, recovery points are created. On day 2, the replica of one of the data sources, for example, DS1, becomes inconsistent while other data sources remain consistent. On day 3, the scheduled consistency check runs and the replica is made consistent. Even if no recovery points are created for DS1 from day 1, the recovery points for other data sources sharing the same replica volume are successfully created. Therefore, the recovery point for DS1 is deleted after Day 10.

Retention range for file data

For file data, using the Create New Protection Group Wizard, you can select a retention range between 1 and 64 days for short-term disk-based protection, up to 12 weeks for short-term tape-based protection, and up to 99 years for long-term tape-based protection. DPM can store a maximum of 64 recovery points for each file member of a protection group.

For example, if you select to synchronize before each recovery point, schedule 6 recovery points daily, and set a retention range of 10 days, recovery points for the files in that protection group never exceed 64. However, if you choose a combination of settings that exceeds the limit of 64 recovery points, DPM warns you during the configuration process so that you can modify your selections; you cannot configure a protection configuration for files that exceeds the 64-recovery-point limit.

Retention range for application data

For application servers, you can use the Create New Protection Group Wizard to select a retention range between 1 and 64 days for short-term disk-based protection, up to 12 weeks for short-term tape-based protection, and up to 99 years for long-term tape-based protection.

For example, if you select to synchronize every 15 minutes and you set a retention range of 10 days, those recovery goals result in a protection plan that maintains 960 recovery points for application data in that protection group after the initial 10 days of data protection.

See Also

Modify protection options

What Is a Recovery Point?

Understanding Data Protection

Co-Locating Data

Protection policy

Based on the recovery goals that you specify for a protection group, System Center 2012 – Data Protection Manager (DPM) configures the *protection policy*, or schedule of jobs, for that protection group. The following are examples of recovery goals:

- “Lose no more than 1 hour of production data.”
- “Provide me with a retention range of 30 days.”
- “Make data available for recovery for 7 years.”
- “Tell me when the data on these tapes expires.”
- “I need faster recovery times for applications.”

Your *recovery goals* quantify your organization's data protection requirements. In DPM, the recovery goals are defined by the configuration of retention range, data loss tolerance, and recovery point schedule. DPM provides default settings for the recovery goals; however, you can modify each or all of the settings.

The *retention range* defines how long you need the backed-up data available. For example, do you need data from today to be available a week from now? Two weeks from now? A year from now?

Data loss tolerance is the maximum amount of data loss, measured in time, that is acceptable to business requirements, and it determines how often DPM should synchronize with the protected computer by collecting data changes from the protected computer. You can change the synchronization frequency to any interval between 15 minutes and 24 hours. You can also select to synchronize just before a recovery point is created, rather than on a specified time schedule.

The *recovery point schedule* establishes how many recovery points of this protection group should be created. For file protection, you select the days and times for which you want recovery points created. For application data protection, the synchronization frequency determines the recovery point schedule.

The combination of recovery points, synchronization, and retention range results in a protection plan—that is, a schedule of jobs to achieve your recovery goals.

See Also

New Protection Group Wizard

Protect Data

Express full backup

An express full backup is a type of synchronization in which the protection agent transfers a snapshot of all blocks that have changed since the previous express full backup (also since the most recent consistency check performed or the initial replica creation for the first express full backup) and updates the replica to include the changed blocks. The impact of an express full

backup operation on performance and time is expected to be less than the impact of a full backup because System Center 2012 – Data Protection Manager (DPM) transfers only the blocks changed since the last express full backup.

Note
The express full backup uses DPM filter technology to identify the changed blocks instead of requiring DPM to read all the data or use checksums. This reduces the performance load on the protected computer significantly.

See Also

How DPM Operations Affect Performance

Managing Performance

Auto discovery

Once each day, System Center 2012 – Data Protection Manager (DPM) queries Active Directory Domain Services to discover new computers. This process is referred to as *auto discovery*.

Note
Auto discovery is limited to a DPM server's domain.

DPM lists the new computers next time when you open either the Protection Agent Installation Wizard or the Create New Protection Group Wizard for client computers. To start protecting data on a new computer, install a protection agent on the computer and then add the data sources to a new or existing protection group.

By default, auto discovery runs at 1:00 A.M. each day. You can modify the auto discovery schedule to better accommodate your network traffic flow or other requirements. For more information, see How to Modify the Auto Discovery Schedule.

See Also

Create a protection group

How to Modify the Auto Discovery Schedule

Protection Agent Installation Wizard

Work with replicas

In System Center 2012 – Data Protection Manager (DPM), a *replica* is a complete copy of protected data residing a single volume on the DPM server. A replica is created for each

protected data source after it is added to its protection group. With data co-location, multiple data sources can have their replicas residing on the same replica volume.

As you monitor your data protection activities, you might need to modify synchronization frequency to better accommodate your data change activity, ensure that your replicas are consistent with their data sources, and delete replicas that are no longer needed. Having a replica that represents your live data provides the foundation for being able to both protect your data and recover your data.

In this section

Understand replicas

Synchronization

Consistency check

Synchronize a replica

Delete a replica

How to Manually Create a Replica

See Also

What Is a Recovery Point?

Understand replicas

In System Center 2012 – Data Protection Manager (DPM), a *replica* is a complete copy of protected data residing a single volume on the DPM server. A replica is created for each protected data source after it is added to its protection group. With co-location, multiple data sources can have their replicas residing on the same replica volume. A replica contains all the properties of the volume, including local recovery point settings, security settings, and sharing.

Note
When you protect a data source that contains a mount point, the mount point itself is not replicated; you must manually re-create the mount point when you recover the data.

Before DPM can start protecting the data sources in a protection group, a replica of the data must be created. After a replica is created for each protected volume, changes to the protected data are transferred to DPM incrementally through synchronization, according to a set schedule.

To create a replica on the DPM server, you can have DPM copy the data from the protected computer over the network or you can manually create a replica from a tape backup or other removable storage medium. Replicating the data over the network requires no intervention, but it can take several hours, depending on network bandwidth and the data size. To minimize the impact on network bandwidth, you can schedule replication for a time when network traffic is low.

Note

If you want to replicate the data over a wide area network (WAN), to avoid loading the WAN during work hours, use the network bandwidth usage throttling settings in DPM.

If your data is backed up on tape, you can manually create a replica on the DPM server from the tape. This method does not affect network bandwidth, and it can save time if you are transferring large amounts of data. However, you must manually copy the data to the DPM server and then manually synchronize the replica with a consistency check before scheduled synchronization and recovery point jobs can succeed. For more information, see Synchronize a replica.

See Also

How to Manually Create a Replica

Synchronize a replica

Consistency check

What Is a Recovery Point?

Synchronization

Synchronization

Synchronization is the process by which System Center 2012 – Data Protection Manager (DPM) transfers data changes from a protected computer to a DPM server and then applies the changes to the replica of the protected data. DPM relies on synchronization to keep replicas synchronized with the data on the protected computers.

Synchronization frequency

You can select a synchronization frequency interval of anywhere from 15 minutes to 24 hours. You can also select to synchronize only before a recovery point is created. If you are protecting data that changes frequently throughout the day, you might want to synchronize your data every 15 minutes. If you are protecting data that changes less frequently, you can schedule fewer recovery points and synchronize your data only before each recovery point is made. For more information, see Modify protection options.

Synchronization modes

DPM provides the following methods for synchronizing a replica:

- Incremental synchronization
- Synchronization with consistency check

Incremental synchronization (also referred to as *synchronization*) transfers changes to data from the protected computer to the DPM server and then applies the changes to the replica. When you

create a protection group, you specify a synchronization schedule or accept the default schedule. In general, you can rely on incremental synchronization to keep a replica consistent with its data sources. This method is faster and more efficient than performing a consistency check because it uses the DPM filter to identify the changed blocks.

Synchronization with consistency check (also referred to as a *consistency check*) transfers the data changes from the protected computer to the DPM server but also performs block-by-block verification to ensure that all the data on the replica is consistent with the protected data. This process is slower than synchronization because all the data on the replica is compared rather than simply applying the data changes to the replica.

A consistency check may be required when the DPM cannot track the changes to a protected data source. This can occur if the change journal runs out of disk space or when a protected computer is shut down unexpectedly during synchronization. A consistency check impacts the performance of both the protected computer and the DPM server to varying degrees, depending on network load, CPU processing power, and timing. If you schedule a daily consistency check, you should schedule it when other network traffic is low.

DPM automatically initiates a consistency check as a daily task if you select the option to automatically perform consistency check if the replica is inconsistent or if you have scheduled a daily consistency check for a protection group. DPM will also initiate a consistency check if you create a protection group, stop protection of that group with a "Retain data" option, and then re-protect the same data.

Because of the processing load imposed on both the DPM server and the protected computer, you should perform a manual consistency check only when it is necessary to make a replica consistent with its data sources.

Note

DPM raises an alert if the change journal runs out of disk space or when a protected computer shuts down unexpectedly during synchronization. The alert indicates that the administrator should run a consistency check.

Change journal

A *change journal* is a Windows feature that tracks changes to NTFS volumes, including additions, deletions, and modifications.

The change journal exists on the volume as a sparse file. You can increase but not decrease the allocated disk space for the change journal, as needed. DPM uses the change journal to identify the set of files that have changed since the last synchronization when backing up file servers or client computers.

See Also

Synchronize a replica

Consistency check

What Is a Recovery Point?

Understand replicas

Consistency check

System Center 2012 – Data Protection Manager (DPM) provides two methods for synchronizing a replica: *incremental synchronization* and *synchronization with consistency check*. Synchronization with consistency check, also referred to simply as a *consistency check*, is the process by which DPM checks for and corrects inconsistencies between a protected data source and its replica. As part of the synchronization process, a consistency check performs block-by-block verification to ensure that all the data on the replica is consistent with the protected data. This process is slower than incremental synchronization because all the data on the replica is compared rather than just applying the data changes to the replica.

DPM automatically initiates a consistency check as a daily task if you select the option to automatically perform consistency check if the replica is inconsistent or if you have scheduled a daily consistency check for a protection group.

You may need to perform synchronization with consistency check to repair inconsistencies between the data on the protected computer and the replica on the DPM server. You can configure your protection group to allow DPM to initiate a consistency check as a daily task if you select the option to automatically perform consistency check if the replica is inconsistent. We recommend you to use this option for workloads lesser than 1-terabyte or workloads within a data center

You can also schedule a daily consistency check during off-peak hours to ensure that the replica remains consistent with the protected data. A scheduled consistency check will only run if inconsistencies are detected during synchronization. We recommend you to use this option for large workloads or for data that is backed up over WAN.

If a replica becomes inconsistent because of a change journal overflow or an unexpected shutdown of the protected computer, a consistency check must be performed. You can perform a one-time manual consistency check or, if a daily consistency check is scheduled, you can wait until DPM performs the consistency check. When a consistency check is performed and inconsistencies between the protected volume and the replica volume are found, DPM makes the replica consistent.

Note

The performance of the protected computer and the DPM server will be affected while a consistency check is running. It is best to schedule consistency checks and perform one-time consistency checks during off-peak hours.

See Also

Modify protection options

Synchronize a replica
Synchronization

Synchronize a replica

System Center 2012 – Data Protection Manager (DPM) provides two methods for synchronizing a replica: *incremental synchronization* and *synchronization with consistency check*. Incremental synchronization (also referred to as synchronization) transfers the changes to protected data from the protected computer to the DPM server and then applies the changes to the replica. Synchronization with consistency check transfers the data changes from the protected computer to the DPM server but also performs block-by-block verification to ensure that all the data on the replica is consistent with the protected data.

You might need to manually synchronize a replica in the following situations:

- You can manually synchronize a replica before you create a recovery point to ensure that you are getting the latest possible recovery point. For this purpose, choose incremental synchronization.
- You must perform a manual consistency check when a replica becomes inconsistent due to an overflow of the change journal or an unexpected shutdown of the protected computer. All synchronization and recovery point jobs will fail until the replica is made consistent by performing a consistency check.
- When you manually create a replica from tape or other removable media rather than over the network, you must perform a consistency check before data protection can begin.
- You should manually synchronize a replica when you make configuration changes to a protected computer, such as the following:
  - Adding items to or removing items from a storage group
  - Changing the file location of protected items on a protected computer

For more information about synchronization methods, see Synchronization

To manually synchronize a replica

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the replica that you want to synchronize.
3. In the **Actions** pane, click **Create recovery point - disk**.
4. In the **Create Recovery Point** dialog box, select either **Create a recovery point after synchronizing** or **Only synchronize**. If you select **Only synchronize**, changes since the last synchronization are transferred and applied to the replica.
5. Click **OK**.

See Also

Modify protection options

Consistency check

What Is a Recovery Point?

Understand replicas

Synchronization

Delete a replica

You can delete a replica when you no longer need to be able to recover data for the associated protection group member. The method you use to delete the replica depends on whether the replica is active or inactive. An active replica is one for which the source data is currently being protected.

To delete an active replica

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the protection group member that you want to delete.
3. In the **Actions** pane, click **Stop protection of member**.
4. In the **Remove from Group** dialog box, select whether you want to delete the replica on disk. If recovery points are on tape, select whether you want to expire the recovery points on tape.
5. Click **OK**.

   Note
   When you delete an active replica, you are also deleting all recovery points for the previously protected data and removing the associated member from the protection group. For more information, see Remove protection group members.

To delete an inactive replica

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display pane, select the inactive replica that you want to delete.
3. In the **Actions** pane, click **Remove inactive protection**.
4. In the **Delete Inactive Protection** dialog box, choose to delete the replica on disk. If recovery points are on tape, select whether or not you want to expire the recovery points on tape.

   Note
   Data for the selected inactive protection members is marked for expiration. The tapes are not marked free until all other data marked for expiration has expired.
5. Click **OK**. After you click **OK**, you cannot cancel this action.

   Note
   When you delete an inactive replica, you are also deleting recovery points for the

previously protected data.

Note
For co-located data sources, see Co-Locating Data on Disk.

To remove a replica using DPM Management Shell

- Use the following syntax to remove a replica:

  Remove-DatasourceReplica [-Datasource] <*Datasource*> **[-Disk] [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  Remove-DatasourceReplica [-Datasource] <*Datasource*> **-Tape [- PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Remove-DatasourceReplica -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Remove-DatasourceReplica -full**" in DPM Management Shell.

See Also

Remove protection group members

Synchronize a replica

Understand replicas

Work with replicas

Co-Locating Data

Create a replica manually

During creation of a protection group using the New Protection Group Wizard, System Center 2012 – Data Protection Manager (DPM) asks you to select a replica creation method to copy the data to be protected to the DPM computer. You can select **Automatically**, for which DPM copies the data across the network, or **Manually**. When you select manual replica creation, you must manually copy the data you want protected to the DPM computer using removable media.

To create a replica manually, you must know the details of the source path on the protected computer and the replica path on the DPM server. It is critical that you retain the same directory structure and properties (time stamps and security permissions) as those for the data that you are protecting.

Note

For large amounts of data, manual replica creation might provide faster performance than replication over the network.

To display the details of the source and replica paths

1. In DPM Administrator Console, go to the **Protection** view.
2. Select the data source you want to replicate on the DPM server.
3. Click **View Details** on the tool ribbon. The **Details of Replica Path** dialog box is displayed.
4. Copy the list view content for reference. To copy the replica path, select a row in the **Details of Replica Path** dialog box, and then press CTRL+C.

To copy data files from a protected computer to the DPM server

1. In the **Protection** view, select the protected data and then locate the **Replica path** in the **Details** pane.
2. In the **Details** pane, select the replica path and copy it into a text editor such as Notepad. The path will look like the following:

   <Drive:>\DPM\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\File System\D-87a82ad4-f9d2-11d9-b758-000d561ae74f\e55173e1-0b7a-4fa4-b4d1-387ac2b016b8\3ed60b1c-dcf8-442e-b441-d771a3d7f014\Users

   Note
   You cannot change the directory to this path in Windows Explorer because it is too large.
3. To access the Users folder, perform the following steps:
   a. At the command prompt, type **mountvol** and then press Enter.
   b. From the list of mounted volumes, pick the volume that corresponds to the appropriate path. The path will look like the following:

      \\?\Volume{a2072784-7573-4dce-a7e9-26713fd12697}

      <Drive:>\DPM\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\File System\D-87a82ad4-f9d2-11d9-b758-000d561ae74f
   c. Type the following to mount the volume to a drive letter:

      mountvol k:\ \\?\Volume{a2072784-7573-4dce-a7e9-26713fd12697}
   d. Click **Start**, double-click **My Computer**, and on the **Tools** menu, click **Folder Options**.
   e. In the **Folder Options** dialog box, on the **View** tab, in the **Advanced settings** box, under **Hidden files and folders**, clear the **Hide protected operating system files (Recommended)** option, click **Yes** to confirm that you want to display the files, and then click **OK**.

      Now you can browse to view the entire path from step 3 in Windows Explorer.
4. Manually copy the data to the Users folder under the drive letter you used to map the volume (K:\ in this example). Overwrite any data in the Users folder.

5. After you copy the data to the replica location, perform a synchronization with consistency check. Protection will start after the synchronization with consistency check has successfully completed.
6. At the command prompt, type the following to remove the drive letter that you used to mount the volume:

   mountvol k:\ /d

   Note
   In Windows Server 2008, run the command from an elevated command prompt.

See Also

New Protection Group Wizard

Optimizing Performance

Understand replicas

Manage Protection Agents

Before you can start protecting data, you must install a protection agent on each computer that contains data that you want to protect.

A *protection agent* is software that you install on each of the computers that you want to protect with System Center 2012 – Data Protection Manager (DPM). The protection agent performs the following functions:

- Records changes to protected data in a change journal. The protection agent creates a separate change journal for each protected volume and stores the journal in a hidden file on that volume.
- Transfers the change journal from the protected computer to the DPM server to enable DPM to synchronize the replica.
- Allows the DPM server to browse the shares, volumes, and folders on the protected computer.

A protection agent is controlled exclusively by the DPM server from which it is installed. You cannot assign an installed protection agent to work with a different DPM server.

The protection agent software consists of two components: the protection agent itself and an *agent coordinator*. The agent coordinator is software that is temporarily installed on a protected computer during installation, update, or uninstallation of a protection agent.

In the **Management** task area, you can do the following:

Task	For More Information
Install protection agents	Installing protection agents

Task	For More Information
Update Protection Agents	Updating Protection Agents
Attach Protection Agents	Attaching Protection Agents
Enable and Disable Protection Agents	Enabling and Disabling Protection Agents
Configure Throttle Settings	Configuring Throttle Settings
Remove Protection Agents	Uninstall the protection agent

In this section

Update or check protection agent status

When you click the **Agents** tab in the **Management** task area, agent status is automatically updated. If you are aware of recent protected computer activity that could affect protection agent status, such as restart of a computer after installation of a protection agent or local uninstallation of a protection agent, you can manually update the status of agents to display the latest information.

To update agent status

1. On DPM Administrator Console, go to the **Management** view.
2. Click **Refresh** on the tool ribbon.

   The current agent status, available updates, and agent version are displayed.

To check agent update status

1. In Control Panel on the protected computer, click **Add or Remove Programs**.
2. In **Change or Remove Programs**, click **Microsoft System Center Data Protection Manager 2010 Protection Agent**.
3. Scroll to the protection agent entry. If **Show Updates** is checked, the agent is listed as an update.

Roll back a protection agent

Use the following procedures to install a previous version of the protection agent.

If you experience problems after updating a protection agent, you can roll back to a version that was working before you installed the update. For more information, see Updating Protection Agents. Installing a previous version of the protection agent involves the following steps:

1. Uninstall the updated protection agent from the protected computer.
2. Reinstall the previous protection agent on the protected computer by using the DPM Administrator Console.

Note

Before you uninstall a protection agent from a protected computer, you must remove all of the protection group members from the protected computer. For information about how to remove protection group members, see Remove protection group members.

To uninstall the updated version of the protection agent

1. In DPM Administrator Console, go to the **Management** view, and then open the **Agents** workspace.
2. Click **Refresh information** on the tool ribbon to update agent status.
3. Select the protected computer with the protection agent that you want to uninstall.
4. Click **Uninstall** on the tool ribbon.
5. In the **Uninstall Agents** dialog box, click **Uninstall Agents**.
6. In the **Enter Credentials and Reboot option** dialog box, enter your user name and password, then select a reboot option. Click **OK**.
7. Wait for confirmation that the protection agent was successfully uninstalled.

To reinstall the previous version of the protection agent

1. In DPM Administrator Console, go to the **Management** view, and then open the **Agents** workspace.
2. Click **Refresh information** on the tool ribbon to update agent status.
3. In the display pane, select the computer that you want to roll back.
4. Click **Install** on the tool ribbon.
5. On the **Select Computers** page, click the computers on which you want to reinstall the previous version of a protection agent, then click **Add**.
6. Click **Advanced**.

   Note

   The **Advanced** option is enabled only when more than one version of the protection agent is available for installation on the selected computers. If enabled, you can use this option to roll back to a previous compatible version.

7. In the **Advanced** dialog box, select the previous version that you want to install.

   Note
   If the previous version that you want to install is not displayed, it means that this previous version is not compatible with the currently installed DPM software. To roll back to a previous version that is not displayed, you must first roll back the DPM software.
8. On the **Enter Credentials** page, type the user name and password for a domain account that is a member of the local administrators group on each of the selected computers.
9. On the **Choose Restart Method** page, select the method to use for restarting the computer after the protection agent is installed.

   Important
   Workstations do not require a restart when you install the protection agent. Servers must be restarted before you can start protecting data. This restart is necessary to ensure that the protection agent gets installed correctly. After restart, it might take a few more minutes before DPM can contact the computer because of the time required to start services.
10. On the **Summary** page, click **Install Agents** to proceed with the installation. DPM installs the previous version of the protection agent that you selected.

    A status box is displayed to indicate whether the installation is successful. You cannot close this box until after installation has either succeeded or failed. For information about resolving agent installation failures, see the Troubleshooting.

List computers that have protection agent installed

Use the following procedures to list computers that have a protection agent installed.

To list computers that have a protection agent installed

- In DPM Administrator Console, go to the **Management** view, and then open the **Agents** workspace.

  The display lists the agent licenses purchased, agents in use, and agent status for each computer.

To list computers that have a protection agent installed using DPM Management Shell

- Use the following syntax to list the computers that have a protection agent installed:

  Get-ProductionServer [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-**

OutBuffer <*Int32*>**]**

For more information, type "**Get-Help Get-ProductionServer -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Get-ProductionServer -full**" in DPM Management Shell.

Uninstall the protection agent

The primary reason to uninstall a protection agent is to stop protecting data on a computer. You can uninstall a protection agent by using DPM Administrator Console or by uninstalling it locally on the protected computer. However, we recommend that you uninstall a protection agent by using DPM Administrator Console whenever possible. If you uninstall an agent locally on the protected computer, you might get irrelevant “Unable to connect” alerts. And, uninstalling a protection agent by using DPM Administrator Console automatically removes the computer from the **Agents** view.

Uninstalling a protection agent by using DPM Administrator Console involves three steps. Following this process ensures that System Center 2012 – Data Protection Manager (DPM) monitors only currently protected computers and is not using disk space to store replicas and recovery points that you no longer need:

1. Remove all protection group members associated with the protected computer.
2. Uninstall the protection agent from the protected computer.
3. Restart the protected computer.

Note

The user has the choice to auto-reboot the protected computer.

You can also uninstall a protection agent locally from a protected computer. You might need to use this procedure if you cannot access a protection agent in DPM Administrator Console.

To remove protection group members associated with a protected computer

1. In DPM Administrator Console, go to the **Protection** view.
2. In the **Group by** options, select **Computer**.
3. Remove all protected data sources associated with the computer.

   Note

   When you remove the last member of a protection group, the group is automatically removed from DPM.

To uninstall a protection agent by using DPM Administrator Console

1. In DPM Administrator Console, go to the **Management** view.

2. On the **Agents** workspace, select the computer from which you want to uninstall the protection agent.
3. On the tool ribbon, click **Uninstall**.
4. In the **Uninstall Agents** dialog box, click **Uninstall Agents**, and then click **Next**.
5. In the **Enter Credentials** dialog box, type the user name, password, and domain for an account that is a member of the local Administrators group on all selected computers, and then click **OK**.
6. Choose whether you want to automatically restart the computer or whether you want to manually restart the computer after the protection agent has been uninstalled.

   A status box is displayed to indicate whether the uninstallation is successful. You cannot close this box until after uninstallation has either succeeded or failed. For information about resolving agent installation failures, see Troubleshooting.

To uninstall a protection agent locally

1. In Control Panel, click **Add or Remove Programs**.
2. In **Change or Remove Programs**, click **Microsoft System Center Data Protection Manager Protection Agent**, and then click **Remove**.
3. Reboot the computer after the protection agent has been uninstalled.

   Note
   When you locally uninstall a protection agent from a computer, DPM Administrator Console continues to list the computer on the **Agents** workspace, with a status of **Error**.

To uninstall a protection agent locally from the command prompt

1. For a 32-bit operating system, at the command prompt type
   Msiexec /x {07CCDE6A-1D92-2C9C-D091-9E682643ABCC}
2. For 64-bit operating system, at the command prompt type
   Msiexec /x {72BF00D8-53E0-1539-F523-4347082BCC11}

   Note
   In Windows 2008 Server and Windows Vista, run the command from an elevated command prompt.

To uninstall a protection agent silently from the command prompt

1. For 32-bit operating system, at the command prompt type
   Msiexec /x {07CCDE6A-1D92-2C9C-D091-9E682643ABCC} /qn /REBOOT=ReallySupress

   For 64-bit operating system, at the command prompt type
   Msiexec /x {72BF00D8-53E0-1539-F523-4347082BCC11} /qn /REBOOT=ReallySupress

   Note

In Windows 2008 Server and Windows Vista, run the command from an elevated command prompt.

See Also

Remove protection group members

Manage Protection Agents

What Is a Protection Agent?

Troubleshoot protection agents

Before you start troubleshooting System Center 2012 – Data Protection Manager (DPM), consider whether any of the following blocking issues might apply to your situation. For more information about resolving issues with agents, see Troubleshooting DPM Installation.

DPM protection agent will not install on a computer

- Is the computer connected to the network and can it be remotely accessed from the DPM server?

  Both the DPM server and the computer to be protected must be connected to the network during installation of a protection agent.
- Does the protected computer have a supported Windows operating system installed?

  Verify the operating system on the computer to be protected.
- Is a firewall enabled on the computer to be protected that could be blocking requests from the DPM server?

  If a firewall is enabled, you need to configure the firewall to allow communication between the DPM server and the computer to be protected. For information about configuring the firewall, see Configuring Windows Firewall on the DPM Server
- Is a firewall enabled on the DPM server?

  If a firewall is enabled, you need to configure the firewall to allow installation of a protection agent on the computer.
- Has a previous version of the protection agent already been installed on the protected computer?

  You cannot install two versions of the protected agent on the same protected computer.
- Is the Remote Registry service running on the computer to be protected?

  The Remote Registry service must be running on both the DPM server and the computer before you can install a protection agent. In Administrative Tools, start the Remote Registry service and then install the protection agent.

- Is Remote Procedure Call (RPC) unavailable?

  RPC must be available. See Microsoft Knowledge Base article 555839, Troubleshooting RPC Server is Unavailable in Windows.
- Is the boot volume on the computer formatted as file allocation table (FAT)?

  Convert the boot volume to NTFS file system if you have sufficient space.

DPM protection agent will not uninstall from a computer

- Is the protected computer disconnected from the network?

  To uninstall a protection agent, the protected computer must be connected to the network.
- Was the protected computer renamed or moved to another Active Directory domain after the protection agent was installed?

  To uninstall a protection agent, the protected computer must have the same name and be in the same domain as it was when the protection agent was installed.

  Uninstall the agent locally, and then remove the entry from DPM Administrator Console.

DPM protection agent is incompatible with DPM or other software

- Did you upgrade the DPM software without updating the protection agent?

  To determine whether an agent update is available, check the **Agents** tab in the **Management** view.
- Did you upgrade a protection agent by using Microsoft Update before DPM received the corresponding server update?

  Because Microsoft Update can occur automatically, ensure that the protection agent and DPM are compatible.

An error occurred when the agent operation attempted to communicate with the DPM Agent Coordinator service on the specified computer

- Did you check the COM permissions?

  Verify COM permissions on the protected computer. See Troubleshooting Protection Agent Installation.

Recover Data

Loss of data is an unfortunate, perhaps even disastrous, event for any organization. System Center 2012 – Data Protection Manager (DPM) helps mitigate such losses by providing you with search and browse features that help you find the data that you need to recover. After you find the data, you can recover the version you find or you can display a list of all available versions so that you can select a specific version to recover. This data can be files, applications, or data from computers running SQL Server, Windows SharePoint Services, or Exchange Server. In addition, DPM supports protection and recovery of desktop computers and virtual servers.

It takes only a few minutes to find data, select a version, and start a recovery job or recovery collection (multiple jobs). Depending on the size of data being recovered, the job can take less than a minute or it could take hours. You can check the status of recovery jobs in the **Monitoring** task area.

In this section

Recover data

In System Center 2012 – Data Protection Manager (DPM), use the Recovery Wizard to recover data. When you recover data, you can use default settings or you can modify recovery options to specify the recovery location and security settings for the recovered data. To minimize the time required for recovery operations and to decrease the size of data being transferred, DPM uses on-the-wire compression for all recovery operations.

How to recover data

1. In DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for the data you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold dates for the recovery points you want to recover.
4. In the **Recoverable item** pane, click to select the item you want to recover.
5. Click **Recover** or **Show all recovery points**. DPM starts the Recovery Wizard.
6. Review your recovery selections, and click **Next**.
7. Specify the type of recovery you would like to perform, and click **Next**.
8. Specify your recovery options, and click **Next**.
9. Review your recovery settings, and click **Recover**.

How to Find Recoverable Data

You can easily and quickly recover data from the recovery points stored on the server for System Center 2012 – Data Protection Manager (DPM). To find your data, browse through the recovery points of protected data sources or search to locate the specific files that you want to recover. After you find the data that you want to recover, you can choose the version that you want to recover.

In this section

How to Browse for Recoverable Data

How to Search for Recoverable Data

How to Browse for Recoverable Data

Recovery points of protected data contain the same folder and file structures as the data sources, making it easy to browse to the data you want to recover. You can browse through the recovery points of each replica to find copies of the protected data. The **Browse** view displays the protected data as follows:

- Files: By volumes
- SQL Server: By SQL instance
- Exchange Server: By Exchange application name
- Windows SharePoint Services: By farms

The following tree elements are shown in the order of their appearance:

- **Domain name**. Multiple domain names can be shown.

- **Protected Computer name**. The name of the protected computer.
- **System state**. Clicking on system state shows system files that can be recovered. All files will be recovered together. Clicking on any one of them selects all.
- **Protected Exchange Servers**. Clicking on the database displays all mailboxes in the list view.
- **Protected SQL Servers**. The SQL instances are displayed. Clicking on a SQL instance displays the recoverable databases.
- **All protected shares**. DPM displays all protected shares that can be recovered.
- **All protected volumes**. DPM displays all protected volumes that can be recovered.

For Exchange Server mailbox recovery, if you select **Previous point in time** on the **Browse** tab, you must select the database from the **Protected data** pane to display recoverable items correctly. If you select **Latest**, DPM returns the following error message and then starts the Recovery Wizard:

"You have chosen to recover 'Latest'' recovery time. For the selected mailbox, the 'Latest' recover time is <time>. For mailbox recovery, the 'Latest' does not apply unsynchronized logs from the protected Exchange server."

To browse for recoverable data

1. In DPM Administrator Console, go to the **Recovery** view.
2. Browse to select computers, folders, and subfolders until you find the data you are looking for.
   a. As you select nodes in the browse pane on the left, the names of the folders and files in that node are displayed in the **Recoverable item** pane.
   b. If you protected shares, you can browse the recovery points in either **All Protected Shares** or **All Protected Volumes**. If you protected volumes, you can browse only for recovery points in **All Protected Volumes**.

To browse for recoverable data using DPM Management Shell

- Use the following syntax to browse for recoverable data:

  Get-RecoverableItem [-RecoverableItem] <*RecoverableObject*> **[-BrowseType]** <*BrowseType*> **[-Async] [-Tag** <*Object*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Get-RecoverableItem -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Get-RecoverableItem -full**" in DPM Management Shell.

See Also

How to Search for Recoverable Data

How to Search for Recoverable Data

You can use System Center 2012 – Data Protection Manager (DPM) to search for copies of protected data by network share or by computer, volume, and path. You can further refine your search by including or excluding subfolders, specifying all or part of a folder or file name, and specifying a range of recovery point times to include in the search.

To search for recoverable data

1. In DPM Administrator Console, go to the **Recovery** view.
2. Select the types of data to search:
   a. Files, including multiple files
   b. Exchange mailboxes
   c. SharePoint sites and documents
3. If you want to find data by using a search string, specify the search string in the **File or folder name** pull-down menu. Selections include the following:
   a. Contains
   b. Exact match
   c. Starts with
   d. Ends with
4. If you want to search by recovery point, in the **Recovery Point Range** pane, use the pull-down calendars to select the search dates.
5. Select the location of the data source you want to search, either **Network (UNC) path** or **Local path on computer**. If you have protected shares, you can search either by network share or by volume. If you have protected volumes, you can search only by volume.
   a. If you select **Network (UNC) path**, type the computer and share name. When performing a search for recoverable data by using a network path, the search results display the local path of the data on the computer, not the network (UNC) path.
   b. If you select **Local path on computer**, in the first box, type the full path that you want to include in your search. For example, **F:\Critical Data\November**. In the drop-down list, select the computer that you want to include in the search.
6. To define additional criteria for your search, check **Search subfolders** if it is not already checked.
7. After you have specified all your search criteria, click **Search**.

   Note
   A maximum of 250 items can be displayed in the results pane. If your search criteria are too broad, you might see a warning message stating that your search

returned more than 250 items. Use the search controls to further refine your search, and then run your search again.

To search for recoverable data using DPM Management Shell

- Use the following syntax to search for recoverable data:

  Get-RecoverableItem [-Datasource] <*Datasource*> **[-SearchOption]** <*SearchSpecifications*> **[-Async] [-Tag** <*Object*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Get-RecoverableItem -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Get-RecoverableItem -full**" in DPM Management Shell.

To create a new search option using DPM Management Shell

- Use the following syntax to create a new search option:

  New-SearchOption [-FromRecoveryPoint] <*DateTime*> **[-ToRecoveryPoint]** <*DateTime*> **[-SearchDetail]** <*SearchForDetail*> **[-SearchType]** <*SearchFilterType*> **[-SearchString]** <*String*> **[-Location** <*String*>**] [-Recursive] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help New-SearchOption -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help New-SearchOption -full**" in DPM Management Shell.

See Also

How to Browse for Recoverable Data

How to Show All Recovery Points

Working with Recovery Points

System Center 2012 – Data Protection Manager (DPM) relies on recovery point technology to allow you to recover your data. A *recovery point*, also referred to as a snapshot, is a point-in-time copy of the files and folders that are protected by the DPM server.

A *recovery point*, also referred to as a *snapshot*, is a point-in-time copy of a replica stored on the server for System Center 2012 – Data Protection Manager (DPM). A *replica* is a complete point-

in-time copy of the protected shares, folders, and files for a single volume on a protected computer.

To start data protection, a full replica of the selected data must be copied to the allocated replica volume on the DPM server.

Note
With data co-location the allocated replica volume will be shared by other data sources to include their replicas.

Thereafter, the replica is periodically synchronized with changes to the protected data. DPM creates recovery points of each replica in a protection group according to a specified schedule. You can access the recovery points to recover previous versions of files in the event of data loss or corruption. You can recover data, and you can also configure end-user recovery so that users can recover their own data.

When you select recovery point times, DPM provides you with estimates for recovery range and maximum data loss. These estimates can help you specify a recovery point schedule that provides adequate data protection and meets your recovery goals. A maximum of eight recovery points can be scheduled per day.

In the **Recovery** task area, you can access recovery points to recover previous versions of files in the event of data loss or corruption. DPM administrators can recover data, or they can configure end-user recovery so that end users can independently recover their own data.

In the **Protection** task area, you can manually create an immediate recovery point to disk or tape. You can also modify the protection options for a protection group to specify when and how often to create recovery points.

Note
You can delete a recovery point only by using DPM Management Shell. You cannot delete a recovery point using DPM Administrator Console.

In this section

How to Create a Recovery Point

As part of the data protection process, System Center 2012 – Data Protection Manager (DPM) creates recovery points, as scheduled, of each replica in a protection group. You establish the recovery point schedule when you create a protection group or when you modify the protection

options for an existing protection group. You can access the recovery points on the DPM server to recover previous versions of data.

Occasionally, you might need to create a manual recovery point. For example, you could create a manual recovery point if you need to recover data and you want to ensure that you are using the latest possible recovery point.

The following options are available when you select **Create recovery point -disk** for file data:

- **Create a recovery point after synchronizing**
- **Create a recovery point without synchronization**
- **Only synchronize (available only for file data)**

The following options are available when you select **Create recovery point - disk** for application data or system state:

- **Create a recovery point using express full backup**
- **Create a recovery point using incremental backup**

If the selected application data does not support incremental backup, the **Create a recovery point using incremental backup** option is disabled.

To create a recovery point from the Protection task area

1. In DPM Administrator Console, go to the **Protection** view.
2. Select the protected volume or share for which you want to create a recovery point.
3. Click **Create recovery point - disk** or **Create recovery point - tape**.
4. In the **Create Recovery Point** dialog box, select one of the available options. The available options depend on the type of data selected and whether the recovery point will be created on disk or tape.

   The new recovery point is displayed in the recovery point list.

To create a recovery point using DPM Management Shell

- Use the following syntax to create a new recovery point for application data on disk:

  New-RecoveryPoint [-Datasource] <*Datasource[]*> **-Disk [-BackupType** <*BackupType*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to create a new recovery point for file data on disk:

  New-RecoveryPoint [-Datasource] <*Datasource[]*> **-Disk -DiskRecoveryPointOption** <*CreateDiskRecoveryPointOption*> **[-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to create a new recovery point on tape:

  New-RecoveryPoint [-Datasource] <*Datasource[]*> **-Tape -ProtectionType**

<*ProtectionType*> **[-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

For more information, type "**Get-Help New-RecoveryPoint -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help New-RecoveryPoint -full**" in DPM Management Shell.

How to Show All Recovery Points

You can use the following procedure in System Center 2012 – Data Protection Manager (DPM) to display a list of all available versions for a selected recovery point, select the version that you want to recover, and then recover the data.

Note
Recovery jobs take priority over synchronization jobs. If a synchronization job is running or is scheduled to start while a recovery job is running, the synchronization job will be canceled. The next scheduled synchronization job will run as scheduled.

To show all recovery points

1. In DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for any version of the data that you want to recover, and then select the data.
3. In the **Recovery time** field, select a recovery time from the drop-down menu.
4. In the **Recoverable item** pane, click the item you wish to recover.
5. Click **Show all recovery points**.
6. In the **All versions** dialog box, select the data that you want to recover and then click **Recover**.

   This opens the **Recovery Wizard** and starts the recovery job. Click **Help** if you need assistance. Click **Close** when the recovery is complete.

To show all recovery points using DPM Management Shell

- Use the following syntax to retrieve all recovery points:

  Get-RecoveryPoint [-Datasource] <*Datasource*> **[-Async] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]Get-RecoveryPoint [-Tape]** <*Media*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-**

OutBuffer <*Int32*>**]**

For more information, type "**Get-Help Get-RecoveryPoint -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Get-RecoveryPoint -full**" in DPM Management Shell.

See Also

How to Browse for Recoverable Data

How to Search for Recoverable Data

Recover data

How to Modify a Recovery Point Schedule

You can use the following procedure to modify the time and days of the week when System Center 2012 – Data Protection Manager (DPM) creates recovery points for a protection group.

To modify a recovery point schedule

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, select the protection group for which you want to modify the recovery point schedule.
3. Click **Modify protection group**. This starts the Modify Group Wizard.
4. Select the group members for the protection group, and click **OK**.
5. Select the data protection method, and click **OK**.
6. On the **Short-Term Goals** screen, in the **File Recovery Points** pane, click **Modify**.
7. Specify a new time, date, and days of the week for the recovery points, and click **OK**.
8. Click **Next**, and then click **Update Group**.

See Also

How to Create a Recovery Point

What Is a Recovery Point?

How to Delete a Recovery Point

You can delete a recovery point for a protection group only by using DPM Management Shell.

Important

In data co-location, as multiple data sources can have their replicas residing on the same replica volume, deleting a recovery point of one data source may delete the recovery point of other data sources. For more information, see Co-Locating Data on Disk.

To delete a recovery point

1. Use the following syntax to retrieve the location of a recovery point:

   Get-RecoveryPointLocation [-RecoveryPoint] <*RecoverySource*>**[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

   For more information, type "**Get-Help Get-RecoveryPointLocation -detailed**" in DPM Management Shell.

   For technical information, type "**Get-Help Get-RecoveryPointLocation -full**" in DPM Management Shell.

2. Use the following syntax to delete the recovery point:

   Remove-RecoveryPoint [-RecoveryPoint] <*RecoverySource*> **[-ForceDeletion] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**] [-WhatIf] [-Confirm]**

   For more information, type "**Get-Help Remove-RecoveryPoint -detailed**" in DPM Management Shell.

   For technical information, type "**Get-Help Remove-RecoveryPoint -full**" in DPM Management Shell.

See Also

Working with Recovery Points

Co-Locating Data

How to Recover Data for File Servers

System Center 2012 – Data Protection Manager (DPM) supports recovery of data for file servers through the Recovery Wizard. When you double-click a protected volume on the **Protected data** pane in the wizard, DPM displays the data that belongs to that volume in the results pane. You can filter protected server names alphabetically by clicking **Filter**. After selecting a data source to recover in the tree view, you can select a specific recovery point by clicking the bold dates in the calendar. When you click **Recover** in the **Actions** pane, DPM starts the recovery job.

To recover protected data for file servers

1. In DPM Administrator Console, go to the **Recovery** view.

2. Browse or search for the data you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
5. Click **Recover** on the tool ribbon. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.
7. Specify the type of recovery you would like to perform:
   a. **Recover to the original location**.
   b. **Recover to an alternate location**. Type the alternate location, or click **Browse** and then, on the **Specify Alternate Recovery Destination** dialog box, select a recovery location. Click **OK**.
   c. **Copy to tape**. This option copies the volume that contains the selected data to a tape in a DPM library. When you select this option, click **Next** and, on the **Specify library** screen, select library details and tape options. You can compress or encrypt data on this screen.
8. After you have specified the type of recovery, click **Next**.
9. Specify your recovery options:
   a. **Existing version recovery behavior**. This option appears only if you selected **Recover to original location** in step 7. Select **Create copy**, **Skip**, or **Overwrite**.
   b. **Restore security**. This option appears only if you selected **Recover to the original location** or **Recover to an alternate location** in step 7. Select **Apply security settings of the destination computer** or **Apply the security settings of the recovery point version**.
   c. **Network bandwidth usage throttling**. Click **Modify** to enable throttling and to select **Settings** and **Work Schedule**, and then click **OK**.
   d. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients. Separate the e-mail addresses with commas.
10. After you have specified the recovery option, click **Next**.
11. Review your recovery settings, and click **Recover**.

Note

Any synchronization job for the selected recovery item is canceled while the recovery is in progress.

To set recovery options for file servers using DPM Management Shell

- Use the following syntax to set recovery options for file data:

  New-RecoveryOption [-TargetServer] <*String*> **[-RecoveryLocation]** <*RecoveryLocation*> **[-DPMLibrary** <*Library*>**] [-RecoverToReplicaFromTape] [-SANRecovery] -FileSystem [-AlternateLocation** <*String*>**] -OverwriteType** <*OverwriteType*> **[-RestoreSecurity] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer**

<*Int32*>**]**

For more information, type "**Get-Help New-RecoveryOption -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help New-RecoveryOption -full**" in DPM Management Shell.

To recover protected data for file servers using DPM Management Shell

- Use the following syntax to recover data for a file server:

  Recover-RecoverableItem [-RecoverableItem] <*RecoverableObject[]*> **[-RecoveryOption]** <*RecoveryOptions*> **[-RecoveryPointLocation** <*RecoverySourceLocation[]*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-RecoveryNotification** <*Nullable`1*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Recover-RecoverableItem -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Recover-RecoverableItem -full**" in DPM Management Shell.

See Also

Recover Data

Recovery Wizard

Understanding Data Recovery[new]

How to Recover Data for Exchange-Based Servers

System Center 2012 – Data Protection Manager (DPM) supports recovery of Exchange Server mailboxes through the Recovery Wizard. When you click an Exchange Server database in the **Protected data** pane in the wizard, DPM displays the mailboxes that belong to that database.

When you select the Exchange Server database to recover, DPM displays the date that the last express full backup was performed. In the results pane, DPM displays the attribute of mailboxes: alias. The results are sorted by display name as a default.

Note

When you recover Exchange storage groups or Exchange databases and the recovery point specified is an incremental recovery point, DPM also recovers the Exchange log files.

Mailbox information—how many mailboxes are present in the database for the selected recovery point—is updated per the express full backup deifies schedule for the protection group.

You can also use Outlook to recover an item that was deleted from an Exchange mailbox.

To recover protected data from an Exchange-based server

1. In the DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for the data you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
5. Click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.

   Note
   If the user of the mailbox you are trying to recover has an active mailbox, you can recover only a previous version of the mailbox.
7. Specify the type of recovery you would like to perform:
   a. **Recover to Exchange Server location**. This option is available only if the latest available recovery point is selected.
   b. **Copy to a network folder.** Click **Next** and then, on the **Specify Destination** dialog box, click **Browse** to select a recovery location. Click **Next**.
   c. **Copy to tape**. This option copies the storage group to tape in a DPM library. When you select this option, click **Next** and, on the **Specify Library** screen, select library details and tape options. You can compress or encrypt data on this screen.
8. After you have specified the type of recovery, click **Next**.
9. Specify your recovery options:
   a. **Mount the databases after they are recovered**. Clear the check box if you do not wish to mount the databases.
   b. **Network bandwidth usage throttling**. Click **Modify** to enable throttling.
   c. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients. Separate the e-mail addresses with commas.
10. Click **Next**.
11. Review your recovery settings, and click **Recover**.

    Note
    Any synchronization job for the selected recovery item is canceled while the recovery is in progress.

To set recovery options for Microsoft Exchange-based servers using DPM Management Shell

- Use the following syntax to set recovery options for an Exchange-based server:

  New-RecoveryOption [-TargetServer] <*String*> **[-RecoveryLocation]** <*RecoveryLocation*> **[-DPMLibrary** <*Library*>**] [-RecoverToReplicaFromTape] [-SANRecovery] [-RestoreSecurity] -RecoveryType** <*RecoveryType*> **[-RollForwardRecovery] [-TargetLocation** <*String*>**] -Exchange [-AlternateDatabase** <*String*>**] [-AlternateStorageGroup** <*String*>**] [-IsRecoveryStorageGroup] [-MountDatabaseAfterRestore] -ExchangeOperationType** <*ExchangeOperationType*> **[-MailboxDisplayName** <*String*>**] [-DatabaseName** <*String*>**] [-StorageGroupName** <*String*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help New-RecoveryOption -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help New-RecoveryOption -full**" in DPM Management Shell.

To recover protected data from Microsoft Exchange using DPM Management Shell

- Use the following syntax to recover data from a file server:

  Recover-RecoverableItem [-RecoverableItem] <*RecoverableObject[]*> **[-RecoveryOption]** <*RecoveryOptions*> **[-RecoveryPointLocation** <*RecoverySourceLocation[]*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-RecoveryNotification** <*Nullable`1*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Recover-RecoverableItem -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Recover-RecoverableItem -full**" in DPM Management Shell.

See Also

How to Recover a Mailbox

Recovery Wizard

Synchronization

How to Recover a Mailbox

In Exchange Server, the Recovery Storage Group (RSG) feature gives the Exchange administrator the option of mounting a second copy of a mailbox database, typically a mailbox database restored from backup. This allows the administrator to extract data from one or more

mailboxes in the respective database without affecting the production databases during working hours.

In Microsoft Exchange Server 2003, you create an RSG using the Exchange Management Console (EMC). With Exchange Server 2007 and Exchange Server 2010 you create an RSG using the Exchange Troubleshooting Assistant (ExTRA). Use the Database Recovery Management Tool to launch ExTRA. You can find the Database Recovery Management Tool in the Exchange Toolbox work center or by using the Exchange Management Shell (EMS).

Note

To recover an Exchange Server 2007 mailbox, the recovery destination must have Exchange Server 2007 installed. To recover an Exchange Server 2003 mailbox, the recovery destination must have Exchange Server 2003 installed.

When mounting a copy of an Exchange Server 2003 mailbox database to an RSG, you can extract the data from a mailbox and then merge the data with another mailbox located in a mailbox database in a storage group, but you can also extract the data and then copy it to a specific folder in another mailbox.

Note

If you are recovering an Exchange Server 2003 mailbox that is active, the **Recover mailbox to an Exchange server database** option is disabled. You must recover the Exchange database files to share on an Exchange server and select the **Bring the database to a clean shut down state after copying the files** check box. Then mount the database to a RSG manually using Exchange Management Console.

To recover a previous version of a mailbox

1. In the DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for the data you want to recover, and then, in the results pane, select the data. If you select **Previous point in time**, you must select the database from the **Protected data** pane to display recoverable items correctly.

   Note

   Only one mailbox can be selected and recovered at a time, and you can search for data by alias, display name, and date range.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the mailbox you want to recover.
5. Click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.
7. Specify the type of recovery you would like to perform:
   a. **Recover mailbox to an Exchange server database**. Type the target server running Exchange, or browse for the path. After the recovery, the recovered mailbox must be connected to a user account using Exchange System Manager.

b. **Copy to a network folder**. Choose the network folder where all database files containing the mailbox will be copied.

Note
The **Copy to Tape** option is disabled if there is no tape drive.

Click **Next** after you have specified the recovery type.

8. If you specified **Copy to a network folder**, on the **Select Recovery Options** page, select the **Bring the database to a clean shut down state after copying the files** check box.
9. Select whether you want to send an e-mail notification to recipients when the recovery is complete.
10. On the **Recovery Destination** page, specify the Exchange server name, the storage group name, and the database name. You can also click **Browse** to search for a recovery destination.

Note
If you recover to an Exchange 2007 server or if you recover an Exchange Server 2007 mailbox, the recovery destination should be a recovery storage group (RSG). If you recover an Exchange Server 2003 mailbox that is online, you must provide an Exchange Server 2003 RSG. If the mailbox is offline, you must specify a storage group that is not a RSG. After DPM has recovered the database files, connect the mailbox to an Active Directory account using Exchange Management Console.

11. Click **Next**.
12. On the **Set Notification** page, select **Send an e-mail when this recovery completes** check box if you want to notify others about the recovery job, and then type the e-mail recipients' names. Separate the e-mail addresses with commas.
13. Click **Next.**
14. Review your recovery settings, and click **Recover**.

Note
Any synchronization job for the selected recovery server will be canceled while the recovery is in progress.

To extract data from a mailbox and merge it with another mailbox

- For Exchange Server 2003, use the Microsoft Exchange Server Mailbox Merge Wizard (ExMerge).
- For Exchange Server 2003 SP1, extract and merge data using the Exchange Server 2003 System Manager GUI.

See Also

How to Find Recoverable Data

How to Recover Data for Exchange-Based Servers
Recovery Wizard
Synchronization

How to Recover Data for SQL Servers

System Center 2012 – Data Protection Manager (DPM) supports recovery of SQL Server databases at the instance level through the DPM Recovery Wizard. You can use the following procedure to recover data for computers running SQL Server.

Important
If you migrated from SQL Server 2000 to SQL Server 2005, if the SQL Server 2000 data was being protected by DPM, and if you restored data from the SQL Server 2000 recovery point to the SQL Server 2005 original location, you must run a consistency check immedately after the recovery is completed.

To recover protected data for computers running SQL Server

1. In DPM Administrator Console, go to the **Recovery** view.
2. Select a SQL instance to view recoverable SQL Server databases. If the database is not part of a protection group, the calendar is disabled, and the database data is not available for recovery, DPM displays the message **No recovery points are available for the items below because they do not belong to any protection group**.
3. Browse or search for the data you want to recover, and then, in the results pane, select the data.
4. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the date for the recovery points you want to recover, and then select the time in the **Recovery time** drop-down menu. If you intend to rename and recover the database, do not select **Latest** for the recovery time.
5. Click to select the recoverable item you want to recover.
6. Click **Recover**. DPM starts the Recovery Wizard.
7. Review your recovery selection, and click **Next**.
8. Specify the type of recovery you would like to perform:
   a. **Recovery to original instance of SQL Server**. The current database files will be overwritten during recovery.
   b. **Rename and recover the database**. This option allows you to keep both the existing database and the recovered database in the original instance of SQL Server. You can specify a new name for the recovered database.

      Note
      You can rename and recover the database only for SQL Server 2005 databases, not for SQL Server 2000 databases.

c. **Copy to a network folder**. Click **Browse**, and select the network folder from the list.

d. **Copy to tape**. This option copies the selected backup of the database to a tape in a DPM library so that you have a copy of the database backup. Click **Next**, and specify library and tape options. You can also choose to encrypt or compress data.

Click **Next** after you specified one of the preceding options.

9. Specify the database state:
   a. **Recover database**. This option performs full recovery and leaves the database ready to use.
   b. **Recover and leave database in restoring state**. This option recovers the database but leaves it non-operational.
10. If logs are available for the selected database, you can copy SQL transaction logs between the selected database and the latest database available for recovery. This option is disabled if there are no logs available for the selected database. To copy SQL transaction logs between the selected version of the database and the latest version available for recovery, in the **Database in restoring state option** pane, click **Copy SQL transaction logs between the selected and latest available recovery**.
11. Specify recovery options for network bandwidth usage throttling and e-mail notifications, and click **Next**.
12. Review your recovery settings, and click **Recover**.

Note

Any synchronization job for the selected recovery item is canceled while the recovery is in progress.

To set recovery options for a SQL Server database by using DPM Management Shell

- Use the following syntax to set recovery options for a SQL server:

  New-RecoveryOption [-TargetServer] <*String*> **[-RecoveryLocation]** <*RecoveryLocation*> **[-DPMLibrary** <*Library*>**] [-RecoverToReplicaFromTape] [-SANRecovery] [-RestoreSecurity] -SQL -RecoveryType** <*RecoveryType*> **[-RollForwardRecovery] [-TargetLocation** <*String*>**] [-AlternateDatabaseDetails** <*AlternateDatabaseDetailsType*>**] [-LeaveDBInRestoringState] [-CopyLogFiles] [-LogFileCopyLocation** <*String*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help New-RecoveryOption -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help New-RecoveryOption -full**" in DPM Management Shell.

To recover protected data for a SQL Server database by using DPM Management Shell

- Use the following syntax to recover data for a SQL server:

Recover-RecoverableItem [-RecoverableItem] <*RecoverableObject[]*> **[-RecoveryOption]** <*RecoveryOptions*> **[-RecoveryPointLocation** <*RecoverySourceLocation[]*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-RecoveryNotification** <*Nullable`1*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

For more information, type "**Get-Help Recover-RecoverableItem -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Recover-RecoverableItem -full**" in DPM Management Shell.

See Also

How to Enable Computer-Level Network Bandwidth Usage Throttling

Recover Data

How to Recover Data for Virtual Machines

When you add a virtual machine to a protection group in System Center 2012 – Data Protection Manager (DPM), you are protecting the complete configuration of the virtual machine, including operating system, applications, and application data. However, you cannot directly recover application data from the recovery points for the virtual machine; you can recover only the entire virtual machine.

To recover application data only for applications running in virtual machines, you must select the application data explicitly as a protection group member. You must have a protection agent installed on the guest operating system.

To recover data for virtual machines

1. In DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for the virtual machine name you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
5. Click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.
7. Specify the type of recovery you would like to perform:
   a. **Recover to original instance**. The current files will be overwritten during recovery.
   b. **Recover to a network folder**. Click **Next**, and on the **Specify Destination** dialog

box, click **Browse** to browse for a folder where you want to copy the database files.

c. **Copy to tape**. Click **Next**, and on the **Specify Library** dialog box, select library details and tape options for the recovery. You can also choose to compress or encrypt the data on tape.

8. Click **Next** after you have specified one of the preceding options.
9. Specify your recovery options:
   a. Select **Apply security settings of the destination computer** or **Apply the security settings of the recovery point version**. This option is enabled only if you chose **Recover to a network folder** in step 7.
   b. **Enable SAN-based recovery using hardware snapshots**. Select this option to use SAN-based hardware snapshots for quicker recovery.

      This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.
   c. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
10. Click **Next** after you have specified your recovery options.
11. Review your recovery settings, and click **Recover**.

Note

Any synchronization job for the selected recovery item will be canceled while the recovery is in progress.

See Also

Recover Data

Recovery Wizard

Working with Recovery Points

How to Recover Data for Desktop Computers

System Center 2012 – Data Protection Manager (DPM) supports recovery of data for desktop computers through the Recovery Wizard. When you double-click a protected volume or share on the **Protected data** pane in the wizard, DPM displays the data that belongs to that volume or share in the results pane. You can filter protected computers names by alphabet by clicking **Filter**.

To recover protected data for desktop computers

1. In DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for the data you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
5. Click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.
7. Specify the type of recovery you would like to perform:
   a. **Recover to the original location**.
   b. **Recover to an alternate location**. Click **Browse** to browse for an alternate recovery destination. On the **Specify Alternate Recovery Destination** dialog box, select the recovery destination and click **OK**.
   c. **Copy to tape**. This option copies the volume that contains the selected data to a tape in a DPM library. Click **Next**, and on the **Specify Library** dialog box, select library details and tape options. You can also choose to compress or encrypt the data on tape.
8. Click **Next** after you have specified one of the preceding options.
9. Specify your recovery options:
   a. **Existing version recovery behavior**. Select **Create copy**, **Skip**, or **Overwrite**. This option is enabled only when you selected **Recover to the original location** in step 7.
   b. **Restore security**. Select **Apply settings of the destination computer** or **Apply the security settings of the recovery point version**.
   c. **Network bandwidth usage throttling**. Click **Modify** to enable network bandwidth usage throttling.
   d. **Enable SAN based recovery using hardware snapshots**. Select this option to use SAN-based hardware snapshots for quicker recovery.

      This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.
   e. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
10. Click **Next** after you have made your selections for the preceding options.
11. Review your recovery settings, and click **Recover**.

Note

Any synchronization job for the selected recovery item will be canceled while the recovery is in progress.

See Also

Understanding Data Recovery[new]

Recover Data

Recovery Wizard

How to Recover Data for Windows SharePoint Services Servers

For computers that are running Windows SharePoint Services, System Center 2012 – Data Protection Manager (DPM) supports recovery of the following data by using the Recovery Wizard:

- **SQL Server databases**
  If you protected a Windows SharePoint Services server as a SQL Server database, you can recover Windows SharePoint Services data by selecting the SQL Server database in the Recovery Wizard.

  Note
  DPM supports the protection of mirrored SQL Server databases for Windows SharePoint Services sites. This additional support requires little change to the procedures for using DPM to protect and recover regular Windows SharePoint Services data.
- **Windows SharePoint Services sites and databases**
  If you protected a Windows SharePoint Services server as a front-end Web server, you can recover the following:
  - Farms
  - Windows SharePoint Services databases with SharePoint writers
  - Sites
  - Documents and lists

Caution
Do not directly recover the Central Administration content database because this could lead to data corruption in the Windows SharePoint Services farm.

Note
When recovering a Windows SharePoint Services farm, DPM recovers the configuration database of the farm but does not display this item in in the **Recoverable item** pane.

For more information, see Managing Protected Servers Running Windows SharePoint Services.

To recover protected data for a computer that is running Windows SharePoint Services

1. In DPM Administrator Console, go to the **Recovery** view.

2. Browse to locate and select the recoverable data item that you want to use to recover, and then click **Recover** on the tool ribbon.

   Warning

   On the **Browse** tab, in the **Recovery points for** area, available recovery points are indicated in bold on the calendar. Select a date in bold, and then select a recovery time from the **Recovery time** menu.

   The Recovery Wizard opens.
3. On the **Review Recovery Selection** page, verify your recovery item selection, and then click **Next**.
4. On the **Select Recovery Type** page, specify one of the following types of recovery:
   a. **Recover all SharePoint content and components**.

      Note

      You cannot recover mirrored databases to the original location because, when there are two instances of SQL Server, there is no concept of an original database.

   b. **Copy database files to a network folder**. To select an alternate recovery destination, click **Browse**, and then click **OK**.

      The recovery destination computer must have a DPM protection agent installed.

   c. **Copy the Windows SharePoint Services farm to tape**. This option copies the Windows SharePoint Services farm that contains the selected recoverable items to a tape. If you select this option, click **Next**, and then specify the library and tape options for recovery. You can choose to compress or encrypt the data on the tape.
5. Click **Next**.
6. On the **Specify Recovery Options** page, select one of the following recovery options:
   a. **Network bandwidth usage throttling**. Click **Modify** to enable network bandwidth usage throttling.
   b. **Enable SAN-based recovery using hardware snapshots**. Select this option to use Storage Area Network (SAN)-based hardware snapshots for quicker recovery.

      This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.

   c. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
7. Click **Next** after you have specified your recovery option.
8. Review your recovery settings, and click **Recover**.

   Note

   Any synchronization job for the selected recovery item will be canceled while the

recovery is in progress.

To set recovery options for servers running Windows SharePoint Services using DPM Management Shell

- Use the following syntax to set the recovery options for servers running Windows SharePoint Services:

  New-RecoveryOption [-TargetServer] <*String*> **[-RecoveryLocation]** <*RecoveryLocation*> **[-DPMLibrary** <*Library*>**] [-RecoverToReplicaFromTape] [-SANRecovery] [-RestoreSecurity] -RecoveryType** <*RecoveryType*> **[-TargetLocation** <*String*>**] -SharePointSite -DatabaseFileTempLocation** <*String*> **-IntermediateSharepointServer** <*String*>**-IntermediateSqlInstance** <*String*> **-ExportFileTempLocation** <*String*> **[-TargetSiteUrl** <*String*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help New-RecoveryOption -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help New-RecoveryOption -full**" in DPM Management Shell.

To recover protected data from servers running Windows SharePoint Services using DPM Management Shell

- Use the following syntax to recover data for a Windows SharePoint Services server:

  Recover-RecoverableItem [-RecoverableItem] <*RecoverableObject[]*> **[-RecoveryOption]** <*RecoveryOptions*> **[-RecoveryPointLocation** <*RecoverySourceLocation[]*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-RecoveryNotification** <*Nullable`1*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Recover-RecoverableItem -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Recover-RecoverableItem -full**" in DPM Management Shell.

Recovering Hyper-V Virtual Machines

System Center 2012 – Data Protection Manager (DPM) supports various recovery scenarios for Hyper-V virtual machines.

The following table describes the various support recovery scenarios for Hyper-V:

Scenario	Description
Recovering a virtual machine to its original location.	The original VHD is deleted. DPM will recover the VHD and other configuration files on the original location by using the Hyper-V VSS writer. At the end of the recovery process, virtual machines will still be highly available. **Note** The resource group must be present for recovery to happen. If the resource group is not available, recover to an alternate location and then make the virtual machine highly available.
Recovering a virtual machine to an alternate location	DPM supports alternate location recovery (ALR), which provides a seamless recovery of a protected Hyper-V virtual machine to a different Hyper-V host, independent of processor architecture. Hyper-V virtual machines that are recovered to a cluster node will not be highly available. For more information about how to make a virtual machine highly available, see Make the virtual machine highly available.
Item-level recovery (ILR) of Hyper-V virtual machines	DPM supports item-level recovery (ILR), which allows you to do item-level recovery of files, folders, volumes, and virtual hard disks (VHDs) from a host-level backup of Hyper-V virtual machines to a network share or a volume on a DPM protected server. **Note** The DPM protection agent does not have to be installed inside the guest to perform item-level recovery.

How to Recover System State

System Center 2012 – Data Protection Manager (DPM) offers two types of system protection – Bare Metal Restore (BMR) and System State recovery. When you computer has stopped working, you can get it back up and working by restoring BMR or System State, depending which

type of protection you have set up. Either ways, the procedure to recover system information is the same.

1. Recover the BMR or System State backup to a network location.
2. Use WinRE to start up your system and connect it to the network.
3. Use Windows Server Backup (WSB) to recover your system information from the network location.

Use the following procedure to recover your system information from DPM to a network location.

To recover system information in DPM

1. In DPM Administrator Console, go to the **Recovery** view.
2. Browse or search for the data you want to recover, and then, in the results pane, select the data.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
4. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
5. Click **Recover**. DPM starts the Recovery Wizard.
6. Review your recovery selection, and click **Next**.
7. Select **Copy to a network folder**. Click **Next**, and on the **Specify Destination** dialog box, click **Browse** to select a destination for the database files. When you have selected a destination, click **OK**.

   Tip
   We recommend that you use a new folder to recover the system information. This will make it easier for you to point WSB to the right folder for recovery.
8. After you have specified the type of recovery, click **Next**.
9. Specify your recovery options:
   a. **Enable SAN based recovery using hardware snapshots.** Select this option to use SAN-based hardware snapshots for quicker recovery.

      This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.
   b. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients. Separate the e-mail addresses with commas.
10. After you have specified the recovery option, click **Next**.
11. Review your recovery settings, and click **Recover**.

    Note
    Any synchronization job for the selected recovery item is canceled while the recovery is in progress.

See Also

Recovering Your Server

Disaster Recovery

Recover Data

How to Configure End-User Recovery

You can enable the end-user recovery option to allow end users to independently recover data by retrieving recovery points of files. Users can recover data through shared folders on the DPM server, through a Distributed File System (DFS) namespace, or by using the **Document Recovery** task pane in Microsoft Office. Enabling end-user recovery involves enabling the end-user recovery feature on the DPM server and installing the shadow copy client software on the client computers.

End-user recovery is supported in the Active Directory Domain Services domains in which the domain controllers are running either Windows Server 2003 or Windows 2000 Server with Service Pack 4 or later installed and with schema modifications enabled.

Note

To get the latest updates for Windows 2000 Server, see Microsoft Knowledge Base article 260910. For instructions for enabling schema modifications on a Windows 2000 domain controller, see Microsoft Knowledge Base article 285172.

In this section

How to Enable End-User Recovery

How to Install the Shadow Copy Client Software

How to Recover Data by Using a Client Computer

How to Disable End-User Recovery

See Also

Recover Data

Understanding Data Recovery

How to Enable End-User Recovery

End-user recovery enables users to independently recover file data by retrieving recovery points of their files. Enabling end-user recovery involves configuring Active Directory Domain Services to

support end-user recovery, enabling the end-user recovery feature on the DPM server, and installing the shadow copy client software on the client computers.

Important
System Center 2012 – Data Protection Manager (DPM) supports only short-term, disk-based recovery for end users.

The following procedures show you how to configure Active Directory Domain Services and enable end-user recovery of file data sources.

Note
Before users can begin independently recovering previous versions of their files, the DPM shadow copy client software must be installed on their computers. For more information, see How to Install the Shadow Copy Client Software.

To configure Active Directory Domain Services and enable end-user recovery on a DPM server if you are a schema and domain administrator in the domain

1. In DPM Administrator Console, click **Options** on the tool ribbon.
2. In the **Options** dialog box, on the **End-user Recovery** tab, click **Configure Active Directory**.
3. In the **Configure Active Directory** dialog box, select **Use current credentials** or type the user name and password for an account that has both schema and domain administrator privileges, and then click **OK**.
4. On the confirmation and notification prompts, click **Yes** and then click **OK**.
5. After configuration of Active Directory Domain Services is complete, select the check box for the **Enable end-user recovery** option and then click **OK**.

To configure Active Directory Domain Services and enable end-user recovery on a DPM server if you are not a schema and domain administrator in the domain

1. Direct a user who is both a schema and domain administrator to configure the Active Directory schema by running **<drive:>\Program Files\Microsoft Data Protection Manager\DPM\End User Recovery\DPMADSchemaExtension.exe** on a Windows Server 2003 computer that is a member of the same domain as the DPM server.

   Note
   If the protected computer and DPM reside in different domains, the schema needs to be extended by running the DPMADSchemaExtension.exe tool on the other domain.
2. In the **Enter Data Protection Manager Computer Name** dialog box, type the name of the computer for which you want end-user recovery data in Active Directory Domain Services, and then click **OK**.
3. Type the DNS domain name of the DPM computer for which you want end-user recovery data in Active Directory Domain Services, and then click **OK**.
4. In the **Active Directory Configuration for Data Protection Manager** dialog box, click

OK.

5. In DPM Administrator Console, click **Options** on the tool ribbon.
6. In the **Options** dialog box, on the **End-user Recovery** tab, select the check box for the **Enable end-user recovery** option, and then click **OK**.

See Also

How to Install the Shadow Copy Client Software

How to Install the Shadow Copy Client Software

Before users can begin independently recovering previous versions of their files and applications, the DPM shadow copy client software must be installed on their computers. If a client for Shadow Copies of Shared Folders is present on the computer, the client software must be updated to support System Center 2012 – Data Protection Manager (DPM).

The shadow copy client software can be installed on computers running Windows XP with SP2 or later and Windows Server 2003 with or without SP1.

Note
Shadow copy client software does not need to be downloaded for computers that run Windows Vista.

The following table shows the locations from which you can download the shadow copy client software for each supported operating system.

Supported Operating System	Shadow Copy Client Software Location
Windows XP SP2	http://go.microsoft.com/fwlink/?LinkId=46064
Windows Server 2003	http://go.microsoft.com/fwlink/?LinkId=184264

Install the client software on users' workstations by using your usual software distribution method—for example, Group Policy Software Installation, Microsoft Systems Management Server, Microsoft System Center Configuration Manager, or shared folders. If your users will install the client software on their own workstations, instruct them to copy the Setup program to any location on their computer, double-click the file name or icon, and then follow the instructions in the wizard.

If the setup fails, DPM displays the end-user recovery permissions update failed alert.

Note

When using the end-user recovery functionality of DPM, disable the local shadow copies on the protected server.

How to Recover Data by Using a Client Computer

After users install the recovery point client, they can recover previous versions of data by retrieving recovery points from server for System Center 2012 – Data Protection Manager (DPM). For more information, see How to Install the Shadow Copy Client Software.

Note

If a user recovers data using Microsoft Word on a Windows Server 2008 operating system, there is no need to install the shadow copy client software.

If a protected file was created in an application that supports recovering previous versions of data, you can recover the file by using the application in which it was created.

To recover data by using a client computer

1. Click **Start**, click **Run**, and type the path to the protected data.
2. Browse to the file, right-click the file name, and then click **Properties**.
3. On the **Properties** menu, click **Previous Versions**, and then select the version that you want to recover from the list of available versions.

To recover data by using applications in Office 2003 or later on a client computer running Windows Server 2000 or Windows 2003

1. Open the application in which the data was created.

   Note

   Applications in Office 2003 or later, such as Word 2003 and Excel 2003, support recovery of previous versions.
2. On the **File** menu, click **Open**.
3. In the **Tools** drop-down list, click **Properties**, click **Previous Versions**, and then select the version you want to recover from the list of available versions.

   Note

   When the user browses for recoverable data, the shadow copy client first checks for local recovery points on the protected computer. If local recovery points are available, a list of existing recovery points on the protected computer is displayed. If no recovery points are available on the protected computer, a list of existing recovery points on the DPM server is displayed.

To recover data by using Microsoft Word 2007 on a client computer running Windows Vista or Windows XP

1. Open the application in which the data was created.

   Note
   This procedure assumes that you selected to have Microsoft Word 2007 make backup copies.

2. Click **Microsoft Office**, and then click **Open**.
3. In the box next to the **File name** box on a computer that is running Windows Vista, or in the **Files of type** box on a computer that is running Windows XP, click **All Files**.
4. If you want to open a backup copy that was saved in a different folder, locate and open the folder.
5. Click the arrow next to **Views**, and then click **Details**. In the **Name** column, the backup copy name appears as **Backup of <document name>**. In the **Type** column, the file type for the backup copy appears as **Microsoft Word Backup Document**.
6. Locate and double-click the backup copy to open it.
7. If you want to work with the backup copy as a regular Word document, click **Microsoft Office**, click **Save As**, and then type a name for the file in the **File name** box.

See Also

How to Disable End-User Recovery

How to Enable End-User Recovery

How to Install the Shadow Copy Client Software

How to Disable End-User Recovery

In System Center 2012 – Data Protection Manager (DPM), if you want to stop allowing end users to recover their own data, you can use the following procedure to disable the end-user recovery option.

To disable end-user recovery

1. In DPM Administrator Console, go to the **Recovery** view.
2. Click **End-user recovery**.
3. On the **End-user recovery** tab, clear the **Enable end-user recovery** check box.
4. Click **OK**.

   This action takes effect after the next successful synchronization job is completed. If you want this action to take effect immediately, you can manually synchronize the replica.

See Also

How to Enable End-User Recovery

How to Manually Create a Replica

Synchronize a replica

How to Find Recoverable Data

Monitoring Alerts

When you monitor alerts, you can monitor data protection activity and error conditions in System Center 2012 – Data Protection Manager (DPM) and take action, when necessary, to resolve issues. In DPM, alerts are displayed in the **Monitoring** view.

Each alert should provide sufficient information to resolve the alert. For additional information about a specific job related to the issue, review the job details on the **Jobs** workspace.

If you have multiple DPM servers, you can monitor them centrally using the Central Console. For information about using the Central Console, see Administering DPM with the Central Console.

In This Section

How to Publish DPM Alerts

How to Display Alert Details

How to Display Inactive Alerts

How to Mark an Alert as Inactive

Understanding Alerts

Resolving Alerts

How to Publish DPM Alerts

The **Alert Publishing** option is used only if you have chosen to centrally monitor your servers for System Center 2012 – Data Protection Manager (DPM) in Microsoft Operations Manager or Operations Manager for System Center. This option is used immediately after you deploy the DPM Management Pack for MOM or Operations Manager, or after you restore the DPM database from a backup to synchronize the Operation Manager display with the current state on the DPM server.

This option publishes all existing actionable DPM alerts that might require a user action to the DPM Alerts event log. The MOM or Operations Manager agent that is installed on the DPM server publishes the alerts in the DPM Alerts event log to MOM or Operations Manager and continues to update the display as new alerts are generated.

For information about the DPM Management Pack, see the Guide for System Center Management Pack for Data Protection Manager .

To publish existing DPM alerts

1. In DPM Administrator Console, go to the **Monitoring** view and click **Options** in the tool ribbon.
2. In the **Options** dialog box, on the **Alert Publishing** tab, click **Publish Active Alerts**.
3. Click **OK**.

See Also

Monitoring Alerts

How to Display Alert Details

In the Alerts workspace of the **Monitoring** view, alerts can be grouped by **Protection Group**, **Computer**, **Status**, or **Severity**. The Quick Search functionality in System Center 2012 – Data Protection Manager (DPM) helps you to quickly find information about single or multiple alerts. To find more information about a particular alert, you can use the **Details** pane. The details for each alert vary, depending on the specific conditions that generated the alert and the type of alert selected.

For example, the details for an active “Free tape threshold reached” alert include information such as **Affected area**, **Occurred since**, **Recommended action**, and **Description**. By contrast, the details for a "Recovery success" information alert also include **Resolution**, which provides a link to manually resolve the alert if needed.

Note
In the Event log, a separate node called DPM Alerts is created. This contains some text in encrypted form and is not for the administrator's use. Instead, the System Center Management Pack for Data Protection Manager uses this to show DPM Alerts in its user interface.

To display alert details

1. In DPM Administrator Console, open the **Monitoring** view, and then open the **Alerts** workspace.
2. Select the alert for which you want more details. The alert information is displayed in the **Details** pane.

To display alert details using Quick Search

1. In the Quick Search box, type your search text.

Alerts that contain the text that you typed are displayed in the **Display** pane with the search text highlighted.

To narrow your search, type more characters or additional words.

2. To widen your search to include alert information displayed in the **Details** pane, at the end of the search results, select the **Search details also** check box that is located next to the Quick Search box. This is a detailed search and will take more time.

See Also

How to Display Job Details

Resolving Alerts

How to Display Inactive Alerts

In System Center 2012 – Data Protection Manager (DPM), when an alert is resolved or when the conditions that generated the alert no longer apply, the alert becomes inactive. When the **Show inactive alerts** option is enabled, inactive alerts are displayed for seven days in the **Alerts** workspace of the **Monitoring** view. After an alert has been inactive for seven days, it is removed from the inactive alerts history and it can no longer be displayed.

If you want to display inactive alerts, you can enable the **Show inactive alerts** option. When the **Show inactive alerts** option is enabled, a status category is added to the **Alerts** workspace in the **Monitoring** view. When you group alerts by protection group, computer, or severity, a status column is added that indicates whether an alert is active or inactive. When you group alerts by status, the alerts are displayed in two groups: **Active** and **Inactive**.

To display inactive alerts

1. In DPM Administrator Console, go to the **Monitoring** view and open the **Alerts** workspace.
2. Select the **Show inactive alerts** check box navigation pane.

See Also

Monitoring Alerts

Resolving Alerts

How to Mark an Alert as Inactive

System Center 2012 – Data Protection Manager (DPM) gives users the ability to mark alerts as inactive. Marking alerts as inactive can be done for a variety of reasons—for example, if the alert is no longer meaningful or if you do not plan to resolve the alert.

Note
Marking an alert as inactive should be evaluated on a case-by-case basis and not done except when absolutely necessary.

When you mark an alert as inactive, the protection status for the protection group will change to **OK** in DPM Administrator Console and in the System Center Management Pack for Data Protection Manager.

To mark an alert as inactive

1. In the DPM Administrator console, go to the **Monitoring** view.
2. In the **Alerts** workspace, select the alert you wish to mark as inactive.
3. From the tool ribbon, click **Inactivate**. DPM displays a dialog box about inactivating alerts. DPM displays the alert only if you select **Show inactive alerts**.

   Note
   Inactivate alerts with caution. When you inactivate an alert, protection status changes to **OK**. If you are using Operations Manager for System Center, the alert is resolved there as well.

See Also

How to Display Alert Details

Monitoring Alerts

Understanding Alerts

Alerts are displayed in the **Monitoring** view on the **Alerts** workspace. By viewing alerts, you can monitor data protection activity and error conditions in System Center 2012 – Data Protection Manager (DPM). You can group alerts by protection group, protected computer, severity, or status. You can also display inactive alerts to review past data protection and recovery activity.

Alert severity

DPM displays each alert with one of three severities described in the following table.

Severity	Description
Informational	Provides general information about DPM operations that might not require any action on your part.
Warning	Provides information about potential problems, such as “Disk threshold exceeded,” that might not require immediate action but should be investigated.
Critical	Provides information about problems that need immediate resolution, either by DPM or by you, to ensure that data is fully protected. “Replica missing” and “Disk missing” are examples of critical alerts.

Alert status

DPM designates the status of an alert as active or inactive. DPM gives users the ability to mark alerts as inactive. Marking alerts as inactive can be done for a variety of reasons—for example, if the alert is no longer meaningful or if you do not plan to resolve the alert.

Note
Whether to mark an alert as inactive should be evaluated on a case-by-case basis and should not done except when absolutely necessary.

An active alert is one that either DPM or the administrator must take action to resolve. An alert is designated as inactive when the associated jobs have completed successfully, the appropriate action has been taken to resolve the alert, the conditions that generated the alert no longer apply, or the administrator has marked the alert as inactive. In some cases, DPM automatically designates an alert as inactive after a pre-defined period of time. For example, a “Recovery success” informational alert becomes inactive after three days.

Dynamic nature of alerts

DPM alerts change dynamically in both severity and status after DPM completes jobs that resolve the alerts or when you take action to resolve them. For example, you might see an active, critical “Replica inconsistent” alert in the **Monitoring** view. To resolve the alert, you manually synchronize the replica with consistency check or, if a daily consistency check is scheduled, DPM performs synchronization with consistency check. After a consistency check is successfully completed, the status of the “Replica inconsistent” alert is changed to inactive and the severity of the alert is changed to informational. The display pane displays only the current severity and status of the alert.

Relationship between alerts and jobs

DPM provides both an alerts view and a jobs view so that you can easily locate both summary and detailed information about data protection activity. The **Alerts** workspace aggregates errors, error conditions, and jobs to provide a summary view of what is happening across the entire system. The **Jobs** workspace provides the operational details for each scheduled, completed, running, canceled, or failed job. For example, in response to multiple recovery point creation failures, the alerts view displays a single “Recovery point creation failures” alert, whereas the jobs view displays an entry for each recovery point creation failure. In the jobs view, you can also display completed recovery point creation jobs for the past 30 days and scheduled recovery point creation jobs for the next 7 days.

As a general rule, you should start troubleshooting an issue in DPM by reviewing the relevant alert details.

Note

In the Event log, a separate node called DPM Alerts is created. This contains some text in encrypted form and is not for the administrator's use. Instead, the System Center Management Pack for Data Protection Manager uses this to show DPM Alerts in its user interface.

See Also

How to Display Inactive Alerts

How to Manually Create a Replica

Resolving Alerts

Resolving Alerts

When System Center 2012 – Data Protection Manager (DPM) generates an alert, it marks the alert with one of the following three severities:

- **Informational** Informational alerts provide information about data protection activities that might not require any action on your part.
- **Warning** Warning alerts provide information about potential problems that do not require immediate action but should be investigated.
- **Critical** Critical alerts provide information about problems that need immediate resolution, either by DPM or by you, to ensure that your data is fully protected.

To resolve a single or multiple alerts that requires action on your part, review the alert details, determine what is causing the problem, and perform the recommended action. To ensure that you are notified of critical alerts, you can subscribe to notifications that will be sent by e-mail.

See Also

Monitoring Alerts

Monitoring Jobs

Jobs are displayed in the **Monitoring** view when you select a filter under **Jobs**. Here you can monitor the activity log of all tasks in System Center 2012 – Data Protection Manager (DPM). Use the **Group by** drop-down list box to group the list of jobs by protection group, computer, status, or type. Use the **Filters** drop-down list box to sort the list of jobs according to a selected set of parameters.

DPM provides both an alerts view and a jobs view so that you can easily access both summary and detailed information about data protection activity. The **Alerts** workspace aggregates information from one or more related jobs and displays actionable tasks. The **Jobs** workspace provides the operational details for each scheduled, completed, running, canceled, or failed job so that you can troubleshoot and identify backup schedules. As a general rule, you should start troubleshooting an issue in DPM by reviewing the relevant alert details. For detailed information about a specific job related to the issue, review the job details.

In this section

Job Types

How to Retry a Job

How to Cancel a Job

How to Check Data Protection Job Status

How to Modify the Jobs Display

How to Display Job Details

How to Display End Time for a Job

How to Use Filters to Search for Jobs

How to Reschedule a Protection Job Using DPM Management Shell

Job Types

To view jobs in System Center 2012 – Data Protection Manager (DPM), in DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** workspace. The following table provides a list of the possible job types that you might see in the display pane on the **Jobs** tab.

Job Type	Description
Replica creation	Occurs when an initial replica of a data source selected for protection is being created in DPM.
Consistency check	Occurs when the replica in DPM is being checked for consistency with the data source on the protected computer. DPM fixes any issues that are found.
Synchronization	Files: Occurs when the replica in DPM is being updated with the changes from the protected computer. Applications: Occurs when the recovery point creation job synchronizes and creates a recovery point.
Recovery point	Occurs when a recovery point of a replica is being created in DPM.
Disk recovery	Occurs when data is in the process of being recovered from a disk-based recovery point.
Tape erase data	Occurs when data on a selected tape is erased.
Drive cleaning	Occurs when a tape drive is cleaned.
Detailed inventory	Occurs when the administrator runs a detailed inventory on a tape.
Fast inventory	Occurs when the administrator runs a fast inventory on a tape.
Tape verification	Occurs when a selected tape is verified.
Data copy	Occurs when selected data is copied.
Tape backup	Occurs when a selected tape is backed up.
Tape recovery	Occurs when data on a tape is recovered.
Copy data - tape	Occurs when data from a tape is copied to disk or to another tape.
Recoverable items recatalog	Occurs when a tape from another DPM server is being recataloged.
Tape recatalog	Occurs when a tape is recataloged.
Library rescan	Occurs when a library is rescanned.
SharePointCatalogTaskType	Occurs when running a scheduled SharePoint

Job Type	Description
	backup.
SharePointExportAndImport	Occurs when a SharePoint item-level recovery is performed.
StagingAreaRestore	Occurs when recovering files or applications from any folder that is located in a DPM server to a protected computer.

See Also

How to Cancel a Job

How to Modify the Jobs Display

How to Retry a Job

Monitoring Jobs

How to Retry a Job

If one or more jobs fail or are canceled by System Center 2012 – Data Protection Manager (DPM), you can retry the jobs. If you manually cancel one or more jobs, they are deleted. Therefore, you cannot retry the jobs.

To retry a job

1. In DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** workspace.
2. Click a job whose status is **Failed**, and then in the click **Retry** on the tool ribbon.
3. In the **Data Protection Manager** message box that appears, click **Yes**. A new job will be scheduled to run immediately.

   Note
   Rescheduling a job does not remove the entry on the **Jobs** display for the failed job.

See Also

How to Cancel a Job

How to Check Data Protection Job Status

How to Modify the Jobs Display

How to Cancel a Job

System Center 2012 – Data Protection Manager (DPM) enables you to cancel single or multiple jobs, such as recoveries, synchronization, recovery points, or consistency checks. For example, if a recovery is negatively affecting network performance, you can cancel the job and run it again.

To cancel a job

1. In DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** workspace.
2. Group by **Status**.
3. Select the scheduled job, and click **Cancel** on the tool ribbon.
4. In the **Data Protection Manager** message box that appears, click **Yes** to confirm that you want to cancel the job.

   Note

   When you cancel a scheduled job, it is deleted, so you cannot retry it. However, if a job fails or is canceled by DPM, you can select that failed job and use the **Retry** command to run it again.

   When you cancel a scheduled job, only that specific job is canceled, not the other jobs scheduled for the same time, and no alert is displayed. For example, if you cancel a synchronization job at 9:00 A.M. on a Tuesday, the 9:00 A.M. synchronization job still occurs, as scheduled, on all subsequent days, including the following Tuesday.

   Sometimes when you cancel a job, the job completes before it can be canceled. This happens when you cancel a job that completes quickly or one that is already near completion.

See Also

Modify protection options

How to Modify the Jobs Display

How to Retry a Job

How to Check Data Protection Job Status

System Center 2012 – Data Protection Manager (DPM) tracks the status of data protection jobs as scheduled, completed, canceled, or failed. In the **Monitoring** view, you can check the status of jobs.

Note

DPM does not support some types of files and displays a warning of unsupported data in these cases. For more information, see the "How to display warnings for unsupported data" procedure below.

To check data protection job status

1. In DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** workspace.
2. In the **Group by** list box, select **Status**.
3. To review details for a specific job, select the job and refer to the information in the **Details** pane. The rest of the table then re-sorts relative to the column title that you click.

   Note
   DPM limits how long a job can run before it is completed. For example, if a synchronization job times out, DPM generates an error and the job status is reported as **Failed**.

How to display warnings for unsupported data

1. In DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** tab.
2. In the **Group by** list box, select **Type**.
3. In the **Status** pane, check all **Synchronization** jobs for warnings about unsupported data.
4. Click the warning for information about which data sources have recovery failures.

   Note
   The maximum number of unsupported data source files displayed is 255.

See Also

How to Cancel a Job

Modify protection options

How to Modify the Jobs Display

How to Use Filters to Search for Jobs

Job Types

How to Modify the Jobs Display

You can customize the data on the **Jobs** tab to reflect the information that you want to see. You can also create filters to save the way you want System Center 2012 – Data Protection Manager (DPM) to display jobs information. For more information about using filters, see How to Use Filters to Search for Jobs.

To modify the jobs display

1. In DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** workspace.
2. Group by **Protection Group**, **Computer**, **Status**, or **Type** to group the displayed information by these categories.
3. To sort jobs by column, in the display pane, click **Source**, **Computer**, **Protection Group**, **Type**, **Start Time**, **Time Elapsed**, or **Data Transferred**.

   The rest of the table then re-sorts relative to the column title that you click.

See Also

How to Cancel a Job

Modify protection options

How to Use Filters to Search for Jobs

How to Display Job Details

In System Center 2012 – Data Protection Manager (DPM), in the **Monitoring** view, in the **Jobs** workspace, jobs can be grouped by **Protection Group**, **Computer**, **Status**, or **Type**. By default, jobs are grouped by status. The Quick Search functionality in DPM helps you to quickly find information about single or multiple jobs. To find more information about a particular job, you can use the **Details** pane. The jobs view can be further refined by including or excluding synchronization jobs, or by using a specific filter. The details vary, depending on the type of job selected. For example, the details for a replica creation job specify status, start time, how long the job has been running or how long it took to complete the job, how much data was copied, data source details, the number of protection group members, and the name of the protection group to which the replica belongs.

Note

For consistency check jobs, DPM displays the number of files scanned and the number of files that were fixed.

To display job details

1. In DPM Administrator Console, go to the **Monitoring** view, and then open the **Jobs** workspace.
2. Select the job for which you want more details. The information for the job is displayed in the **Details** pane, in the lower part of the console.

To display job details using Quick Search

1. In the Quick Search box, type your search text.

   Jobs that contain the text that you typed are displayed in the workspace with the search text highlighted.

   To narrow your search, type more characters or additional words.
2. To widen your search to include job information displayed in the **Details** pane, at the end of the search results, select the **Search details also** check box that is located next to the Quick Search box. This is a detailed search and will take more time.

See Also

How to Cancel a Job

Modify protection options

How to Modify the Jobs Display

How to Retry a Job

How to Use Filters to Search for Jobs

How to Display End Time for a Job

System Center 2012 – Data Protection Manager (DPM) displays end times for jobs in the **Details** pane. You can use this end time with a DPM filter to select all jobs that failed during a select period of time. This can help you analyze when jobs failed and find other jobs that failed during a specific time period.

To display end time for a job

1. In DPM Administrator Console, go to the **Monitoring** view.
2. Open the **Jobs** workspace, and under **Failed**, select the job you want DPM to display.

   DPM displays the following job information in the **Details** pane: **Type**, **Status**, **Description**, **End time**, **Start time**, **Time elapsed**, **Data transferred**, **Cluster Node**, and **Recovery Point Type**. For tape jobs, DPM displays **Type**, **Status**, **End time**, **Start time**, and **Library**.

See Also

How to Check Data Protection Job Status

How to Use Filters to Search for Jobs

How to Use Filters to Search for Jobs

Filters allow you to display jobs in System Center 2012 – Data Protection Manager (DPM) in a variety of ways. You can filter by job, by job status, by protection group or computer, or you can create your own filter using various options.

To use filters

1. In DPM Administrator Console, go to the **Monitoring** view.
2. Select a default filter from the **Browse** pane on the left.

To create a filter

1. In DPM Administrator Console, go to the **Monitoring** view.
2. On the **Browse** pane, click **Create filter**.
3. Click **Create** on the tool ribbon.
4. Enter a filter name: for example, Scheduled Jobs.
5. Select the **Time from** option from the drop-down menu or choose a time.

   Note
   If you select **Choose date** from the pull-down menu, DPM displays a pop-up calendar so that you can click a date.
6. Select the **Time to** option from the pull-down menu.
7. On the **Jobs** tab, select one or more job types and job status.
8. On the **Protection** tab, select whether to group by protection group or by computer, and select the protection group and members for which you want information displayed. Also, if you want DPM to filter jobs on external media, select **External tape jobs**.
9. On the **Other** tab, optionally specify the **Time elapsed** in **Minutes** or **Hours** and the **Data transferred** in MB and then select or clear the check boxes next to the libraries to which you want to apply the filter.

   Note
   DPM allows you to choose a **Greater than** or **Less than** value for **Time elapsed** and **Data transferred**.
10. Click **Preview** to preview the filtered jobs display, or click **Save** to save the filter.

    Important
    You need to refresh the filter to detect jobs of any new or modified protection group.

To refresh a filter

1. In DPM Administrator Console, go to the **Monitoring** view.
2. On the **Browse** pane, select the filter you want to refresh.

3. Click **Refresh** on the tool ribbon.

See Also

[How to Delete a Filter]

[How to Modify a Job Search Filter]

[How to Save Filters]

[Monitoring Jobs]

How to Save Filters

When you protect multiple data sources, the number of jobs increases exponentially, as does the need to better diagnose and address job failures. System Center 2012 – Data Protection Manager (DPM) allows you to better manage jobs by saving searches with filters.

To save a filter

1. In DPM Administrator Console, go to the **Monitoring** view.
2. Open the **Jobs** workspace.
3. Click **Create** on the tool ribbon.
4. Enter a filter name: for example, **Scheduled Jobs**.
5. Select the **Time from** option from the pull-down menu, or choose a time.

   Note
   If you select **Choose date** from the pull-down menu, DPM displays a pop-up calendar so that you can click a date.
6. Select the **Time to** option from the pull-down menu.
7. On the **Jobs** tab, select one or more job types and job status.
8. On the **Protection** tab, select whether to group by protection group or by computer, and select the protection group and members for which you want information displayed. If you want DPM to filter jobs on external media, you can also select **External tape jobs**.
9. On the **Other** tab, optionally specify the **Time elapsed** in **Minutes** or **Hours** and the **Data transferred** in MB and then select the libraries to which you want to apply the filter.

   Note
   DPM allows you to choose a **Greater than** or **Less than** value for the **Time elapsed** and **Data transferred**.
10. Click **Preview** to preview the filtered jobs display, or click **Save** to save the filter and search.

    Important

You need to refresh the filter to detect jobs of any new or modified protection group.

See Also

How to Delete a Filter

How to Modify a Job Search Filter

How to Use Filters to Search for Jobs

How to Modify a Job Search Filter

System Center 2012 – Data Protection Manager (DPM) allows you to modify job search filters that you have created and saved. If you receive too many results from a saved filter, consider changing the parameters to refine your search.

Note
Default filters cannot be modified or deleted.

To modify a job search filter

1. In DPM Administrator Console, go to the **Monitoring** view.
2. Select the filter you want to modify from the **Filters** list.
3. On the tool ribbon, click **Modify**.
4. On the **Jobs**, **Protection**, and **Other** tabs, make your changes to the search parameters.
5. Click **Preview** to preview the filtered jobs display, or click **Save** to save your changes to the filter.

   Important
   You need to refresh the filter to detect jobs of any new or modified protection group.

See Also

How to Delete a Filter

How to Use Filters to Search for Jobs

How to Delete a Filter

If a filter is no longer useful or if it returns too many results, you can use the following procedure in System Center 2012 – Data Protection Manager (DPM) to delete the filter.

To delete a filter

1. In DPM Administrator Console, go to the **Monitoring** view.
2. Open the **Jobs** workspace, and select the filter you want to delete from the **Filters** pull-down menu.
3. Click **Delete filter** on the tool ribbon.

   Note
   The default filter cannot be deleted.

See Also

How to Modify a Job Search Filter

How to Use Filters to Search for Jobs

How to Reschedule a Protection Job Using DPM Management Shell

You can set the start time for protection jobs only by using DPM Management Shell. The protection jobs that you can reschedule are catalog pruning and detailed inventory.

To schedule a protection job

1. Use the following syntax to retrieve the current start time for a protection job:

   Get-ProtectionJobStartTime [-ProtectionGroup] <*ProtectionGroup*> **[-JobType]** <*ProtectionJobType*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
2. Use the following syntax to set the start time for a protection job:

   Set-ProtectionJobStartTime [-ProtectionGroup] <*ProtectionGroup*> **[-JobType]** <*ProtectionJobType*> **[-StartTime]** <*DateTime*> **[-MaximumDurationInHours]** <*Int32*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
3. Use the following syntax to remove the start time for a protection job:

   Set-ProtectionJobStartTime [-ProtectionGroup] <*ProtectionGroup*> **[-JobType]** <*ProtectionJobType*> **-Remove [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

   For more information, type "**Get-Help Set-ProtectionJobStartTime -detailed**" in DPM Management Shell.

   For technical information, type "**Get-Help Set-ProtectionJobStartTime -full**" in DPM

Management Shell.

See Also

How to Reschedule a Maintenance Job

Understanding Data Protection

Using Reports

You can use reporting in System Center 2012 – Data Protection Manager (DPM) to track the success of synchronization and recovery point jobs, review disk and tape utilization, and monitor trends in data protection activity. In addition, you can evaluate backup service performance over long periods of time to ensure that backup needs are being met. Using DPM reporting, you can view reports, schedule reports, and subscribe to reports sent by e-mail.

DPM reporting uses SQL Server to collect data and SQL Server 2008 Reporting Services to generate reports. Reporting Services provides tools that you can use to monitor and/or troubleshoot DPM reporting. For more information about troubleshooting DPM reporting, see the Troubleshooting. For more information about SQL Server Reporting Services, see Microsoft SQL Services Reporting Overview.

In This Section

About Reports

Report Types

How to Print Reports

How to Display Reports

How to Schedule Reports

How to Create or Modify Report Subscriptions

About Reports

Reporting in System Center 2012 – Data Protection Manager (DPM) enables you to create and customize both new reports and historical reports.

A *new report* is created dynamically, based on the options that you select when you set up the report. New reports are not saved for future reference; they are disposed of when closed. If you want to save a new report that you have created, you must export it by using the Reporting Services Web toolbar. For more information, see How to Display Reports.

A *historical report* is created and saved for future reference only when you schedule a report. You choose the options that you want at the time you schedule the report. When you schedule a

report, you set the option for the number of reports, up to a maximum of 18, that you want to save in history for that report type. Only scheduled reports that run successfully are saved as history. For more information, see How to Schedule Reports.

A report selected through DPM Administrator Console always opens as a Web page in Internet Explorer.

See Also

How to Display Reports

How to Schedule Reports

Report Types

Using Reports

Report Types

DPM reporting offers six standard reports that you can generate, review, and analyze. These reports help you realize the full benefits of System Center 2012 – Data Protection Manager (DPM). The following table lists the reports and their definitions. You can click the links to view more details about the reports.

Report Type	Description
Status Report	Includes status of recently run recovery point creation and recovery jobs. The report shows trends in the frequency of errors that occur and lists the number of alerts.
Disk Utilization Report	Provides a summary view of disk capacity, allocation, and usage of disk space for the DPM storage pool. The data is collected per computer and is aggregated for all computers. You can use this report to identify the costs associated with backup for various protected computers plus identify trends in disk usage to plan for capacity.
Recovery Report	Provides details about recovery times and statistics of recovery jobs for tracking recovery performance. The data is collected per computer or protection group and is aggregated for all computers.
Tape Management Report	Provides details for managing tape rotation and

Report Type	Description
	decommissioning tapes. The report also displays which tapes are due to be brought back from recycling. The data is collected per library and aggregated for all libraries.
Tape Utilization Report	Provides trends in tape utilization to assist in capacity planning and making decisions about allocating additional tapes.
Recovery Point Status Report	The Recovery Point Status report provides the recovery point status of all selected data sources. This report gives administrators a high-level view of whether backup service-level agreements (SLAs) are being met for every data source.

See Also

How to Create or Modify Report Subscriptions

How to Display Reports

How to Print Reports

How to Schedule Reports

Status Report

The Status Report provides the status of all recovery points for a specified period, lists recovery jobs, and shows the total number of successes and failures for recovery points and disk-based and tape-based recovery point creations. This report shows trends in the frequency of errors that occur and lists the number of alerts.

Frequently Asked Questions

While you are reviewing the data in the Status Report, you might have the following questions about how to use the data or interpret the report.

Why is the trend of recovery point job failures rising?

This can be caused by a variety of issues. You can review the details for a recovery point job failure in the **Monitoring** task area and determine the resolution. For more information, see How to Display Job Details.

Why is the protection objective not being met?

A recovery point is created only if the corresponding synchronization job, since the last recovery point job, was run successfully. If the corresponding synchronization job failed, the scheduled recovery point will not be created.

See Also

How to Print Reports

Report Types

Using Reports

Working with Recovery Points

Disk Utilization Report

The Disk Utilization Report provides a summary view of disk capacity, disk allocation, and usage of disk space in the storage pool for System Center 2012 – Data Protection Manager (DPM). The data is collected per protected computer and aggregated for all protected computers or per protection group and aggregated for all protection groups.

The first page of the report, the summary page, shows disk utilization statistics for all protected computers or protection groups at a protected computer or protection group level, as specified in the report parameters. Subsequent pages, the detail pages, show disk utilization details for each protected computer or protection group at a volume level.

Frequently asked questions

While you are reviewing the data in the Disk Utilization Report, you might have questions about how to use the data or interpret the report.

How do I determine whether the DPM server is running out of disk space?

There are several data points that you might want to consider:

- If “Disk Used” size is within 70 to 80 percent of “Total Disk Capacity,” you might soon run out of disk space. To avoid interruption of data protection activities, you should add disks to the storage pool.
- If “Disk Used” size is very close to the “Disk Allocated” size, the replica and recovery point volumes are nearly full. If the amount of protected data is expanding, you should consider increasing the disk space allocated for replicas. For more information, see How to Modify Disk Allocation.

- If “Disk Allocated” size is close to “Total Disk Capacity” and you plan to protect a new volume, you might need to add disks to the storage pool or stop protecting other volumes so that you can protect the new volume. For more information, see Remove protection group members.

How do I see the disk utilization for data sources that are co-located?

To view the disk utilization report for co-located data sources, you can generate a disk utilization report for the protection group having co-located data sources.

1. In DPM Administrator Console, go to the **Reporting** view.
2. Select **Disk Utilization** report, and click **View** on the tool ribbon. Alternatively, you can right-click the **Disk Utilization** report in the **display** pane and then click **View**.
3. On the **New** tab, select display options for the report and then click **OK**. For **Group by**, select **protection group** to group items in the report by protection group. You can view the disk allocated and disk used for the protection groups having co-located data sources.

 **To view the co-located replica details of each co-located data source**

1. In DPM Administrator Console, go to the **Protection** view.
2. In the **display** pane, right-click the protection group and select **Modify disk allocation**.
3. On the **DPM Server** tab, click **Collocated Protection**.

Why are disk utilization statistics reported for inactive protection groups?

If you delete a protection group but retain its associated replicas and recovery points, the replicas and recovery points continue to use disk space. As long as the replicas and recovery points are retained, the Disk Utilization Report will continue to display disk usage statistics for the deleted protection group, both on the summary page and on the detail pages. Disk utilization statistics for deleted protection groups are displayed under the “(Inactive Replicas)” heading. For information about deleting protection groups, replicas, and recovery points, see Working with Protection Groups.

What does a negative change for Disk Usage Growth Rate mean?

A negative number indicates that the size of data in the storage pool is decreasing over time. A positive number indicates that the size of data in the storage pool is increasing over time.

Does the Storage Pool Details table include disk usage for protected computers?

No, the table specifies only the disk space allocated and used for replicas and recovery points in the storage pool on the DPM server.

Why is disk utilization for inactive replicas not reported correctly in the Disk Utilization Report?

For existing protection groups or protected computers, the Disk Utilization Report does not display the current information for replicas that were removed, added, or removed from protection on the day that the report is generated. Disk utilization for these replicas will be correct in reports generated at least a day after the change is made.

How do I determine whether the change journal on the protected computer is running out of disk space?

The disk utilization data for the change journal is displayed in the last column of the Storage Pool Details table. DPM sets the default for change journal space at 300 MB. For more information, see How to Modify Disk Allocation.

To determine whether a change journal is running out of disk space

1. In DPM Administrator console, go to **Protection** view.
2. Select the protection group associated with the change journal.
3. Click **Modify disk allocation** on the tool ribbon.
4. Click the **Protected computer** tab to display the current disk allocation for the change journal.
5. Compare the allocated disk space with the data in your report to determine whether the change journal is running out of disk space.

See Also

How to Print Reports

Recovery Report

The Recovery Report provides statistics on administrator-initiated recoveries only. It displays recoveries in both time taken and size over the selected time period. The data is collected per protected computer and aggregated for all protected computers, or it is collected per protection group and aggregated for all protection groups.

The first page of the report, the summary page, shows recovery statistics for all protected computers or protection groups at a protected computer or protection group level, as specified in

the report parameters. Subsequent pages, the detailed pages, show details of recoveries for each protected computer or protection group at a volume level.

Frequently Asked Questions

While you are reviewing the data in the Recovery Report, you might have the following questions about how to use the data or interpret the report.

Do the pie charts include data for all entities protected by DPM?

Yes, pie charts include all data being protected by DPM.

Why is the number of recovery job failures increasing?

A rising trend in recovery job failures might be due to an increased number of network outages or job cancellations. The data for recovery failures includes only administrator-initiated cancellations of recovery jobs, not cancellations initiated by end-users. To determine the common causes for recovery job failures, check the details of the Recovery Report.

For information about the status of recovery jobs for the last 30 days, see How to Check Data Protection Job Status.

See Also

How to Print Reports

How to Schedule Reports

Recover Data

Report Types

Using Reports

Tape Management Report

The Tape Management Report provides details for managing tape rotation. The report lists all libraries that are below the free tape threshold. The data is collected per library and aggregated for all libraries.

Frequently Asked Questions

While you are reviewing the data in the Tape Management Report, you might have the following questions about how to use the data or interpret the report.

A tape that has been decommissioned still appears in the Tape Management Report—how can I update the report?

Update the DPM library information by following these steps:

1. Properly remove the tape from the drive by following the recommended procedures of the tape library vendor.
2. Power down and then restart the tape library.
3. In DPM Administrator Console, on the **Libraries** tab in the **Management** task area, click **Inventory library**.
4. In the **Inventory** dialog box, select **Detailed inventory**, and then click **Start**.

What happens when the data on a tape expires?

When the data on a tape expires, return the tape to the tape library for reuse. Expired tapes that have not been returned to the tape library will be marked as "overdue" in the Tape Management Report.

What is a free tape threshold?

The *free tape threshold* is the number of tapes in a specified library that are available for use by DPM. If the number of libraries below the free tape threshold is equal to the free tape threshold value on the Tape Management Report, you must add tape to the library and mark it as free or future backup jobs will fail.

See Also

How to Print Reports

Managing Tapes

Using Reports

Tape Utilization Report

The Tape Utilization Report provides trends in tape utilization to assist in capacity planning and making decisions about allocating additional tapes.

The first page of the report, the summary page, shows tape utilization statistics for all protection groups as specified by the time period in the report parameters. This allows system administrators to view trends in tape usage to allow them to make early purchase decisions.

Frequently Asked Questions

While you are reviewing the data in the Tape Utilization Report, you might have the following questions about how to use the data or interpret the report.

How often should I run a Tape Utilization Report?

You should run the Tape Utilization Report whenever you need to make decisions about the capacity and utilization of your tape library. You might want to run a Tape Utilization Report once a quarter.

How do I determine when I will run out of capacity on the tape?

The Tape Utilization Report provides trends of tape usage. If you notice that tape usage has been increasing on the backup server, you can estimate the percentage for the number of tapes that will be used over the next report period. If the trend for tape usage is upward, estimate when you will run out of capacity and acquire additional tapes before you no longer have space.

The Tape Utilization Report shows unrecognized tapes in the library. How do I get DPM to recognize the tapes?

When a tape containing data is added to the tape library and the tape label displays as "Unknown", you can use DPM to identify the tape.

When DPM identifies the tape, it reads the tape header and updates the tape label as follows:

- A tape created by the DPM server displays the assigned tape label.
- A tape created by another DPM server displays **Imported** as the tape label.
- A tape that contains content that was not created by DPM displays **Unrecognized** as the tape label.

See Also

How to Identify an Unknown Tape

How to Print Reports

Managing Tapes

Report Types

Using Reports

Recovery Point Status Report

System Center 2012 – Data Protection Manager (DPM) features an enhanced recovery point status reporting. It gives administrators a high-level view of whether backup service level agreements (SLAs) are being met for every data source. It is also useful to backup operators who can quickly identify if backup SLAs are being met and then prioritize the data source that the operator needs to focus on.

This report can be configured to be sent as an e-mail so that administrators don’t need to log on to the DPM server to track recovery point status.

Viewing recovery point status

The Recovery Point Status report provides the recovery point status of all selected data sources. If a minimum of one good recovery point is present in the specified recovery point window, the status is shown as green. A blank recovery point window indicates that no recovery point is present in that time window.

You can view this report from either the **Protection** view or the **Reporting** view of the Administrator Console.

If you start the report from the **Protection** view, you can view the report for all the data sources that interest you. Starting the report from the **Reporting** view will only show data for data sources protected by that DPM server.

Viewing report from Reporting tab

1. Double-click **Recovery Point Status Report** in the **Reporting** view of the Administrator Console. This will bring up the **Recovery Point Status Options** dialog box.
2. On the **General** tab in the **Recovery Point Status Options** dialog box, you have:
   - Date and time options – Specify the date range for which the report should be generated.
   - Protection type – Select whether the report should display items protected on disk, tape or online or a combination of these.
3. On the **Advanced** tab in the **Recovery Point Status Options** dialog box, you can specify a different the recovery point window for each protection group.
4. Click **Generate** to view the report.

Viewing report from Protection tab

On the **Protection** view, use the **View recovery point status** link. If you have not selected a protection group, DPM will display the status for all protection groups. If you have selected one or more protection groups or data sources, then only the status of selected items will be displayed.

Warning

If you select an inactive data source no report will be generated.

Setting scheduling and e-mail options

You can schedule when you want the Recover Point Status report to run using the **Schedule** option on the tool ribbon of the **Protection** view.

On the Schedule tab

- Specify whether you want the report to run on a schedule.
- Specify the frequency for when the report will be run.
- Specify how many days' worth of reports need to be maintained in history.

On the E-mail tab

- Specify the people to whom the report must be emailed.
- Specify the format for the report.

See Also

Report Types

Recovery Point Status Options - General Tab

Recovery Point Status Options - Advanced Tab

Recovery Point Status Options - General Tab

On the **General** tab on the **Recovery Point Status Options** screen, you can generate a report to view the status for all protection groups. If you have selected one or more protection groups or data sources, then only the status of the selected items will be displayed.

This page contains the elements described in the following table.

Elements

Name	Description
Date from	Use the **Data from** box to select the date from which the report should be generated.
Time from	Use the **Time from** box to select the start time from which the report should be generated.
Date to	Use the **Date to** box to select the end date till which the report should be generated.
Disk	In the protection type section, select **Disk** check box for generating a report having display items protected on disk.
Tape	In the protection type section, select **Tape** check box for generating a report having display items protected on tape.

After selecting the recovery point status options, click **Generate report**.

See Also

Recovery Point Status Report

Recovery Point Status Options - Advanced Tab

On the **Advanced** tab on the **Recovery Point Status Options** screen, you can generate a report to view the recovery point status for all protection groups.

This page contains the elements described in the following table.

Elements

Name	Description
Protection group	Displays the list of all protection groups created by you.
Recovery point window	Select a recovery point window for each protection group. The minimum time interval for each entry in the Recovery point window is 1 hour and a maximum of 1 month.

After selecting the recovery point status options, click **Generate report**.

See Also

Recovery Point Status Report

How to Print Reports

Reports in System Center 2012 – Data Protection Manager (DPM) have been designed to print on A4 paper without horizontally splitting the information across pages. The MHTML and PDF formats are not editable, so you cannot modify the report to fit other paper sizes.

For best print results, use the following procedures for printing reports.

To print MHTML reports

1. On the Internet Explorer **File** menu, click **Page Setup**.
2. Set paper size to A4.

3. In the **Orientation** area, select a **Portrait** orientation.
4. In the **Margins** area, set the margins to values no greater than the following (in inches): **Left:** 0.11, **Right:** 0.11, **Top:** 0.11, **Bottom:** 0.11.
5. Print the report.

To print a PDF report

1. In Adobe Acrobat, open the **Print** dialog box.
2. Set **Page Scaling** to **Shrink large pages** (the default setting).
3. Select **Auto-Rotate and Center**.
4. On the **Advanced** tab, set the orientation to **Portrait**.
5. Print the report.

To print a report using Microsoft Excel 2003

1. On the **File** menu, click **Page Setup** and then click the **Page** tab.
2. Set the orientation to **Portrait**.
3. Set **Scaling** to **Select Fit to 1 page(s) wide by 1 tall (preferred)**

   - Or –

   Set **Adjust to** to **80-85% of normal size**.
4. Set the paper size to **A4**.
5. On the **Margins** tab, set the **Top**, **Left**, **Bottom**, and **Footer** margins to 0.
6. On the **Sheet** tab, clear the **Gridlines** check box if it is selected.
7. Print the report.

To print a report using Microsoft Excel 2007

1. Click in the file.
2. On the **Page Layout tab**, click **Orientation**.
3. Set the orientation to **Portrait**.
4. Click **Size** and click **A4** to set the paper size.
5. Click **Margins**, click **Custom**, and set the **Top**, **Left**, **Bottom**, and **Footer** margins to 0.
6. In the **Scale to Fit** area, in the **Scale** field, set the scale to 80%.
7. In the **Sheet Options** area, clear the **Print** check box if it is selected.
8. Print the report.

See Also

How to Create or Modify Report Subscriptions

How to Display Reports

How to Schedule Reports

Report Types

How to Display Reports

You can display both new and historical reports in Internet Explorer through the Administrator Console for System Center 2012 – Data Protection Manager (DPM). Before displaying reports for the first time, it is recommended that you allow at least 24 hours of data protection activity to ensure that there is sufficient data to report.

You can use the features of the Reporting Services Web toolbar at the top of each report to customize the report display, to export the report, and to print the report. The following table describes what you can do with each toolbar feature.

Feature	Description
Page controls	Navigate between report pages by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Zoom	Change page magnification. The range is from **Page Width** to **10%**. The default is **100%**.
Find | Next	Search for words or phrases within the report. Click **Find** for the first occurrence of a value; for subsequent occurrences of the same value, click **Next**.
Export	Select a report format, and export the report in that format. Choose from Web archive (MHTML), Web page for Internet Explorer 5.0 or later (HTML), Acrobat (PDF), or Excel.
Refresh	Refresh the contents of the page.
Print	Print the report.

To display a new report

1. In DPM Administrator Console, click **Reporting** on the navigation bar.
2. Select a report, and click **View** on the tool ribbon.

   Alternatively, you can double-click a report or right-click a report in the display pane and click **View**.
3. On the **New** tab, select display options for the report and click **OK**.
   a. **Group by**: Choose whether to group items in the report by protected computer or by

protection group.

b. **Granularity**: Select **Weeks**, **Months**, **Quarters**, or **Years**.

The following table explains how DPM interprets each unit of time.

Unit of time	Definition
Week	Seven days—from Sunday through Saturday.
Month	A full month from the first to the last day of the month.
Quarter	Jan–Mar, Apr–Jun, Jul–Sept, or Oct–Dec.
Year	January 1 to December 31 of a particular year.

c. **Content**: Select the time period for which you want to display report data. The time period covered for each report is displayed at the top of the report.

To exclude the current time period from the report, clear the **Include the data for this week** check box. This setting is selected by default.

To display historical reports

1. In the DPM Administrator Console, go to the **Reporting** view.
2. Select a report and click **View** on the tool ribbon.

   Alternatively, you can double-click a report in the display pane, right-click it, and click **View**, or you can click **View** in the **History** section of the **Details** pane.
3. Click the **History** tab.
4. From the **Available reports** list, click the specific report that you want to view and then click **OK**.

   The **Available reports** list displays all saved copies of a report. When the number of historical reports saved equals the maximum number specified in the report schedule, the next report that is saved will replace the oldest copy of the report, so you can retain the maximum number of copies at all times.

See Also

About Reports

How to Print Reports

How to Schedule Reports

How to Create or Modify Report Subscriptions

How to Schedule Reports

No reports are scheduled in System Center 2012 – Data Protection Manager (DPM) by default. To prompt DPM to start creating and saving historical reports, you must specify report creation schedules. Each of the standard reports operates on an independent schedule. You can schedule DPM reports to run one time, weekly, or monthly, and you can customize the way data is organized within the report. When you schedule reports, you can also elect to send reports to specified recipients via e-mail.

Note
You cannot set multiple schedules for a report. If you modify a report schedule, the previous schedule is replaced.

Although you can schedule a report to run at any time, you might not see meaningful data in the report until after DPM has been protecting data for a week or longer. For example, DPM needs to collect protection activity data for at least one week, Sunday to Saturday, to generate a meaningful weekly report.

To schedule a report

1. In DPM Administrator Console, go to the **Reporting** view.
2. On the display pane, select the report that you want to schedule.
3. Click **Schedule** or right-click the report icon and then click **Schedule**.
4. In the **View <name of report>** dialog box, select the **Run the <name of report> according to the schedule options** box.
5. On the **Schedule** tab, select schedule options and click **OK**.
   a. **Frequency:** Choose the frequency of the report, using the guidelines in the following table.

Select this…	To generate…
Once	A one-time report on the specified date for the current time period or for the specified number of past full weeks, months, quarters, or years.
Weekly	A weekly report on the specified date for the current week or for the specified number of past full weeks (Sunday through Saturday).
Monthly	A monthly report on the specified date

	for the current month or for the specified number of past full months.

b. **Date**: Choose the day of the week on which to generate the report. If you chose **Once** as the **Frequency** setting, choose the date on which to generate the report.

c. **Time**: Choose the time of day to generate the report.

d. **Group by**: Choose whether to group items in the report by protected computer or by protection group.

e. **Granularity**: Select **Weeks**, **Months**, **Quarters**, or **Years**. The **Granularity** setting is limited by the parameter you select in the **Frequency** box. For example, if you select a weekly frequency, you are limited to weekly granularity.

The following table explains how DPM interprets each unit of time.

Unit of Time	Definition
Week	Seven days—from Sunday through Saturday.
Month	A full month from the first to the last day of the month.
Quarter	Jan-Mar, Apr–Jun, Jul–Sept, or Oct–Dec.
Year	January 1 to December 31 of a particular year.

f. **Content**: Select the time period for which you want to include report data.

The term “Last” in the **Content** box is defined as the last full time period. For example, **Last 2 weeks** is defined as the past two full weeks excluding the current week. If today is a Tuesday, the last two weeks are the previous two full weeks (Sunday to Saturday). The time period covered for each report is displayed at the top of the report. The term “Current” is defined as the current time period even if it is only a partial time period.

g. **Number of copies to retain in history**: Select the number of reports you want to retain in history, up to a maximum of 18. When the number of reports saved equals the number specified in this box, the next saved report will replace the oldest copy of the report, so you can retain the maximum number of copies at all times.

6. Repeat Steps 2 through 5 for each report that you want to schedule.

See Also

How to Display Reports

How to Print Reports

How to Create or Modify Report Subscriptions
Report Types

How to Create or Modify Report Subscriptions

When you schedule reports, you can enable the option to send reports to subscribers via e-mail. Before you enable this option, you must specify the SMTP server that System Center 2012 – Data Protection Manager (DPM) will use to send reports.

Reports are sent through e-mail as file attachments. A subscriber cannot view an attached report unless the required software is installed on the destination computer. For example, if an administrator selects HTML as the report format, the browser on the destination computer must be able to display Internet Explorer version 4.0.1 or later. The following table provides the minimum software requirements for viewing reports sent by e-mail.

Report Format	Required Software
HTML	Internet Explorer 4.0.1 or later
Excel	Microsoft Office Excel 97 or later
PDF	Adobe Reader 4 or later

To subscribe to reports

1. In DPM Administrator Console, go to the **Reporting** view.
2. On the display pane, right-click the report to which you want to subscribe and click **Schedule**.

   Alternatively, you can right-click a report in the display pane and click **Schedule**.
3. On the **E-mail** tab, in the **Recipients** box, type the e-mail addresses of all the people or groups to whom DPM should send reports, and then click **OK**.
   a. Separate multiple e-mail addresses with commas.
   b. Enter only e-mail addresses that are valid on the designated SMTP server.
4. Select the HTML, Excel, or PDF report format, and click **OK**.
5. Repeat Steps 2 through 4 for each type of report that you want to distribute via e-mail.

To add a subscriber to an existing report subscription

1. In DPM Administrator Console, go to the **Reporting** view.
2. On the display pane, right-click the report for which you want to add e-mail recipients and click **Schedule**.

3. On the **E-mail** tab, in the **Recipients** box, add the subscriber to the list of recipients, separating it from the last entry by a comma, and then click **OK**.

To modify the report format for an existing report subscription

1. In DPM Administrator Console, go to the **Reporting** view.
2. On the display pane, right-click the report for which you want to modify the report format and click **Schedule**.
3. On the **E-mail** tab, in the **Report format** box, select the HTML, Excel, or PDF reort format, and then click **OK**.

See Also

How to Display Reports

How to Print Reports

How to Schedule Reports

Report Types

Using Reports

Setting System Options

Data Protection Manager (DPM) enables you to set or modify system options to comply with your data protection requirements and preferences.

In This Section

How to Enroll in the Customer Experience Improvement Program

How to Enable End-User Recovery

How to Modify the Auto Discovery Schedule

For information about subscribing to alerts and notifications and configuring the SMTP server, see Configuring the SMTP Server.

How to Enroll in the Customer Experience Improvement Program

After you enroll in the Customer Experience Improvement Program, DPM gathers anonymous information about your hardware, software configurations, and usage patterns of various DPM features and sends it to Microsoft. Microsoft uses this information to improve the quality,

reliability, and performance of Microsoft software. This program is optional and anonymous, and you can opt out at any time.

For more information, see the Microsoft Customer Experience Improvement Program privacy policy (http://go.microsoft.com/fwlink/?LinkID=84784).

To enroll in the Customer Experience Improvement Program

1. In the **Actions** pane, click **Options**.
2. On the **Customer Feedback** tab, click **Yes, I want to participate anonymously in this program (Recommended)** to enroll in the program.
3. If you do not want to enroll in the program, click **No, thank you**.
4. To apply your changes, click **OK**.

See Also

Setting System Options

How to Enable End-User Recovery

End-user recovery enables users to independently recover file data by retrieving recovery points of their files. Enabling end-user recovery involves configuring Active Directory Domain Services to support end-user recovery, enabling the end-user recovery feature on the DPM server, and installing the shadow copy client software on the client computers.

Important
DPM supports only short-term, disk-based recovery for end users.

The following procedures show you how to configure Active Directory Domain Services and enable end-user recovery of file data sources.

Note
Before users can begin independently recovering previous versions of their files, the DPM shadow copy client software must be installed on their computers. For more information, see How to Install the Shadow Copy Client Software.

To configure Active Directory Domain Services and enable end-user recovery on a DPM server if you are a schema and domain administrator in the domain

1. In DPM Administrator Console, click **Options** on the tool ribbon.
2. In the **Options** dialog box, on the **End-user Recovery** tab, click **Configure Active Directory**.
3. In the **Configure Active Directory** dialog box, select **Use current credentials** or type the user name and password for an account that has both schema and domain administrator privileges, and then click **OK**.

4. On the confirmation and notification prompts, click **Yes** and then click **OK**.
5. After configuration of Active Directory Domain Services is complete, select the check box for the **Enable end-user recovery** option and then click **OK**.

To configure Active Directory Domain Services and enable end-user recovery on a DPM server if you are not a schema and domain administrator in the domain

1. Direct a user who is both a schema and domain administrator to configure the Active Directory schema by running **<drive:>\Program Files\Microsoft Data Protection Manager\DPM\End User Recovery\DPMADSchemaExtension.exe** on a Windows Server 2003 computer that is a member of the same domain as the DPM server.

   Note
   If the protected computer and DPM reside in different domains, the schema needs to be extended by running the DPMADSchemaExtension.exe tool on the other domain.
2. In the **Enter Data Protection Manager Computer Name** dialog box, type the name of the computer for which you want end-user recovery data in Active Directory Domain Services, and then click **OK**.
3. Type the DNS domain name of the DPM computer for which you want end-user recovery data in Active Directory Domain Services, and then click **OK**.
4. In the **Active Directory Configuration for Data Protection Manager** dialog box, click **OK**.
5. In DPM Administrator Console, on the **Action** menu, click **Options**.
6. In the **Options** dialog box, on the **End-user Recovery** tab, select the check box for the **Enable end-user recovery** option, and then click **OK**.

See Also

How to Install the Shadow Copy Client Software

How to Modify the Auto Discovery Schedule

Once each day, DPM queries Active Directory Domain Services to discover new computers in your network.

Note
The default time for auto discovery is 1:00:00 A.M.

To modify the auto discovery schedule

1. In DPM Administrator Console, click **Options**.
2. In the **Options** dialog box, on the **Auto Discovery** tab, select the time of day when you

want auto discovery to run.

3. Click **OK**.

See Also

Setting System Options

Auto discovery

Optimizing Performance

DPM provides several ways to increase server performance expectations and optimize DPM performance. Network speed, the performance characteristics of the protected computer, the size of your protected data, and the rate at which the protected data changes can affect your actual results.

In This Section

How to Enable Computer-Level Network Bandwidth Usage Throttling

How to Enable On-the-Wire Compression

How to Stagger Synchronization Start Times

How to Manually Create a Replica

How to Create a Manual Replica for Application Servers

How to Modify the Schedule for Express Full Backups

How to Enable Computer-Level Network Bandwidth Usage Throttling

Network bandwidth usage throttling limits the amount of network bandwidth that DPM can use to create and synchronize replicas. Throttling helps to ensure that network bandwidth is available to applications other than DPM.

Network bandwidth usage throttling enables you to limit the amount of network resources a synchronization job can consume. However, network bandwidth usage throttling can lengthen the amount of time each synchronization job takes to complete.

By default, the throttling option is not selected.

To enable computer-level network bandwidth usage throttling

1. In DPM Administrator Console, go to the **Management** view.

2. Open the **Agent** workspace, and select the computer you want to throttle.
3. Click **Throttle computer**.
4. In the **Throttle** dialog box, check **Enable network bandwidth usage throttling**.
5. Select **Throttle Settings** and **Work Schedule** for the computer.

   Note
   You can configure network bandwidth usage throttling separately for work hours and nonwork hours, and you can define the work hours for the protected computer.
6. To apply your settings, click **OK**.

See Also

Optimizing Performance

How to Enable On-the-Wire Compression

Compression decreases the size of data being transferred during replica creation and synchronization and allows more data throughput with less impact to network performance. However, this option adds to the CPU load on both the DPM server and the protected computers. The amount of compression and improvement on network performance depends on workload.

Compression is enabled at the protection group level and applies to replica creation, synchronization, and consistency check operations. Recovery jobs also use compression.

To enable on-the-wire compression

1. In DPM Administrator console, go to the **Protection** view.
2. Click **Optimize performance**.
3. On the **Network** tab, check **Enable on-the-wire compression**.
4. To apply your changes, click **OK**.

See Also

Optimizing Performance

How to Stagger Synchronization Start Times

To optimize performance, you can offset the start time of synchronization jobs across different protection groups so that all of them do not start at the same time. Offsetting synchronization start times can also be used to optimize secondary protection of another DPM server.

To stagger synchronization start times

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display area, select a protection group.
3. Click **Optimize performance** on the tool ribbon.
4. On the **Network** tab, select the hours and minutes to offset the start of the synchronization job in the **Offset <time> start time by** field.

   Note
   The maximum allowed value for offset is the same as the synchronization frequency.
5. To apply your changes, click **OK**.

   Note
   Changing the start time offsets recovery points for files by the equivalent amount of time. This setting does not apply to protection groups for client computers.

See Also

Optimizing Performance

Synchronization

How to Manually Create a Replica

During creation of a protection group using the Create New Protection Group Wizard, DPM asks you to select a replica creation method to copy the data to be protected to the DPM computer. You can select **Automatically**, for which DPM copies the data across the network, or **Manually**. When you select manual replica creation, you must manually copy the data you want protected to the DPM computer using removable media.

To create a replica manually, you must know the details of the source path on the protected computer and the replica path on the DPM server. It is critical that you retain the same directory structure and properties (time stamps and security permissions) as those for the data that you are protecting.

Note
For large amounts of data, manual replica creation might provide faster performance than replication over the network.

To display the details of the source and replica paths

1. In DPM Administrator Console, go to the **Protection** view.
2. Select the data source you want to replicate on the DPM server.

3. Click **View Details** on the tool ribbon. The **Details of Replica Path** dialog box is displayed.
4. Copy the list view content for reference. To copy the replica path, select a row in the **Details of Replica Path** dialog box, and then press CTRL+C.

To copy data files from a protected computer to the DPM server

1. In the **Protection** view, select the protected data and then locate the **Replica path** in the **Details** pane.
2. In the **Details** pane, select the replica path and copy it into a text editor such as Notepad. The path will look like the following:

   <Drive:>\DPM\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\File System\D-87a82ad4-f9d2-11d9-b758-000d561ae74f\e55173e1-0b7a-4fa4-b4d1-387ac2b016b8\3ed60b1c-dcf8-442e-b441-d771a3d7f014\Users

   Note
   You cannot change the directory to this path in Windows Explorer because it is too large.
3. To access the Users folder, perform the following steps:
   a. At the command prompt, type **mountvol** and then press Enter.
   b. From the list of mounted volumes, pick the volume that corresponds to the appropriate path. The path will look like the following:

      \\?\Volume{a2072784-7573-4dce-a7e9-26713fd12697}

      <Drive:>\DPM\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\File System\D-87a82ad4-f9d2-11d9-b758-000d561ae74f
   c. Type the following to mount the volume to a drive letter:

      mountvol k:\ \\?\Volume{a2072784-7573-4dce-a7e9-26713fd12697}
   d. Click **Start**, double-click **My Computer**, and on the **Tools** menu, click **Folder Options**.
   e. In the **Folder Options** dialog box, on the **View** tab, in the **Advanced settings** box, under **Hidden files and folders**, clear the **Hide protected operating system files (Recommended)** option, click **Yes** to confirm that you want to display the files, and then click **OK**.

      Now you can browse to view the entire path from step 3 in Windows Explorer.
4. Manually copy the data to the Users folder under the drive letter you used to map the volume (K:\ in this example). Overwrite any data in the Users folder.
5. After you copy the data to the replica location, perform a synchronization with consistency check. Protection will start after the synchronization with consistency check has successfully completed.
6. At the command prompt, type the following to remove the drive letter that you used to mount the volume:

   mountvol k:\ /d

Note
In Windows Server 2008, run the command from an elevated command prompt.

See Also

New Protection Group Wizard

Optimizing Performance

Understand replicas

How to Create a Manual Replica for Application Servers

The following DPM procedure applies for applications such as SQL Server, Exchange Server, Windows SharePoint Services, and Virtual Server. However, you can also stop the application service, copy the files between the protected server and the destination (DPM) server, and then restart the application service. For applications such as Virtual Server, this might be a more efficient approach.

For Windows SharePoint Services, the following data sources are copied:

- All of the SQL databases—configuration database, content databases, security support provider databases, and the search database.
- Search indexes, if you have enabled a search service or server.

To create a manual replica for application servers

1. Use the specific application administrator console to determine the location of the data files for the data source you are protecting. For example, use SQL Management Studio for Microsoft SQL Server 2005 databases.
2. Use the native backup tool to back up the data files of the data source. In Windows Server 2003, click **Start**, click **Run**, and then enter **ntbackup**.

   You should perform a file-level backup and not an application backup. For example, back up the Exchange log and databases as files and not as an application.

   Important
   Use the Volume Shadow Copy Service (VSS) parameter of the Ntbackup tool to ensure that the file backup includes recovery points. The parameter is */SNAP:on*.
3. In DPM Administrator Console, go to the **Protection** view.
4. In the display pane, select a data source.
5. In the **Details** pane, click **Click to view details**. The **Details of Replica Path** dialog box displays the original path of the data files on the protected server and the target path where this data should be copied.

6. Use Ntbackup to restore the data files to the corresponding paths on the DPM server to create the manual replica.
7. When you have copied the data to the DPM Server from DPM Administrator Console, go to the **Monitoring** view and then open the **Alerts** workspace.
8. In the **Manual Replica Creation Pending** alert, you can choose to run a consistency check job.

   Note
   You can also run a consistency check job in the **Protection** area of the navigation pane for this data source.

See Also

[About the Details of Replica Path Dialog Box]
[Optimizing Performance]

About the Details of Replica Path Dialog Box

When you create a manual replica for application servers, DPM displays a **Details of Replica Path** dialog box. The path defined under the **Destination (DPM Server)** column in the **Details of Replica Path** dialog box corresponds to the volume root of each corresponding data file on the source protected server. You must re-create the folder hierarchy under this volume root so that the folder hierarchy under the specified DPM replica path is the same as the relative path/folder hierarchy under the volume root of the protected server. This must be done for each data file that is part of the data source.

If the SQL database files are located under G:*Dir*, the files are named G:*Dir**Dir*.mdf and G:*Dir**Dir*_log.ldf. Using this example, the **Details of Replica Path** dialog box displays the following paths.

Source—Protected Server	Destination—DPM Server
`G:\on widgets.corp.microsoft.com`	`C:\Program Files\Microsoft DPM\DPM\Volumes\Replica\widgets.corp.microsoft.com\SqlServerWriter\Dir\5f933057-a1fa-432c-9c2f-86d64e91e21f\Full\G-Vol\`

To perform a manual load, copy **dir\dir.mdf** and **dir\dir_log.ldf** under the path so that the final paths are as follows:

Database:

C:\Program Files\Microsoft DPM\DPM\Volumes\Replica\widgets.corp.microsoft.com\SqlServerWriter\Dir\5f933057-a1fa-432c-9c2f-86d64e91e21f\Full\G-Vol\dir\dir.mdf

Log:

C:\Program Files\Microsoft DPM\DPM\Volumes\Replica\widgets.corp.microsoft.com\SqlServerWriter\Dir\5f933057-a1fa-432c-9c2f-86d64e91e21f\Full\G-Vol\dir\dir_log.ldf

For more information about how to use specific application administrator consoles, see the following links:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008

See Also

How to Create a Manual Replica for Application Servers

How to Modify the Schedule for Express Full Backups

To provide quick recovery of application data, DPM must create an express full backup periodically. The express full backup operation typically increases the demand on the server's resources by 5 percent for several minutes. To reduce the demand on the server's resources, you can schedule fewer express full backups, but this can increase data recovery time.

Note
You can modify the schedule for express full backups only for applications that are part of a protection group. For files that are part of a protection group, use the Create New Protection Group Wizard to specify your short-term backup objective.

To modify the schedule for express full backups

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, select a protection group for which you want to modify the express full backup schedule.
3. Click **Optimize performance** on the tool ribbon.
4. On the **Express Full Backup** tab, select the available times for the express full backups

and click **Add**.

5. Select the days of the week for the express full backups.
6. To apply your changes, click **OK**.

Note
To modify the express full backup, you need to use the **Modify protection group** wizard.

See Also

Optimizing Performance

DPM Wizards

DPM provides wizards for the following areas of functionality:

- Creating a new protection group
- Installing a protection agent
- Recovering data

These wizards change dynamically depending on the type of data sources you are protecting and recovering.

In This Section

New Protection Group Wizard

Protection Agent Installation Wizard

Recovery Wizard

New Protection Group Wizard

The Create New Protection Group Wizard guides you through the process of protecting your data both for servers and client computers. You can create two kinds of protections groups:

Servers. Select this option for backing up file servers and application servers.

Clients. Select this option for backing up data from laptops and desktops.

Protection group creation involves making a series of decisions about how you want to configure the group. These decisions are provided in the following table:

Server	Clients
• Selecting the data you want to protect.	• Selecting the computers you want to

Server	Clients
• Selecting the kind of protection method that you want. • Specifying your recovery goals. • Allocating space on the storage pool for replicas and recovery points. • Specifying library and tape details. • Specifying when and how replica creation will occur. • Specifying performance improvement methods.	backup. • Specifying the template for inclusion and exclusion from backups. • Selecting the kind of protection method that you want. • Specifying synchronization and recovery goals. • Allocating space on the storage pool for replicas and recovery points. • Specifying library and tape details. • Specifying performance improvement methods.

Throughout the protection group creation process, the wizard provides default options that you can override if you select. If you have questions at any point in the process, click **Help**.

For guidelines for creating protection groups, see Planning Protection Groups.

See Also

Server Computers

Client Computers

What Is a protection group?

Working with Protection Groups

Server Computers

The Create New Protection Group Wizard guides you through the process of protecting your data on server computers. Select the **Servers** option in the **Select Protection Groups Type** page for backing up file servers and application servers.

In This Section

Welcome

Select Protection Group Type

Select Group Members

Select Data Protection Method

Specify Exchange Protection Options

Specify Exchange DAG Protection

Specify Short-Term Goals

Specify Short-Term Protection

Review Disk Allocation

Specify Long-Term Goals

Select Library and Tape Details

Choose Replica Creation Method

Choose Consistency Check Options

Specify online protection data

Specify online protection goals

Summary

Status

See Also

Working with Protection Groups

What Is a protection group?

Welcome

The **Welcome** page provides an overview of how DPM protects data. Use the **Welcome** page of the Create New Protection Group Wizard to begin creating a protection group.

This page contains the elements described in the following table.

Elements

Name	Description
Do not show this Welcome page again	Select if you do not want the wizard to display the **Welcome** page when you create protection groups in the future.

To proceed with the installation, click **Next**.

See Also

New Protection Group Wizard

Select Protection Group Type

Use the **Select Protection Group Type** page of the Create New Protection Group Wizard to select the type of computers that you want to protect. You can use the **Servers** option to backup up file servers and application servers and the **Clients** option for backing up data from laptops and desktops.

This page contains the elements described in the following table.

Elements

Name	Description
Servers	Select this option for backing up file servers and application servers. You must select this option, if you want to use Windows Azure Online Backup.
Clients	Select this option for backing up data from laptops and desktops.

After selecting a protection group type, click **Next**.

See Also

New Protection Group Wizard

Select Group Members

Use the **Select Group Members** page of the Create New Protection Group Wizard to select the data sources you want to protect. For guidelines for creating protection groups, see Planning Protection Groups.

Note
The computers that contain the members that DPM will protect must meet the protected computer requirements. For information about the protected computer software requirements, see Protected Computer Requirements.

This page contains the elements described in the following table.

Elements

Name	Description
Available members	Expand the computer nodes to display the available data sources on each computer. Place a check mark in the box next to each data source that you want to include in the protection group. As you select data sources, your selections appear in the **Selected members** box. **Note** In SQL, by default auto-protection is turned on when you select an entire instance of SQL Server. This auto-protection setting causes new databases that are added to the instance of SQL Server to be automatically protected. To turn off auto-protection, right-click the selected instance of SQL Server and then click **Turn off auto protection**. For more information about SQL Server instance auto-protection, see Adding Databases to a SQL Server.
Remove	Click to remove selected data sources from the **Selected members** box.
View	Click to view a list of excluded folders.
Exclude Files	Click to exclude file types.

Note
DPM does not support protection of some types of files and displays a warning of unsupported data in these cases. For more information about how to list the file types that DPM does not support, see the "How to display warnings for unsupported data" procedure in How to Check Data Protection Job Status.

Note
DPM does not protect reparse points found in file systems or in application paths. If you have selected volumes, folders or applications in this protection group, DPM will protect all data except the reparse points. For more information about data types that are not protected, see Unsupported Data Types.

After selecting the members for the protection group, click **Next**.

Selecting virtual machines for protection

If you are protecting clustered virtual machines, you can choose the virtual machine protection in two ways:

- First expand all the host computers and wait for the inquiry to finish. Then expand cluster node and select the virtual machines you want to protect.
- Expand the cluster node , then expand one virtual machine under a host computer and wait for inquiry to finish. Then expand other virtual machines under the same host.

See Also

New Protection Group Wizard

Exclude File Types

Exclude Folders

Exclude Folders

Use the **Exclude Folders** dialog box to view excluded folders from the protection group.

This page contains the elements described in the following table.

Elements

Name	Description
Exclude folder list	Lists the folders excluded from the protection group. You cannot exclude folders in the **Exclude Folders** dialog box. To exclude a folder, click **OK** to return to the **Select Group Members** page. Ensure that the parent of the folder that you do not want protected is selected, and then clear the check box of the folder that you do not want protected.

After viewing the excluded folders, click **OK**.

See Also

New Protection Group Wizard

Select Group Members

Exclude File Types

Use the **Exclude File Types** dialog box to exclude files from protection by file name extension.

This page contains the elements described in the following table.

Elements

Name	Description
File types to exclude	Type the file types you want to exclude from protection, and then click **OK**. Use a comma to separate multiple file types—for example, .doc, .jpg, .bmp. **Note** Exclusion by file name extension will apply to all members of the protection group.

See Also

New Protection Group Wizard

Select Group Members

Select Data Protection Method

Use the **Select Data Protection Method** page of the Create New Protection Group Wizard to select how you want to protect your data. You can select short-term protection using either disk or tape, and you can select long-term protection using only tape.

This page contains the elements described in the following table.

Elements

Name	Description
Protection group name	Accept the default name, or type a new name for the protection group.
I want short-term protection using:	For servers:

Name	Description
	Select this check box for short-term protection, and then select the media you want to use from the drop-down list. **Important** If you do not have a tape library attached to the DPM server, only **Disk** is available for short-term protection For client computers Select this check box for short-term protection. **Important** For client computers, only disk-based short-term protection is available.
I want long-term protection using tape	Select this check box for long-term protection using tape. **Important** When protecting servers, if you are using tape for both short-term and long-term protection, DPM creates copies of the latest short-term tape full backup to generate your long-term tape backup. Therefore, we recommend that you schedule your short-term protection full backup to run a day prior to your long-term protection. This enables your long-term tape backup to leverage the short-term tape backup that DPM created the day before. If you schedule the long-term tape backup to run prior to the short-term tape backup, the long-term backup will not leverage the latest short-term full backup.
I want online protection	Select this to enable Windows Azure Online Backup for the protection group. **Important** You must select **I want short-term protection using:** with **Disk** before you select this option.

After selecting a name and a protection method for the protection group, click **Next**.

See Also

New Protection Group Wizard

Specify Exchange Protection Options

Use the **Specify Exchange Protection Options** page of the Create New Protection Group Wizard to specify whether you want to check the integrity of the Exchange Server databases and to select the cluster node that you want to protect.

For information about managing Exchange Server clusters, see Managing Protected Servers Running Exchange.

This page contains the elements described in the following table.

Elements

Name	Description
Run Eseutil to check data integrity	Click this check box to check the integrity of the Exchange Server databases. The Exchange Server Database Utilities (Eseutil.exe) must be installed on the protected server for tape-based protection. For disk-based protection, you must also install Eseutil.exe on the DPM server. For more information about Eseutil.exe, see Eseutil.
Protect active node	This option applies only for Exchange Server 2007 CCR. Click this option to select the active node as the node that DPM will protect.
Protect passive node	This option applies only for Exchange Server 2007 CCR. Click this option to select the passive node as the node that DPM will protect. If the passive node is not available, select the node that you want to fail over to from the drop-down list.
Protect only the specified node	This option applies only for

Name	Description
	Exchange Server 2007 CCR. Click this option to specify the node that you want DPM to protect, and then select the protection node from the drop-down list.
Run for both database and log files (may be slow if databases are large)	This check box applies only for Exchange Server 2010 and is recommended when protecting stand-alone servers.
Run for log files only (Recommended for DAG servers)	This check box applies only for Exchange Server 2010 and is recommended when protecting DAG servers.

After specifying the Exchange Server protection options for the data sources, click **Next**.

See Also

New Protection Group Wizard

Specify Exchange DAG Protection

Use the **Specify Exchange DAG Protection** page of the Create New Protection Group Wizard to select the databases for copy backup and express full backup. For protecting multiples copies of the same database, select only one database for express full and incremental backup and then select the remaining copies for copy backup.

This page contains the elements described in the following table.

Elements

Name	Description
Database copies selected for Full Backup	As you select the databases for full backup your selections appear in the **Database copies selected for Full Backup** box.
Database copies selected for Copy Backup	As you select the databases for copy backup your selections appear in the **Database copies selected for Copy Backup** box.
Copy >	Click to select the databases for **Copy Backup**.
< Full	Click to select the databases for **Full Backup**.

After selecting the databases for the protection group, click **Next**.

See Also

New Protection Group Wizard

Specify Short-Term Goals

Use the **Specify Short-Term Goals** page of the Create New Protection Group Wizard to generate your short-term disk-based recovery goals.

This page contains the elements described in the following table.

Elements

Name	Description
Retention range	Type or select how long you need your backed-up data available. You can select a retention range between 1 and 64 days for short-term disk-based protection.
Synchronization frequency: Every	Click this option to select how often you want to synchronize the replica on your DPM server with the changes on your protected computer. You can select a synchronization frequency interval of anywhere from 15 minutes to 24 hours. The default behavior is every 15 minutes, which means that the DPM server will never be more than 15 minutes behind the computer it is protecting. The average Recovery Point Objective (RPO) is 15 minutes from any event that critically impacts the computer or disk.
Synchronization frequency: Just before a recovery point	Click this option to synchronize the data just before a scheduled recovery point. **Note** The network traffic is potentially greater at the time of synchronization when you

Name	Description
	select this option. For more information about synchronization, see Managing Performance.
Recovery points for files: Modify	Click **Modify** to change the recovery point schedule for file data. Recovery points for files are created according to the schedule you configure. For file protection, you select the days and times that you want DPM to create your recovery points to accommodate your business needs and recovery requirements.
Application recovery points	Recovery points for application data is based on the synchronization frequency when incremental backup is supported. For data protection of applications that do not support incremental backups, for example SQL Server databases using the simple recovery model, the express full backup schedule determines the recovery point schedule
Express full backup: Modify	Click **Modify** to change the express full backup schedule. To enable faster recovery time, DPM regularly performs an express full backup, a type of synchronization that updates the replica to include the changed blocks. **Note** Performing frequent express full backups may impact performance on the production server. For more information about express full backups, see "Express full backups" in Managing Performance. For application data protection, the recovery point schedule is based on the synchronization frequency for incremental backups. If incremental backups are not supported, the recovery points are based on the express full backup schedule.

After specifying your short-term recovery goals for the protection group, click **Next**.

See Also

New Protection Group Wizard

Specify Short-Term Protection

Use the **Specify Short-Term Protection** page of the Create New Protection Group Wizard to generate your short-term tape-based recovery goals.

This page contains the elements described in the following table.

Elements

Name	Description
Retention range	Type or select how long you need your backup data available. You can select a retention range between 1 and 12 weeks for short-term tape-based protection.
Frequency of backup	Select how often you want to back up your data. You can select a backup frequency of daily, weekly, or biweekly depending on your retention range.
Backup mode	Select your backup type. For tape-based backup, instead of recovery points, you configure your type of backup as follows: • Full and incremental backups (Available only when you select a daily backup frequency). **Important** If you select this backup type, the retention range will be longer than the one you specified (up to a maximum of 1 week) because of a dependency between full and incremental backups. • Full backup only

Name	Description
	For more information about full and incremental backups, see Defining Recovery Goals.
Full backup time	Select your daily backup schedule. When you select daily full backups, you specify the time. When you select weekly or every two weeks, only full backup is available.
Full backup days	Select your daily backup schedule. When you select daily full backups, you specify the day. When you select weekly or every two weeks, only full backup is available.
Incremental backup time	Available only when you select daily full and incremental backups. Specify the time for the full backup and for the incremental backup.
Incremental back days	Available only when you select daily full and incremental backups. Specify the days for the full backup and for the incremental backup. You can select the days that you want DPM to create your recovery points to accommodate your business needs and recovery requirements. **Note** You must select at least two days for daily backups. Incremental backup cannot be scheduled on days of full backups.

After specifying your short-term protection on tape for the protection group, click **Next**.

See Also

New Protection Group Wizard

Review Disk Allocation

Use the **Review Disk Allocation** page of the Create New Protection Group Wizard to review and change the space allocations on the storage pool for the replicas and recovery points that DPM recommends for the protection group. Space is also allocated on protected file servers and workstations for the change journal.

We recommend that you accept the default space allocations that DPM recommends unless you are certain that they do not meet your needs. Overriding the default allocations can result in allocation of too little or too much space. For information about how DPM allocates disk space, see Allocating Space for Protection Groups.

This page contains the elements described in the following table.

Elements

Name	Description
Modify	Click **Modify** to change the disk space allocation on the DPM server and the protected computer, or to specify a custom volume.
Collocate data in DPM Storage Pool	Select this check box for co-locating data to enable DPM to protect more number of data sources per replica volume.
Automatically grow volumes	Select this check box to automatically allocate volumes when more disk space is required for protecting the selected data source for the specified retention range. DPM automatically grows the volumes by 25% when the used disk space is more than 90%.

After reviewing the disk allocations for the protection group, click **Next**.

See Also

New Protection Group Wizard

Co-Locating Data

Modify Disk Allocation - DPM Server Tab

Modify Disk Allocation - Protected Computer Tab

Modify Disk Allocation - DPM Server Tab

On the **DPM Server** tab on the **Modify Disk Allocation** screen, you can change the space allocations that DPM recommends for the protection group.

For information about allocating disk space, see Planning Protection Groups.

This page contains the elements described in the following table.

Elements

Name	Description
Storage Type	Select the storage location. Your options are **Storage pool** or **Custom volume**.
Replica Volume	Type the disk space for the replica volume, or select the custom volume to use for the replica volume.
Recovery Point Volume	Type the disk space for the recovery point volume, or select the custom volume to use for the recovery point volume.
Custom Volume	Select the custom volume. Any volume that is attached to the DPM server can be selected as a custom volume except the volume that contains the system and program files **Note** DPM cannot manage the space in custom volumes. If DPM alerts you that a custom replica volume or recovery point volume is running out of space, you must manually change the size of the custom volume by using Disk Management.
Calculate	Click this link to calculate the data size for the data source.

After modifying the disk allocations for the protection group, click **OK**.

See Also

New Protection Group Wizard

Modify Disk Allocation - Protected Computer Tab

On the **Protected Computer** tab on the **Modify Disk Allocation** screen, you change the space allocations that DPM recommends for the protected computer.

For information about allocating disk space, see Planning Protection Groups.

This page contains the elements described in the following table.

Elements

Name	Description
Space Allocated	Type the disk space you want to allocate on the protected computers for the change journal.

After modifying the disk allocations for the protection group, click **OK**.

See Also

New Protection Group Wizard

Specify Long-Term Goals

Use the **Specify Long-Term Goals** page of the Create New Protection Group Wizard to generate your long-term recovery goals.

For information about recovery point schedules for long-term protection, see Planning Protection Groups.

This page contains the elements described in the following table.

Elements

Name	Description
Retention range	Type or select how long you need your backed-

Name	Description
	up data available. You can select a retention range between 1 and 99 years.
Frequency of backup	Select the backup frequency that you want. The backup frequency is based on the specified retention range, as shown in the following list: • When the retention range is 1–99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly. • When the retention range is 1–11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly. • When the retention range is 1–4 weeks, you can select backups to occur daily or weekly  **Note** On a stand-alone tape drive, for a single protection group, DPM uses the same tape for daily backups until there is insufficient space on the tape. For multiple protection groups, DPM requires separate tapes. Therefore, we recommend that you minimize the number of protection groups that you create if you are using a stand-alone tape drive for your backups.
Recovery points	Lists the recovery point schedule. Each express full backup creates a recovery point for application data. If the application supports incremental backups, each synchronization also creates a recovery point.
Restore Defaults	Click to restore the defaults back to a three month retention range and a weekly backup frequency.
Customize	Click to change the tape label and to customize the schedule of backup jobs for your recovery goals. This schedule will replace the default schedule.

Name	Description
Modify	Click to modify the long-term backup schedule. You have a number of scheduling options for long-term protection, depending on your retention range and backup frequency. If the frequency of backup is set as daily, then you can select the days that you want DPM to create your recovery points to accommodate your business needs and recovery requirements. **Important** You must select at least two days for daily backups.

After specifying your long-term recovery goals for the protection group, click **Next**.

See Also

New Protection Group Wizard

Customize Recovery Goal screen

Use the **Customize Recovery Goal** screen to customize the schedule of backup jobs for your recovery goals. When you customize the schedule of backup jobs for a protection group, you specify a recovery goal for each backup interval. You can specify a recovery goal for up to three backup frequency intervals.

This screen contains the elements described in the following table.

Elements

Name	Description
Backup every	Specify a daily, weekly, monthly or yearly backup frequency interval. **Note** By default, when customizing the recovery goal, the number of days for backups is one day. To select more than one day, use the **Modify** button in

Name	Description
	the **Select Long-Term Goal** page. You must select at least two days for daily backups.
Retention range	Specify the retention range for the tape.
Number of backup copies	Specify the number of copies of the tape that you want make.
Tape Label	Select the tape label, and then click the tape label again to edit the label.
Run backup for all (ignore overlap of days).	Click to run a backup for all the frequency intervals if any of the backups fall on the same day.
Run backup only for the recovery goal with the longest retention range.	Click to run the backup with the longest retention range only if any of the backups fall on the same day.

After customizing the protection goals, click **OK**.

See Also

New Protection Group Wizard

Specify Long-Term Goals

Modify Long-Term Backup Schedule

Use the **Modify Long-Term Schedule** screen to change your long-term backup schedule. The scheduling options you can modify for long-term protection depend on your retention range and backup frequency.

This page contains the scheduling options for long-term protection.

Elements

Backup frequency	Scheduling options
Daily	• Time for daily backup. • Day of week and time for monthly backup.

Backup frequency	Scheduling options
	• Date and time for yearly backup.
Weekly	• Day of week and time for weekly backup. • Day of week and time for monthly backup. • Date and time for yearly backup.
Biweekly	• Day of week and time for biweekly backup. • Day of week and time for monthly backup. • Date and time for yearly backup.

Monthly	• Date and time for monthly backup (monthly backups are performed on the specified day of the month).
	  • Examples:
	  • If on Jan 10 you schedule a monthly backup to run on the 15th day of the month, the first backup will happen on January 15.
	  • If on Jan 10 you schedule a monthly backup to run on the 5th day of the month, then the first backup will happen on Feb 5.
	• If you schedule a monthly backup within 24 hours from the current time and date, then the first backup will happen the next month on the specified day.
	Example:
	If on Jan 10 3:00 P.M. you schedule a monthly backup to run on the 11th day of the month at 10:00 A.M., then the first backup will happen on Feb 11 10:00 A.M. and then every month thereafter.

Quarterly	• Date and time for quarterly backup (quarterly backups are performed in January, April, July, and October on the specified day of the month).
	  • Examples:
	  • If on Jan 10 you schedule a quarterly backup to run on the 15th day of the month, the first backup will happen on January 15 and

Backup frequency	Scheduling options
	every three months thereafter. • If on Jan 10 you schedule a quarterly backup to run on the 5th day of the month, then the first backup will happen on April 5 and then every three months thereafter. • If you schedule a quarterly backup within 24 hours from the current time and date, then the first backup will happen the next quarter on the specified day and every three months thereafter. Example: If on Jan 10 3:00 P.M. you schedule a quarterly backup to run on the 11th day of the month at 10:00 A.M., then the first backup will happen on April 11 at 10:00 A.M. and then every three months thereafter.
Half-yearly	• Date and time for half yearly backup (half yearly backups are performed two times in a year on the specified month and date). • Examples: • If on January 10 2009 you schedule a half yearly backup to run on the January 15, then the first backup will happen on January 15 2009 and then every six months thereafter. • If on January 10 2009 you schedule a half yearly backup to run on the January 5, then the first backup will happen on July 5 2009 and then every six months thereafter. • If you schedule a half yearly backup within 24 hours from the current time and date, then the first backup will happen after six months on the specified month and date and then every six months thereafter. • Example: • If on January 10 2009 3:00 P.M.

Backup frequency	Scheduling options
	you schedule a half yearly backup to run on the January 11 at 10:00 A.M., then the first backup will happen on July 11 2009 at 10:00 A.M. and then every six months thereafter.

Yearly	• Date and time for yearly backup (yearly backups are performed one time in a year on the specified month and date).
	  • Examples:
	  • If on January 10 2009 you schedule a yearly backup to run on the January 15, then the first backup will happen on January 15 2009 and then every year thereafter.
	  • If on January 10 2009 you schedule a yearly backup to run on the January 5, then the first backup will happen on January 5 2010 and then every year thereafter.
	• If you schedule a yearly backup within 24 hours from the current time and date, then the first backup will happen the next year on the specified month and date and every year thereafter.
	  • Example:
	  • If on January 10 2009 3:00 P.M. you schedule a yearly backup to run on the January 11 at 10:00 A.M., then the first backup will happen on January 11 2010 at 10:00 A.M. and then every year thereafter.

After modifying the long-term backup schedule, click **OK**.

See Also

New Protection Group Wizard

Specify Long-Term Goals

Select Library and Tape Details

Use the **Select Library and Tape Details** page of the Create New Protection Group Wizard to specify the number of copies that you need and how many tapes you want to allocate for long-term protection. You also specify whether you want DPM to encrypt and compress the data, and whether you want to check the backup for data integrity.

This wizard page contains the elements described in the following table.

Elements

Name	Description
Library	Select the library that you want to use for your tape backups.
Drives allocated	Type or select the number of drives you want to allocate for the tape backups.
Copy library	Select the library you want to use for multiple backup copies. **Note** Use **Copy library** only if you specified that you wanted multiple tape backup copies. If did not specify multiple copies, accept the default library (same as the primary **Library**).
Check backup for data integrity	Click this check box to check for data integrity between the backup copy versions.
Compress data	Click this option to enable data compression on tape.
Encrypt data	Click this option to encrypt the data before it is written to tape.
Do not compress or encrypt data	Click this option if you do not want DPM to perform data compression or encryption.

After specifying the library and tape details for the protection group, click **Next**.

See Also

New Protection Group Wizard

Choose Replica Creation Method

Use the **Choose Replica Creation Method** page of the Create New Protection Group Wizard to select how you want to create the replica for each protected volume in the protection group. In DPM, a replica is a full copy of the protected data on a single volume.

This page contains the elements described in the following table.

Elements

Name	Description
Automatically	Select this option to have DPM replicate the data across the network.
Now	Select this option to have DPM immediately begin copying the data from the computers you are protecting to the DPM server.
Later	Select this option to schedule the initial copy at a later time—most probably after business hours.
Manually	Select this option to use tape, USB storage, or other portable media to transfer the baseline data to the DPM server. This is the preferred option when synchronizing large amounts of data across a slow WAN connection for the first time. For more information about manual replica creation, see Creating Replicas Manually.

After specifying your replica creation method for the protection group, click **Next**.

See Also

New Protection Group Wizard

Choose Consistency Check Options

Use the **Consistency check options** page of the Create New Protection Group Wizard to run consistency check on inconsistent replicas.

This wizard page contains the elements described in the following table.

Elements

Name	Description
Run a consistency check if a replica becomes inconsistent	Click this check box to allow DPM to run consistency check automatically if the replica is inconsistent.
Run a daily consistency check according to the following schedule	Click this check box to run a daily consistency check according to the selected schedule.
Start time	Select the time to run a daily scheduled consistency check.
Maximum duration	Select the maximum time that is needed for running a daily consistency check.

After specifying the consistency check options for the protection group, click **Next**.

See Also

New Protection Group Wizard

Consistency check

Specify online protection data

Use the Specify Online Protection Data page to select the data sources in the protection group that must be protected online. Currently DPM supports online protection only for file servers and Hyper-V virtual machines. All other data sources will be grayed out.

Specify online protection goals

Use the **Specify Online Protection Goals** page to generate your online recovery goals.

Elements

Name	Description
Retention range	Type or select how long you need your backed-up data available online. You can select a retention range between 1

Name	Description
	and 30 days for short-term disk-based protection.
Synchronization frequency	Select **Daily** or **Weekly** based on the frequency you want to set.
Synchronization Schedule	You can set synchronization to happen two times in a day. Select the times are which you want the synchronization jobs to run and move then to the **Scheduled time** box. These settings will also decide when your initial replication will happen. Ensure that your settings synchronize with your throttling schedule. **Note** The number of recovery points is no longer limited to two per day. You can have up to 120 recovery points at any given point of time. For more information see, Calculating maximum number of recovery points.

After specifying your online protection goals for the protection group, click **Next**.

Calculating maximum number of recovery points

DPM allows you to store up to 120 recovery points. Here are a few examples to show how DPM calculates how many recovery points you can create.

The maximum permitted number of backups in a day can be calculated as:

Number of backups in a day (N) = 120 / Maximum number of days on which backups are taken in the retention range (M)

If you are taking daily backups and have a retention range of 10 days, then M is 10 since within a window of 10 days you will get 10 backups since one is taken every day. This means you can take a maximum of 12 backups one each day.

If you are taking backups on five days of a week with retention range of 10 days, M in this case is eight since in a 10-day window the least number of days on which a backup is not taken is two. So you can schedule up to 15 backups per day.

Summary

Use the **Summary** page of the Create New Protection Group Wizard to confirm the settings of your protection group.

This page lists the settings you have selected. Confirm that the settings are correct, and then click **Create Group** to create the protection group. To change the settings, click **Back**.

Note that if you are modifying a protection group the following jobs will be canceled. For more information about jobs that are canceled when you modify a protection group, see Managing Performance.

Servers

Replication jobs	Archive jobs
Configure protection	Short-term and Long-term archive
Synchronization	Data set copy
Consistency check	Data set verification
Shadow copy	Recovery from tape
Initial replication	
Recovery from shadow copy	

Clients

Replication jobs	Archive jobs
Configure protection	Short-term and Long-term archive
Shadow copy	Data set copy
Recovery from shadow copy	Data set verification
	Recovery from tape

See Also

New Protection Group Wizard

Status

Use the **Status** page of the Create New Protection Group Wizard to view the status of the tasks that DPM is performing. If all tasks succeed, the protection group is created. If a task fails, click the **Errors** tab for more information.

1. To exit the wizard, click **Close**.
2. To view the status of replica creation and synchronization jobs for the new protection group, go to the **Monitoring** view, and then open the **Jobs** workspace.

See Also

New Protection Group Wizard

Client Computers

Select the **Clients** option in the **Select Protection Group Type** of the Create New Protection Group Wizard to backup data from client computers - laptops and desktops.

For guidelines for creating protection groups, see Planning Protection Groups.

In This Section

Select Group Members

Specify Protection Rules

Select Short-Term Goals

Allocate Storage

Select Group Members

Use the **Select Group Members** page of the Create New Protection Group Wizard to select the client computers you want to protect.

This page contains the elements described in the following table.

Elements

Name	Description
Computer name	On the Select Group Members page, select the computers you want to protect from the list box.

Name	Description
	 **Important** Computers across domains are not listed in the Computer name box. To find a computer across a trusted domain, you must type the fully qualified domain name of the computer you want to protect (for example, Computer1.Domain1.corp.microsoft.com, where Computer1 is the name of the target computer that you want to protect, and Domain1.corp.microsoft.com is the domain to which the target computer belongs).
Add	Click **Add** to move the computers to the **Selected computers** list box. As you add the computers, your selections appear in the **Selected computers** list box.
Remove	Click **Remove** to remove the computers from the Selected computers list box.
Add Multiple Computers	If you want to add multiple computers, you can create a .txt file containing the computers you want to add. To add the computers, click **Add Multiple Computers**. You must enter each computer in the file on a new line. We recommend that you provide the fully qualified domain name (FQDN) of the target computers. For example, enter multiple computers in a .txt file as Computer1.Domain1.corp.microsoft.com, Computer2.Domain1.corp.microsoft.com, Computer3.Domain2.corp.microsoft.com.

After selecting the computers for the protection group, click **Next**.

See Also

New Protection Group Wizard

Add From File

To add multiple computers from the Select Group Members page in Create New Protection Group Wizard, use the **Add From File** dialog box to upload the .txt file that contains names of the all computers that you want to add.

We recommend that you provide the fully qualified domain name (FQDN) of the target computers. For example, enter multiple computers in a .txt file as follows:

Computer1.Domain1.corp.microsoft.com

Computer2.Domain1.corp.microsoft.com

Computer3.Domain1.corp.microsoft.com

This page contains the elements described in the following table.

Elements

Name	Description
Text file location	The location of the text file (.txt) that contains names of all the computers that you want to add.

After selecting the text file (.txt), click **OK**.

See Also

New Protection Group Wizard

Select Group Members

Specify Protection Rules

Use the **Specify Inclusions and Exclusions page** page of the Create New Protection Group Wizard to specify the folders to include or exclude for protection and file types that you want to exclude on the selected computers.

This page contains the elements described in the following table.

Elements

Name	Description
Enter the Folder Path	Specify the folders to include or exclude for

Name	Description
	protection on the selected computers from the drop-down list box or type in the specific paths. Type the folder names in the **Folder** column using variables such as %programfiles%, or you can use the exact folder name.
Rule	Select the **Include** or **Exclude** option for each entry in the **Rule** column. To automatically back up a folder from the selected computers, select the **Include** option. To disallow backup of folders from the selected computers, select the **Exclude** option. **Important** If you have folder a selected with the **Exclude** option that has a subfolder selected with the **Include** option, no data is backed up. However, if you have selected a folder that has the **Include** option that has a subfolder selected with the **Exclude** option, the folder will be backed up but its subfolder will not be backed up.
Add Rows	Click **Add** to add a new rule for folder inclusions and exclusions to the drop-down list box.
Remove Rows	Click **Remove** to remove selected rules or typed paths from the drop-down list box.
Allow users to specify protection members	Click this check box to let your end users add more folders on the computer that they want to backup. **Note** To enable this check box, you must select at least one folder that has the **Include** option set in the **Rule** column.
File type exclusions	Under **File type exclusions**, type the file types to exclude using their file name extensions separated by commas. **Note**

Name	Description
	The selected file types will not be backed up even if they are included in a folder that has the **Include** option or in a folder added by end-users.

After specifying the folders to include or exclude for protection and file types that you want to exclude on the selected computers, click **Next** to continue.

See Also

New Protection Group Wizard

Select Short-Term Goals

Use the **Specify Short-Term Goals** page of the Create New Protection Group Wizard to generate your short-term disk-based recovery goals.

This page contains the elements described in the following table.

Elements

Name	Description
Retention range	Type or select how long you need your backed-up data available. You can select a retention range between 1 and 64 days for short-term disk-based protection.
Synchronization frequency: Every	Select how frequently you want the client computers to synchronize data automatically to the DPM server replica. You can select a synchronization frequency interval between 1 hour to 24 hours. The default behavior is every 4 hours. This means that the selected client computers will automatically try to synchronize if the last successful synchronization happened more than 4 hours ago.
Recovery points for client computers:	Click **Modify** to change the recovery point

Name	Description
Modify	schedule for client computer data. Recovery points are created according to the schedule you configure. For client computer protection, you select the days and times that you want DPM to create your recovery points to accommodate your business needs and recovery requirements.
Alert me when the recovery points fail for: days	Select the **Alerting option** to receive alerts when the recovery points fails for the selected number of days.

After specifying your short-term recovery goals for the protection group, click **Next**.

See Also

New Protection Group Wizard

Working with Recovery Points

Allocate Storage

Use the **Allocate storage** page of the Create New Protection Group Wizard to review and change the space allocations on the storage pool for the replicas and recovery points that DPM recommends for the protection group. Space is also allocated on client computers for the change journal.

Note
We recommend that you co-locate your data if you have a large number of client computers. You will not be able to protect 1000 client computers with one DPM server without co-locating your data. We recommend that you co-locate if you have 10 or more client computers in a protection group.

This page contains the elements described in the following table.

Elements

Name	Description
Number of computers	Displays the total number of selected client computers.

Name	Description
Data per computer	Select the disk space required for the protected data on each client computer.
Disk space allocated in DPM	Displays the disk space allocated for the selected number of client computers.
Collocate client computers in DPM Storage Pool	Select this check box for collocating client computer data.
Automatically grow the volumes	Select this check box to automatically grow volumes when more disk space is required for protecting data on client computers.

After reviewing the disk allocations for the protection group, click **Next**.

See Also

New Protection Group Wizard

Co-Locating Data

Protection Agent Installation Wizard

The DPM Protection Agent Installation Wizard guides you through the process of either installing protection agents on computers that you want to protect or adding protected computers to the DPM server.

Throughout the protection agent installation process, the wizard provides default options that you can override if you choose. If you have questions at any point in the process, click **Help**.

See Also

Manage Protection Agents

Install Agents

Attach Agents

Install Agents

The DPM Protection Agent Installation Wizard guides you through the process of installing protection agents on computers that you want to protect. Throughout the protection agent installation process, the wizard provides default options that you can override if you choose. If you have questions at any point in the process, click **Help**.

In This Section

See Also

Protection Agent Installation Wizard
Manage Protection Agents

Select Agent Deployment Method

The Select Agent Deployment Method page of the Protection Agent Installation Wizard guides you through the process of installing protection agents on your computers that you want to protect or adding protected computers to the DPM server.

This page contains the elements described in the following table.

Elements

Name	Description
Install Agents	Select this option to install protection agents in the computers. **Important** To install the protection agent, you must be a member of the Administrators group on the computer that you want to protect.
Attach agents	Select this option for adding computers that you want to protect. **Important** If you have not already installed the protection agent, then you must

Name	Description
	manually install it on the computer that you want to protect.
Computer on trusted domain	Select this option to add a computer that belongs to the same domain as the DPM server domain, or is in a domain that has a two-way trust with the DPM server domain. DPM queries Active Directory Domain Services for the computer and displays it in the **Computer name** list in the **Select Computers** page of the Protection Agent Installation Method Wizard.
Computer in a workgroup or untrusted domain	Select this option to add a computer that is part of a workgroup or on a domain that does not have two-way trust with the DPM server domain.

Throughout the protection agent installation process, the wizard provides default options that you can override if you choose. If you have questions at any point in the process, click **Help**.

After selecting the available options, click **Next**.

See Also

Protection Agent Installation Wizard

Manage Protection Agents

Select Computers

Use the **Select Group Members** page of the Protection Agent Installation Wizard to select the computers you want to protect.

If you are installing a protection agent on a computer with a firewall enabled, or if you are manually installing a protection agent on the target computer using command line options, see Installing Protection Agents.

If you are installing a protection agent and encounter network or permissions related issues due to domain policies, we recommend that you install the protection agent manually.

For information about installing a protection agent by using a server image on the computer without specifying the DPM server, see "Installing a protection agent using a server image".

For information about the topics listed above see Manage Protection Agents.

If you have installed the agents on the computers you want to protect and want to attach them to the DPM server, see Attaching agents from a trusted domain and Attaching agents in workgroups or untrusted domains.

This page contains the elements described in the following table.

Elements

Name	Description
Computer name	In the **Computer name** box, select one or more computers (50 maximum) from the **Computer name** list. If you know the name of a specific computer on which you want to install the protection agent, type the name of the computer in the **Computer name** box. DPM queries Active Directory Domain Services for the computer and then adds it to the **Computer** list. If you do not know the name of the computer, browse the list to find the computer. **Important** Servers across domains are not listed in the Computer name box. To find a computer across a trusted domain, you must type the fully qualified domain name of the computer you want to protect (for example, **Server1.Domain1.corp.microsoft.com**, where *Server1* is the name of the target computer that you want to protect, and *Domain1.corp.microsoft.com* is the domain to which the target computer belongs).
Add	Click to add the selected computers to the **Selected computers** box.
Remove	Click to remove the selected computers from the **Selected computers** box.
Advanced	Click to install an earlier version of the protection agent that existed before you updated to the most recent version.

Name	Description
	This button is enabled only when there is more than one version of a protection agent available for installation on the computers.

After selecting the computers on which you want to install the protection agents, click **Next**.

Attaching agents from a trusted domain

To add multiple computers from the Select Computers page in Protection Agent Installation Wizard, use the **Add From File** dialog box to upload the .txt file that contains names of the all protected computers that you want to add to the DPM server.

We recommend that you provide the fully qualified domain name (FQDN) of the target computers. For example, enter multiple computers in a .txt file as follows:

Computer1.domain1.corp.microsoft.com

Computer2.domain1.corp.microsoft.com

Computer3.domain2.corp.microsoft.com

This page contains the elements described in the following table.

Name	Description
Text file location	The location of the text file (.txt) that contains names of all the protected computers that you want to add.

After uploading the text file (.txt), click **OK**.

Attaching agents in workgroups or untrusted domains

Use the **Select computers** page of the Protection Agent Installation Wizard to add a protected computer that is in a workgroup or in an untrusted domain to the DPM server.

This page contains the elements described in the following table.

Name	Description
Computer name	Type the name of the protected computer in the Computer name box. **Important** To add a computer not joined to any

Name	Description
	domain or in an untrusted domain, type one of the following: • Fully qualified domain name of the protected computer (for example, computer1.Domain1.corp.microsoft.com, where computer1 is the name of the target computer that you want to protect, and Domain1.corp.microsoft.com is the domain to which the target computer belongs) if DPM server and the protected computer can access each other using FQDNs. • The NETBIOS of the protected computer if DPM server and the protected computer can access each other using NETBIOS names.
Username	After you install the DPM protection agent on the computer, you need to run SetDpmServer.exe and then specify the username which would be used for authentication.
Password	Type the password for the username.
Add	Click **Add** to move the computer to the **Selected computers** box. As you add the computer, your selections appear in the **Selected computers** box.
Remove	Click **Remove** to remove the computers from the **Selected computers** box.

After adding the protected computers that you want to add to the DPM server, click **Next**.

See Also

Protection Agent Installation Wizard

Enter Credentials

Use the **Enter Credentials** page of the Protection Agent Installation Wizard to enter the user name and password for a domain account that is a member of the local administrators group on all selected computers.

This page contains the elements described in the following table.

Elements

Name	Description
User name	Type the user name for a domain account that is a member of the local administrators group on all selected computers.
Password	Type the password for the user account.
Domain	Accept or type the domain name of the user account that you are using to install the protection agent on the target computer. This account may belong to the current or trusted domain.

After entering the user credentials for the domain account, click **Next**.

See Also

Protection Agent Installation Wizard

Select Cluster Nodes

Use the **Select Cluster Nodes** page to select other nodes in the cluster that you have not yet selected.

This page contains the elements described in the following table.

Elements

Name	Description
No, do not add any other servers to my selected servers list	Click this option if you do not want to add other nodes in the cluster on which to install

Name	Description
	protection agents.
Yes, add the following servers which are cluster nodes to my selected server list	Click this option if you want to install the protection agents on other nodes in the cluster, and then select the computers from the list on which you want the protection agents installed.

After selecting the option you want for installing protection agents on other nodes in a cluster, click **Next**.

See Also

Protection Agent Installation Wizard

Choose Restart Method

Use the **Choose Restart Method** page to select the method you want to use to restart the servers after the protection agent is installed.

The server must be restarted before you can start protecting data. This restart is necessary because the DPM protection agent installs a volume filter driver, and the protection agent will not be active until the server is restarted.

This page contains the elements described in the following table.

Important

For computers having Windows Server 2003 or Windows XP operating systems, DPM will decide if it requires a restart.

Installing protection agents on any other operating systems does not require a restart.

Elements

Name	Description
Yes. Restart the selected computers after installing the protection agents.	Click this option if you want to restart the selected computers after the protection agents are installed. **Note** For computers having Windows Server 2003 or Windows XP operating systems, DPM will decide if it requires

Name	Description
	a restart. Installing protection agents on any other operating systems does not require a restart.
No. I will restart the selected computers later.	Click this option if you want to restart the selected computers at a later time. **Note** In a production environment, you would generally select this option to avoid restarting the computers during the business day. For computers having Windows Server 2003 or Windows XP operating systems, DPM will decide whether it requires a restart. If the protection agent status is displayed as **restart required**, then you must restart the protected computer for configuring the protection successfully.

After selecting one of the restart methods, click **Next**.

See Also

Protection Agent Installation Wizard

Summary

Use the **Summary** page of the Protection Agent Installation Wizard to verify the tasks that the wizard is going to perform.

If the tasks are correct, click **Install** to install the protection agent. To change the tasks, click **Back**.

See Also

Protection Agent Installation Wizard

Installation

Use the **Installation** page of the Protection Agent Installation Wizard to view the status of the tasks that DPM is performing. If a task fails, click the **Errors** tab for more information.

1. To exit the wizard, click **Close**.
2. To view the status of protection agents, click **Management** on the navigation bar.

See Also

Protection Agent Installation Wizard

Recovery Wizard

The Recovery Wizard guides you through the process of recovering data protected by Data Protection Manager (DPM) and backed up on disk and tape.

To view the data sources that Microsoft System Center Data Protection Manager (DPM) protects and the level of data that you can recover using DPM, see the table listed in What Is a protection group?

The Recovery Wizard helps you make decisions about how you want to recover data and where you want to recover it from. These decisions can vary depending on the type of data you want to recover and include the following options:

- Reviewing the recovery selection
- Selecting the recovery type
- Specifying the destination
- Specifying recovery options

At various times during the recovery process, the Recovery Wizard provides default options, which you can override if you choose.

Note

Click **Help** on any wizard page if you need assistance while working in the wizard.

See Also

DPM Wizards

How to Recover Data for Desktop Computers

How to Recover Data for Exchange-Based Servers

How to Recover Data for File Servers

How to Recover Data for SQL Servers

How to Recover Data for Virtual Machines

Recovering Hyper-V Virtual Machines

How to Recover Data for Windows SharePoint Services Servers

How to Recover System State

Review Recovery Selection

Use the **Review Recovery** page of the Recovery Wizard to review information for the items that you chose to recover. This page contains the elements described in the following table.

Elements

Name	Description
Recovery point	Ensure that the recovery point is the one you have selected: latest or a specific time.
Recover from	Ensure that the data you want to recover is on disk or tape.
Recovery item	Ensure that the item you wish to recover is listed in the **Item details** pane.
Recovery source	Ensure that the path for the recovery source is accurate.

To proceed with the recovery, click **Next**.

See Also

How to Recover Data for Desktop Computers

How to Recover Data for Exchange-Based Servers

How to Recover Data for File Servers

How to Recover Data for SQL Servers

How to Recover Data for Virtual Machines

Recovering Hyper-V Virtual Machines

How to Recover Data for Windows SharePoint Services Servers

How to Recover System State

Recover Data

Recovery Wizard

Select Recovery Type

Use the **Select Recovery Type** page of the Recovery Wizard to select the type of recovery you want to perform. This page contains the elements described in the following table. The available options depend on the type of data you are recovering.

File Servers and Desktop Computers

Name	Description
Recover to the original location	Select this option to recover files to their original location. The old database and its files are overwritten during the recovery process.
Recover to an alternate location	Select this option to copy the recovered files to an alternate destination. Click **Browse** to specify an alternate location.
Copy to tape	Select this option to copy the storage group to a tape in a DPM library. Note that the storage group or volume can also contain data that was not selected for recovery. **Important** The **Copy to tape** option in the Recovery Wizard is available only to the DPM administrator. The Recovery

Name	Description
	administrator and Tape administrator do not have permissions to use this option.

Exchange-Based Servers

Name	Description
Recover to original Exchange Server location	Select this option if you do not want to specify an alternate location. The old database and its files are overwritten during the recovery process. **Note** This option is available only if the latest recovery point is selected. If a database is selected for recovery, only the latest point in time can be recovered. All the databases in the storage group are dismounted during recovery. The database is remounted after the recovery is complete.
Recover to any instance of SQL Server	Select this option if you do not want to specify an alternate location. The old database and its files are overwritten during the recovery process. **Note** This option is available only if the latest recovery point is selected. If a database is selected for recovery, only the latest point in time can be recovered. All the databases in the storage group are dismounted during recovery. The database is remounted after the recovery is complete.
Copy to a network folder	Select this option to copy the recovered data to a network folder. Type the location on the next page.

Name	Description
Recover to another database or storage group on an Exchange server	Select this option to recover to another database or storage group on an Exchange-based server that has a protection agent installed.
Recover to a Recovery Storage Group	Select this option to recover Exchange data sources to a recovery storage group.

SQL Servers

Name	Description
Recover to the original instance of SQL Server (overwrite database)	Select this option if you want the current database files to be overwritten during the recovery process. This option is not available for mirrored databases.
Recover to any instance of SQL Server	Select this option to recover data onto the same instance of SQL Server in an alternate database, or on an alternate instance of SQL Server without affecting your production environment.  **Note** If you recover data to the same instance of SQL Server with the same database name, it will affect your production environment.
Copy to a network folder	Select this option to copy the recovered data to a network folder. You can select the location of the network folder on the next page.
Copy to tape	Select this option to copy the data to tape creating a long-term archive or portable media of the data for any recovery point.

Microsoft SharePoint (Farm Level)

Name	Description
Recover all SharePoint content and components	Select this option to overwrite the SharePoint farm's configuration database and all the content databases while they are online. This option is not available: For databases that are part of the recovery point where backup metadata enumeration failed. At the time of a recovery point creation, backup metadata enumeration can fail for the following reasons: "ConfigureSharePoint.exe –EnableSharePointProtection" was not run with correct farm administrator credentials on the front-end Web server. SharePoint VSS writer was in bad state on the front-end Web server. **Note** If some SQL Server databases in the selected SharePoint farm are mirrored, additional options are shown on the next page. See the following section for help on these options.
Copy all SharePoint content and component files to a network folder	Select this option to copy all the farm's databases to a network folder. The network folder path can be provided in the **Alternate folder** text box by using the **Browse** button.
Copy the Windows SharePoint Services farm to tape	Select this option to copy the SharePoint farm databases to a tape in a DPM library.

Microsoft SharePoint (Farm Level with Mirrored SQL Server Databases)

Name	Description
You find the following options when some SQL Server databases in the selected SharePoint farm are mirrored and you select the **Recover all SharePoint content and components** option on the **Select Recovery Type** page of the Recovery Wizard.	

Name	Description
Typical recovery	Select this option to recover the mirrored SQL Server databases to the instances of SQL server that were hosting these databases as the principal database when the selected recovery point was created.
Custom recovery	Select this option to recover the mirrored SQL Server databases of the SharePoint farm to the instances of SQL Server. At the point of recovery point creation, for each mirrored SQL Server database, you can select either of its partner instances of SQL Server (principal/mirror). Before you select the instance of SQL Server, ensure the following: The selected instance of SQL Server is online. The SQL Server alias that is being used on the front-end Web server points to the selected instance of SQL Server.

Microsoft SharePoint (Content Database Level)

Name	Description
Recover to the original instance of SQL Server of the selected Windows SharePoint Services farm	Select this option to overwrite the specified database while it is online. This option is not available: For databases that are part of the recovery point where backup metadata enumeration failed. At the time of a recovery point creation, backup metadata enumeration can fail for the following reasons: When “ConfigureSharePoint.exe –EnableSharePointProtection” was not run with the correct farm administrator credentials on the front-end Web server. When the SharePoint VSS writer was in bad state on the front-end Web server. For mirrored databases.

Name	Description
	 **Note** To recover mirrored database to its original instance of SQL Server, select the **Recover to any SQL Instance** option and then specify the recovery destination path pointing to its original instance of SQL Server on the **Specify Alternate Recovery Location** page.
Recover to any SQL instance	Select this option to recover the selected database to: The original instance of a SQL Server if the selected database is offline. The original instance of a SQL Server as a different database. (You can change the name of the database on the **Specify Alternate Recovery Location** page of the Recovery Wizard). An alternate instance of a SQL Server.  **Note** If you recover the database to the same instance of a SQL Server with the same database name, it can affect your production environment.
Copy the database files to a network folder	Select this option to copy the selected SharePoint database to a network folder. The network folder path can be provided in the **Alternate folder** text box by using the **Browse** button.

Microsoft Office SharePoint Server 2007 (MOSS) Shared Service Provider (SSP) or Windows SharePoint Services 3.0 Search

Name	Description
Recover all the SharePoint Search index components	Select this option to recover the SharePoint Search/MOSS Shared Services Provider (SSP) components to their original locations. For more information, see Recovering SharePoint Data.
Copy the SharePoint Search index components to an alternate network folder	Select this option to copy the recovered search index components to an alternate network folder.
Copy the SharePoint Search index components to tape	Select this option to copy the SharePoint Search or MOSS SSP Search components to a tape in a DPM library.

Microsoft SharePoint (Item-Level - Site Collections, Sites, Lists, Document Libraries, Documents, List Items and Other Items in the Farm)

Name	Description
Recover to original site	Select this option to recover the selected item to the URL where it belonged at the time of backup (as displayed in the recoverable item pane).
Recover to an alternate site	Select this option to recover the selected item to a different URL within the same SharePoint farm.

Virtual Servers

Name	Description
Recover to the original instance	Select this option to recover files to their original location. The old database and its files are overwritten during the recovery process.
Recover to a network folder	Select this option to recover the data to a network folder. You can select the location on

Name	Description
	the next page.
Copy to tape	Select this option to copy the virtual machine to a tape in a DPM library.

Hyper-V

Name	Description
Recover to the original instance	Select this option to recover a virtual machine to its original location. The original files are overwritten during the recovery process.
Recover as virtual machine to any host	Select this option to recover a virtual machine to a different Hyper-V host, or to an alternate location on the same Hyper-V host. **Important** Restoring the virtual machine to the same Hyper-V host overwrites an existing instance of the same virtual machine present on the same Hyper-V host. **Note** Hyper-V virtual machines that are recovered to a cluster node are not highly available. For more information about how to make a virtual machine highly available, see Make the virtual machine highly available (http://go.microsoft.com/fwlink/?LinkID=160484).
Copy to a network folder	Select this option to recover the VHD and other configuration files of the virtual machine to a network folder. **Note** After recovery, you must manually create a virtual machine by using the recovered VHD files of the virtual machine.
Copy to tape	Select this option to copy the virtual machine to a tape in a DPM library.

System State

Name	Description
Copy to a network folder	Select this option to copy the recovered system state data to a network folder. You can select the location on the next page.
Copy to tape	Select this option to copy the system state data to a tape in a DPM library.

DPM Servers

Name	Description
Recover replica to primary DPM server	Select this option when you are recovering a primary DPM server. For more information about recovering protected computers and DPM servers, see Managing Disaster Recovery.

To proceed with the recovery, click **Next**.

Specify Library

Use the **Specify Library** page of the Recovery Wizard to select the library and specify the tape options for recovery. This page contains the elements described in the following table.

Elements

Name	Description
Copy item	Lists the path of the item you want to copy to tape.
Primary library	Specify a library for the recovery.
Copy library	The **Copy library** option is enabled only when the primary library has a single drive.
Tape label	DPM supplies a default tape label name. You can edit this field.

Name	Description
Data on tape	Select **Compress** to compress data on tape**, Encrypt** to encrypt data on tape so that it can be read only by a DPM server, or **Do not compress or encrypt**.

To proceed with the recovery, click **Next**.

See Also

Compress data in a protection group

Encrypt data in a protection group

Managing Tapes

Recover Data

Recovery Wizard

Specify Destination

Use the **Specify Destination** page of the Recovery Wizard to specify where you want to locate the database files or a Hyper-V virtual machine to recover.

This page contains the elements described in the following table.

Elements

Name	Description
Copy destination	Browse to select a copy destination path. **Note** The alternate recovery destination must be on a server that has a protection agent installed.

To proceed with the recovery, click **Next**.

See Also

Recover Data

Recovery Wizard

Select Recovery Type

Specify Alternate Recovery Destination

Use the **Specify Alternate Recovery Destination** page of the Recovery Wizard to select the recovery destination corresponding to the selected data source. Click the plus signs to expand the directory tree.

Note
A Hyper-V virtual machine recovered to a cluster will not be highly available automatically. If you want to make it highly available, you need to configure it manually after the recovery.

Click **OK** to proceed.

See Also

Recovery Wizard

Select Recovery Type

Select Instances of SQL Server

Use the **Select Instances of SQL Server** page of the Recovery Wizard to select the instance or instances of SQL Server that you want the corresponding mirrored database to be recovered to.

Click **Next** to continue.

See Also

Recovery Wizard

Select Recovery Type

Specify Alternate Recovery Location

Use the **Specify Alternate Recovery Location** page of the Recovery Wizard to specify where you want to locate the database files that you are recovering.

When recovering a mirrored SQL Server database, you must always recover to an alternate location. If you want to recover to the original location, you must still recover to an alternate location, and then provide the path to one of the partners of the mirrored database.

This page contains the elements described in the following table.

Elements

Name	Description
Instance of SQL Server	Browse to select an instance of SQL Server for the database that you are recovering.  **Note** For mirrored SQL Server databases you can recover to the “latest” point-in-time.
Recovered database name	Specify the name of the recovered database.
Database file locations	Specify the database file locations for the database you are recovering.

To proceed with the recovery, click **Next**.

See Also

Recover Data

Recovery Wizard

Select Recovery Type

Specify Database Recovery Completion State

Use the **Specify Database State** page of the Recovery Wizard to specify the recovery option for recovering the selected SQL Server database. This page contains the elements described in the following table. Available options will depend on the type of data you are recovering.

Elements

Name	Description
Leave database operational	Select this option to perform a full recovery and leave the database ready to use.
Leave database non-operational but able to restore additional transaction logs	Select this option to recover the database but leave it non-operational.
Copy SQL transaction logs between the selected recovery point and the latest	Select this option if you want to copy transaction logs for the database restoring

Name	Description
recovery point	state. This option is disabled if no transaction logs are available for the selected database.

To proceed with the recovery, click **Next**.

See Also

How to Recover Data for Desktop Computers

How to Recover Data for Exchange-Based Servers

How to Recover Data for File Servers

How to Recover Data for SQL Servers

How to Recover Data for Virtual Machines

Recovering Hyper-V Virtual Machines

How to Recover Data for Windows SharePoint Services Servers

How to Recover System State

Recover Data

Recovery Wizard

Select Recovery Process

The **Select Recovery Process** page of the Recovery Wizard guides you through the process of performing an item-level recovery of site collections, sites, document libraries, lists, and documents from Microsoft SharePoint Foundation 2010 or
Microsoft Office SharePoint Server 2010 farm both with and without a recovery farm.

This page contains the elements described in the following table.

Elements

Name	Description
Recover without using a recovery farm	Select this option if the version of the target Microsoft SharePoint 2010 farm is same as at the time of the selected recovery point.
Recover using a recovery farm	Select this option if the version of the target Microsoft SharePoint 2010 farm has changed from the time, the selected recovery point was created.

After selecting the available options, click **Next**.

See Also

Recovery Wizard

Select Recovery Type

Specify Temporary Server

The **Specify Temporary Server** page of the Recovery Wizard enables you to specify server parameters that will be used to host the temporary copy of the SharePoint content database.

This page contains the elements described in the following table.

Elements

Name	Description
Front-end Web Server:	Select this option to specify the SharePoint Front-end Web Server of the recovery farm to temporarily stage data prior to recovery.
SQL instance:	Select this option to specify the instance of SQL Server to stage the temporary copy of the SharePoint content database that contains the requested SharePoint item before recovery. If you are using the recovery farm, then the instance of SQL Server should be on the same computer that was selected as the Front-end Web Server. If you are not using the recovery farm then you can select one of the following Same instance of SQL Server where the database was backed up from (Production SQL Server): In this case only a temporary copy of the database will be copied and removed after the recovery is completed. This temporary copy will not over-write any of the SharePoint farm's content. DPM's instance of SQL Server. Any other instances of SQL Server. **Note**

Name	Description
	If you are using DPM's instance of SQL Server or any other instances of SQL Server then make sure that its version is equal to or a has a later version than the version of the production SQL Server.
Database file location:	To copy the database files, specify a file location on the SQL Server.
Target site URL:	Select this option to specify a URL within the same SharePoint farm under which you would want to recover the selected SharePoint item. This option is enabled only if you are performing a recovery to an alternate location within the same SharePoint farm.

After specifying the server parameters, click **Next**.

See Also

Recovery Wizard

Select Recovery Type

Specify Staging Location

The **Specify Staging Location** page of the Recovery Wizard enables you to specify a temporary file location on the SharePoint farm to which the recovery is being done. This file location is used to temporarily store the SharePoint item that has requested for recovery.

This page contains the element described in the following table.

Elements

Name	Description
File location	Specify a temporary file location on the Web Front-end Server of the SharePoint farm you want to recover selected item to.

After specifying a temporary file location, click **Next**.

See Also

Recovery Wizard

Select Recovery Type

Specify Recovery Options

Use the **Specify Recovery Options** page of the Recovery Wizard to specify options to apply to recovery. This page contains the elements described in the following table. Available options will depend on the type of data you are recovering.

Elements

File Servers and Desktop Computers	Why choose this option?
Existing version recovery behavior	Select **Create copy**, **Skip**, or **Overwrite**. **Important** If you are recovering data protected from a case-sensitive server onto a server that is not case sensitive, select the **Create copy** option. Otherwise, if they differ in case but have the same name, only some of your files will be recovered.
Restore security	This option appears only if you selected **Recover to original location** or **Recover to an alternate location** in the **Select Recovery Type** screen. Select **Inherit security settings of target when overwriting or of parent folder when creating copy** or **Apply the security settings of the recovery point version**.
Network bandwidth usage throttling	Click **Modify** to enable or disable throttling settings and specify a work schedule.
Notification	If you have subscribed to alerts and notifications in DPM, select the **Send an e-mail when this recovery completes** check box to have DPM notify you. To enable this, you must configure a Simple Mail Transfer Protocol

	(SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.
Recipients	If you select the **Send an e-mail when this recovery completes** check box, type the e-mail address of the recipients you want to send the notification to. Separate the e-mail addresses with commas.
Exchange-Based Servers	**Why choose this option?**
Mount the databases after they are recovered	Select whether or not to mount the Exchange databases after DPM recovers them.
Bring the database to a clean shutdown after copying the files	This option brings the database files to a mountable condition by copying the logs. Select this option only if the destination is an Exchange-based server that has the same version of the Exchange application as at the time of protection.
Network bandwidth usage throttling	Click **Modify** to enable or disable throttling settings and specify a work schedule.
Notification	If you have subscribed to alerts and notifications in DPM, select the **Send an e-mail when this recovery completes** check box to have DPM notify you. To enable this, you must configure a Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.
Recipients	If you select the **Send an e-mail when this recovery completes** check box, type the e-mail address of the recipients you want to send the notification to. Separate the e-mail addresses with commas.
SQL Servers - Specify Database State	**Why choose this option?**
Recover database	Select this option to perform a full recovery and leave the database ready to use.
Recover and leave database in restoring state	Select this option to recover the database but leave it non-operational.
Network bandwidth usage throttling	Click **Modify** to enable or disable throttling

	settings and specify a work schedule.
Notification	If you have subscribed to alerts and notifications in DPM, select the **Send an e-mail when this recovery completes** check box to have DPM notify you. To enable this, you must configure a Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.
Recipients	If you select the **Send an e-mail when this recovery completes** check box, type the e-mail address of the recipients you want to send the notification to. Separate the e-mail addresses with commas.
SQL Servers - Database Restoring State Option	**Why choose this option?**
Copy SQL transaction logs between the selected and latest available recovery	Select this option if logs are available for the selected database for the most current data.
Windows SharePoint Services Servers	**Why choose this option?**
Network bandwidth usage throttling	Click **Modify** to enable or disable throttling settings and specify a work schedule.
Enable SAN-based recovery using hardware snapshots	Select this option to enable SAN-based recovery using hardware snapshots for quicker recovery. Before you can recover data on a SAN using hardware snapshots, you must have the following: A SAN where hardware snapshot functionality is enabled; a SAN with the capability to create a clone and split a clone to make it writable, and the protected computer and the DPM server connected to the same SAN.
Notification	If you have subscribed to alerts and notifications in DPM, select the **Send an e-mail when this recovery completes** check box to have DPM notify you. To enable this, you must configure a Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see

	Configuring the SMTP Server.
Recipients	If you select the **Send an e-mail when this recovery completes** check box, type the e-mail address of the recipients you want to send the notification to. Separate the e-mail addresses with commas.
Virtual Servers	**Why choose this option?**
Apply security settings of the destination computer	Select this option if you want the recovered data to have the same security settings as the destination server.
Apply the security settings of the recovery point version	Select this option if you want the recovered data to retain its existing security settings.
Enable SAN-based recovery using hardware snapshots	Select this option to enable SAN-based recovery using hardware snapshots for quicker recovery. Before you can recover data on a SAN using hardware snapshots, you must have the following: A SAN where hardware snapshot functionality is enabled, a SAN with the capability to create a clone and split a clone to make it writable, and the protected computer and the DPM server connected to the same SAN.
Notification	If you have subscribed to alerts and notifications in DPM, select the **Send an e-mail when this recovery completes** check box to have DPM notify you. To enable this, you must configure a Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.
Recipients	If you select the **Send an e-mail when this recovery completes** check box, type the e-mail address of the recipients you want to send the notification to. Separate the e-mail addresses with commas.
System State	**Why choose this option?**
Enable SAN-based recovery using hardware	Select this option to enable SAN-based recovery using hardware snapshots for quicker

snapshots	recovery. Before you can recover data on a SAN using hardware snapshots, you must have the following: A SAN where hardware snapshot functionality is enabled, a SAN with the capability to create a clone and split a clone to make it writable, and the protected computer and the DPM server connected to the same SAN.
Notification	If you have subscribed to alerts and notifications in DPM, select the **Send an e-mail when this recovery completes** check box to have DPM notify you. To enable this, you must configure a Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.
Recipients	If you select the **Send an e-mail when this recovery completes** check box, type the e-mail address of the recipients you want to send the notification to. Separate the e-mail addresses with commas.
DPM Servers	For more information about recovering protected computers and DPM servers, see **Disaster Recovery [DPMv3Help]**.

To proceed with the recovery, click **Next**.

For step-by-step instructions for recovering a DPM server from a secondary DPM server in case of disaster, see **Disaster Recovery [DPMv3Help]**.

See Also

How to Enable Computer-Level Network Bandwidth Usage Throttling

How to Recover Data for Desktop Computers

How to Recover Data for Exchange-Based Servers

How to Recover Data for File Servers

How to Recover Data for Windows SharePoint Services Servers

How to Recover Data for SQL Servers

How to Recover Data for Virtual Machines

How to Recover System State

Recover Data

Recovery Wizard

Summary

Use the **Summary** page of the Recovery Wizard to verify the tasks that the wizard is going to perform.

If the tasks are correct, click **Recover** to begin recovery of your data. To change the tasks, click **Back**.

Note
Any synchronization job for the selected recovery item will be canceled while the recovery is in progress.

See Also

How to Recover Data for Desktop Computers

How to Recover Data for Exchange-Based Servers

How to Recover Data for File Servers

How to Recover Data for SQL Servers

How to Recover Data for Virtual Machines

Recovering Hyper-V Virtual Machines

How to Recover Data for Windows SharePoint Services Servers

How to Recover System State

Recovery Wizard

DPM Client

System Center 2012 – Data Protection Manager (DPM) enables you to protect and recover the files and folders on your computer in case of data loss or corruption. Your backup administrator configures backup and protection for your computer according to your company protection policy and gives you the ability to manage your backups so that you can perform your own data recoveries.

In This Section

Getting Started with the Data Protection Manager Client

Data Protection Manager Client FAQ

Managing Protected Files and Folders

Recovering Files and Folders on Your Computer
Troubleshooting Data Protection Manager Client Issues

Getting Started with the Data Protection Manager Client

The Data Protection Manager (DPM) Client includes features that make your protected files and folders available to you from the DPM icon displayed in the notification area (also known as the system tray). By default, when you are running the DPM Client, the DPM icon appears in the notification area. When you move the mouse pointer over the DPM icon, the DPM synchronization status information is displayed. For example, **Last sync: 1 hour ago, Automatically every 4 hrs**.

The following options are available when you click the DPM icon in the notification area:

Options

Name	Description
Synchronize now	Starts the synchronization process. When the Synchronization process is running, the link changes to **Cancel Synchronization**.
Open DPM Client	Opens the **Data Protection Manager Client**, and displays the last viewed tab. To view the company protection policy information set by your backup administrator, on the **Summary** tab, click the **Company Protection Policy** link.
Recover data	Opens the Data Protection Manager Client, and displays the **Recovery** tab.
Help	Starts Data Protection Manager Client Help. Provides feature overviews and procedures for performing protection and recovery tasks.

Data Protection Manager Client FAQ

You can use the following links to find answers to frequently asked questions about DPM synchronization and recovery.

In This Section

What is synchronization?

When the data changes on your computer, DPM makes a point-in-time copy of your files and folders and copies them to the DPM server. This synchronization process keeps the data on your computer synchronized with the data on the DPM server.

What happens when I synchronize my data?

When you synchronize your data, the changes to the data on your computer are copied to a replica on the DPM server. You synchronize the data on your computer to keep it consistent with the data on the DPM server. Note that the data that you synchronize is not immediately available for recovery. The data will become available for recovery when DPM creates a recovery point, which you will be able to see from the recovery point schedule.

When should I synchronize my data?

You want to synchronize your data according to the amount of data loss you are prepared to sustain. For example, if you synchronize your data just once each day, DPM will restore your data to within a day of a data loss event. If you set up an hourly synchronization schedule, DPM will restore your data to within an hour of a data loss event.

What is a recovery point?

To protect your data, DPM starts by creating a complete point-in-time copy of the files and folders you want to protect on your computer. This copy is called a *replica*. A *recovery point* is a point-in-time copy of the replica and it is stored on the DPM server. If you experience data loss or corruption, you can access the recovery points of a previous version of your files and folders to recover your data.

How do I access my recovery points on the DPM server?

You use the Data Protection Manager (DPM) Client to search for your recovery points. Available recovery points are listed in the DPM Client in the display pane and include the time stamps and the open links (backup folder locations on the DPM server) for each of the available recovery points.

Managing Protected Files and Folders

The Data Protection Manager (DPM) Client provides you with current information about your protected files and folders and gives you options to synchronize changes from your computer to the DPM server.

In This Section

How to View Information and Synchronize Files and Folders

The DPM Client enables you to view summarized information and synchronize your protected files and folders.

To view summarized information and synchronize protected items

1. Click **Start**, point to **All Programs**, click **Microsoft System Center Data Protection Manager 2012**, and then click **DPM Client**.

   The DPM Client appears in the task tray.

   Note

   The DPM icon may be hidden by default in Windows 7.
2. In the **Data Protection Manager Client**, click the **Summary** tab.
3. On the **Summary** tab, DPM provides information about disk space that is used by the protected items. The first section lists the last time a synchronization was successfully performed and the synchronization schedule.

   If you experience issues with synchronizing your data, click the **Details** link. The **Backup Failure Details** dialog box appears, which contains a link that your backup administrator

can use to display troubleshooting details.

To synchronize your files and folders at this time, click **Synchronize Now**.

4. To view the company protection policy information set by your backup administrator, on the **Summary** tab, click the **Company Protection Policy** link.
5. The second section displays the latest recovery point on the DPM server, which is the time interval since the last time the recovery point was created.

See Also

Managing Protected Files and Folders

How to Protect Files and Folders on Your Computer

In addition to the files and folders that are backed up by default, your company protection policy may allow you to configure additional files and folders for backup. This setting is controlled by your backup administrator.

Contact your backup administrator to give you permission to configure protection of additional files and folders. You can use the steps described in this section to configure protection.

To protect data items

1. Click **Start**, point to **All Programs**, click **System Center 2012 – Data Protection Manager (DPM)**, and then click **Data Protection Manager Client**.
2. In the **Data Protection Manager Client**, click the **Protected Items** tab.
3. Select the files and folders that you want to protect in the tree view, and then click **OK**.

   To determine the data size of the selected files and folders, click **Calculate**.

   Note
   By default, the company protection policy set by your backup administrator might cause some files and folders to be un-protectable or protectable. To view your company protection policy, on the **Summary** tab, click the **Company Protection Policy** link.

See Also

Managing Protected Files and Folders

How to View Information and Synchronize Files and Folders

Recovering Files and Folders on Your Computer

DPM allows you to recover your files and folders from your computer in case of data loss or corruption. You start protecting your data by creating recovery points, also referred to as local snapshots of the files and folders on your computer. Your DPM administrator sets a recovery point schedule according to your company protection policy.

Important
Local snapshots cannot be created on Windows XP client computers.

In This Section

How to Recover Files and Folders on Your Computer

With System Center 2012 – Data Protection Manager (DPM), you can recover files and folders from backups that are stored locally on your computer.

Note
By default, DPM allows only the local administrator to perform recoveries on the computer.

To recover data from backups stored locally

1. Right-click any file or folder that you want to restore, and then click **Restore previous versions**.

   In the **Properties** dialog box, on the **Previous Versions** tab, there is a list of available previous versions of the file or folder. The list includes files and folders that are saved to a backup as well as local recovery points.
2. Before you restore a previous version of a file or a folder, ensure that it is the correct version. To do this, select the previous version, and then click **Open** to view its contents.
3. After you verify that it is the correct version of the file or folder, click **Restore**.

Enabling non-administrators to recover files

If you want to allow users who are not administrators on a computer to be able to recover files, you must create the following registry key on the protected computer.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent\ClientProtection
Value	ClientOwners
Data	Comma-separated list of users who should be allowed to perform recoveries on this computer.
Type	String

How to Recover Files and Folders Stored on the DPM Server

System Center 2012 – Data Protection Manager (DPM) enables you to recover files and folders from backups stored on the DPM server that are managed by your backup administrator. To recover your data, you need to know the name of the DPM server on which the data was backed up. To find out the name of the DPM server, contact your backup administrator.

To recover data from backups stored on the DPM server

1. Click **Start**, point to **All Programs**, click **System Center 2012 – Data Protection Manager (DPM)**, and then click **Data Protection Manager Client**.
2. In the Data Protection Manager Client, click the **Recovery** tab.
3. In the **Search for recovery points on** text box, type the name of DPM server on which the data was backed up, or click the **Search** button to start the search for the existing recovery points on the DPM server.

   Note
   To find out the name of the DPM server, contact your backup administrator.
4. To access the backups stored on the DPM server, in the list of files and folders, click the **open** link that belongs to the respective recovery points.

   Note
   Available recovery points are listed in the display pane. In the display pane, the **Time** column lists the time stamps and the **Link** column lists the open links (backup folder locations on the DPM server) for the each available recovery points.
5. Select the previous version you want to restore and then click **Restore**.

See Also

Recovering Files and Folders on Your Computer

Troubleshooting Data Protection Manager Client Issues

The following table provides guidance for troubleshooting issues that may occur when you use the Data Protection Manager Client to protect data on your computer.

Issue	Cause	Resolution
In **Data Protection Manager Client**, on the **Summary** tab, the **Current status** displays **Unable to contact DPM server**.	The client computer is not connected to the corporate network. -OR- The DPM server is unavailable.	Retry the operation after you connect to the corporate network. If you still cannot contact the DPM server, ask your backup administrator to make sure that the DPM server is running.
On the **Summary** tab of the Data protection Manager dialog box, the **Current Status** displays **Client not configured for protection**.	The client computer has not been added to the protection group list on the DPM server.	Contact your backup administrator. To troubleshoot this issue, they must do the following: Add the client computer to an existing protection group on the DPM server. -OR- Create a new protection group for the client computer on the DPM server.

DPM Self-Service Recovery Tool

The Self-Service Recovery Tool (SSRT) for System Center 2012 – Data Protection Manager (DPM) enables end users to recover SQL Server databases that are backed up by the DPM server, without any intervention from the DPM administrator.

In This Section

Installing the DPM Self-Service Recovery Tool

This topic provides instructions to install the DPM Self-Service Recovery Tool (SSRT) for SQL Server databases.

Prerequisites

End users must install the .NET Framework 3.5 on their client computers.

To install DPM SSRT, end users must have administrative privileges on their client computers.

Installing DPM SSRT

You can find the DPM SSRT client application installer on the DPM product DVD, in the DpmSqlEURInstaller folder.

Upgrading the Prerelease Version of DPM SSRT

To upgrade the prerelease version of DPM SSRT to release to the manufacturing (RTM) version of DPM SSRT, you must first uninstall the prerelease version.

See Also

Getting Started with the DPM Self-Service Recovery Tool

Getting Started with the DPM Self-Service Recovery Tool

This topic summarizes the steps for getting started with the DPM Self-Service Recovery Tool (SSRT). To use the DPM SSRT, the DPM administrator must configure the DPM server to authorize end users to perform self-service recovery of SQL Server databases.

To start the DPM SSRT tool, Click **Start**, point to **All Programs**, and then click **DPM Self-Service Recovery Tool**. This opens the DPM SSRT console. All end user operations, such as starting and managing recovery jobs, are performed from the DPM SSRT console. The DPM SSRT console also displays a list of available recovery jobs for SQL Server databases.

To connect to a DPM server, in the DPM SSRT console, click **Connect to DPM Server**. Enter the name of the DPM server to which you want to connect. If you do not know the name of the DPM server or do not have the required permissions on the DPM server, contact your DPM administrator.

Before you start a new recovery job, ensure that you are connected to the DPM server that backs up the SQL Server databases that you plan to recover. To start a new recovery job, in the DPM SSRT console, click **New Recovery Job**. The Recovery Wizard will guide you through the process of recovering SQL Server databases.

See Also

Performing a Self-Service Recovery

DPM Self-Service Recovery Wizard

Performing a Self-Service Recovery

This section describes how to connect to a DPM server, recover SQL Server databases, and monitor recovery jobs by using the DPM Self-Service Recovery Tool (SSRT).

In This Section

Connecting to a DPM Server

Recovering a SQL Server Database

Monitoring Recovery Jobs

See Also

DPM Self-Service Recovery Wizard

Connecting to a DPM Server

Before you can perform recoveries from the DPM Self-Service Recovery Tool (SSRT) console, you must connect to a DPM server that backs up the SQL Server databases that you plan to recover. The steps for connecting to a DPM server include the following:

1. In the DPM SSRT console, click **Connect to DPM Server**.
2. Enter the name of the DPM server to which you want to connect. If you do not know the name of the DPM server or do not have the required permissions on the DPM server,

contact your DPM administrator.

After you connect to the DPM server, the server retrieves information about all the recovery-related jobs for SQL Server databases that were configured by using your user account and permissions. By default, DPM displays recoveries done in the last 30 days. This information is automatically refreshed for jobs that are in progress. You can also manually refresh the information by using **Refresh** from the **Actions** menu.

Note

If you want to recover SQL Server databases from another DPM server, click **Connect to Another Server** in the DPM SSRT console. This operation will disconnect the DPM SSRT from the currently connected DPM server. For recovering SQL Server databases from multiple DPM servers, you can start multiple instances of DPM SSRT.

See Also

Recovering a SQL Server Database

Monitoring Recovery Jobs

DPM Self-Service Recovery Wizard

Recovering a SQL Server Database

The DPM Self-Service Recovery Tool (SSRT) offers you the following options for recovering a SQL Server database:

Recover to any instance of SQL Server. Enables you to recover to any instance of SQL Server that has been preconfigured by your DPM administrator, and then mount the recovered database. This option is recommended when you have transaction logs to be replayed during recovery.

Note

- You cannot recover a database to its original location.
- When recovering to a different instance of SQL Server or to the same instance of SQL Server, make sure that you enter a different database name.

Copy to a network folder. Enables you to recover SQL Server databases as files to a network folder.

To recover a SQL Server database to any instance of SQL Server

1. In the DPM SSRT Console, click **New Recovery Job** to start the **Recovery Wizard**.
2. Select the **SQL Server Instance Name** and the **Database Name** that you want to recover, and then click **Next**.

   Important
   If you are using availability groups, provide the name of the availability group instead of the SQL Server instance name and leave the Database Name empty. The name should be in the format AGNAME.ClusternameFQDN\AGNAME, where AGNAME is the name of the availability group.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the date from the calendar and the time from the drop-down list for the recovery points that you want to recover, and then click **Next**.
4. Select **Recover to any instance of SQL Server**. This option enables you to recover to any instance of SQL Server which is preconfigured by your DPM administrator.
5. Click **Next**. Select the **SQL Server Instance Name**.
6. Select the **Database file location**. You can either select a folder path that is preconfigured by your DPM administrator or select a **custom path** for the selected instance of SQL Server.
   - **Folder path that is preconfigured by your DPM administrator**. The database files will always be recovered to a new folder that is created during recovery under the folder path that is preconfigured by your DPM administrator.
   - **Custom path**. If you select **custom path**, then in the **Database file locations** section, under the **Database file location** column, you can specify a folder path for each database file.

     Note
     The **custom path** option will be available only if your DPM administrator has configured this option for you on the DPM server.
7. Specify the **Recovered Database Name**, and then click **Next**.
8. Specify the database state and then click **Next**.
9. Select the **Send an e-mail when this recovery completes** check box to notify you when the recovery job is completed. Specify the recovery options and then click **Next**.

   Note
   The check box is enabled only if your DPM administrator had configured e-mail notifications on the DPM server.
10. On the Summary page, review the recovery settings, and then click **Recover**.

To copy a SQL Server database to a network folder

1. In the DPM SSRT Console, click **New Recovery Job** to start the **Recovery Wizard**.
2. Select the **SQL Server Instance Name** and the **Database Name** that you want to recover, and then click **Next**.
3. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the date from the calendar and the time from the drop-down list for the recovery points that you want to recover, and then click **Next**.
4. Select **Copy to a network folder**. This option enables you to recover SQL databases as files to a network folder. Specify the name of the destination server and destination folder path. Click **Next**.

   Note
   If the recovery point that you selected was not created from an express full backup, you will be presented with new recovery point choices. DPM can only copy files from a recovery point that is associated with an express full backup. Select an alternate recovery point and then click **Next**.
5. Select the **Send an e-mail when this recovery completes** check box to notify you when the recovery job is completed. Specify the recovery options and then click **Next**.

   Note
   The check box is enabled only if your DPM administrator had configured e-mail notifications on the DPM server.
6. On the Summary page, review the recovery settings, and then click **Recover**.

See Also

Monitoring Recovery Jobs

Performing a Self-Service Recovery

DPM Self-Service Recovery Wizard

Monitoring Recovery Jobs

You can use the DPM Self-Service Recovery Tool (SSRT) console to monitor recovery jobs for SQL Server databases configured by your DPM administrator.

Viewing Recovery Job Status

Recovery jobs for SQL Server databases are displayed in the **Jobs** list view in the DPM SSRT console. The following table provides the possible types of recovery job status that you might see in the **Jobs** list view in the DPM SSRT console.

Recovery Job Status	Description
In Progress	The recovery job is still in progress. For more information about the recovery job in progress, double-click the recovery job.
Completed	The recovery job was completed successfully.
Failed	The recovery job was canceled or failed.

To find operational details such as **Status description**, **elapsed time**, and **data transferred** for any recovery job, double-click the recovery job.

Rerunning a Failed Recovery Job

You can rerun a failed recovery job from the DPM SSRT console. To rerun a failed recovery job, select the recovery job and then click **Rerun**.

Note
To be able to rerun a recovery job started by a different user, you must have permission both to recover the database and to recover to the location it was being recovered to. If you do not have these permissions, you cannot rerun the recovery job.

Stopping a Recovery Job

To stop a recovery job that is in progress, select the recovery job and then click **Stop**.

See Also

Performing a Self-Service Recovery

DPM Self-Service Recovery Wizard

DPM Self-Service Recovery Wizard

The Recovery Wizard guides you through the process of recovering SQL Server databases. This wizard changes dynamically, depending on the type of recovery you select. The wizard includes the following options:

Specifying database details of the SQL Server database that you want to recover.

Specifying a recovery point for recovering a SQL Server database.

Selecting a recovery type. You can recover a SQL Server database to any instance of SQL Server which is preconfigured by your DPM administrator, or you can recover it as database files to a network folder.

Specifying recovery options to specify options that apply for recovery. Which recovery options are available depends on the type of recovery that you select.

Note

Click **Help** on any wizard page for more information.

In This Section

Welcome

Specify Database Details

Specify Recovery Point

Select Recovery Type

Specify Recovery Options

Summary

See Also

Performing a Self-Service Recovery

Welcome

The **Welcome** page of the Recovery Wizard enables you to start a recovery job to recover a SQL Server database that is backed up by DPM.

This page contains the following elements.

Elements

Name	Description
Do not show this Welcome page again	Select if you do not want the wizard to display the **Welcome** page when you begin a recovery job in the future.

To continue with the recovery, click **Next**.

See Also

DPM Self-Service Recovery Wizard

Specify Database Details

Use the **Specify Database Details** page of the Recovery Wizard to specify the details of the SQL Server database that you want to recover.

This page contains the following elements.

Elements

Name	Description
SQL Server Instance Name	Select an instance of a SQL Server from the drop-down list.
Database Name	Select the name of the SQL Server database from the drop-down list.

To continue with the recovery, click **Next**.

See Also

DPM Self-Service Recovery Wizard

Specify Recovery Point

Use the **Specify Recovery Point** page of the Recovery Wizard to select the recovery point to use for recovering SQL Server databases.

This page contains the following elements.

Elements

Name	Description
Recovery time	Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date from the calendar and the time from the drop-down list for the recovery

Name	Description
	points that you want to recover.

To continue with the recovery, click **Next**.

See Also

DPM Self-Service Recovery Wizard

Select Recovery Type

Use the **Select Recovery Type** page of the Recovery Wizard to select the type of recovery you want to perform. This page contains the following elements.

Elements

Name	Description
Recover to any instance of SQL Server	Select this option to recover a database to any instance of SQL Server on either the same SQL Server or another SQL Server that has been preconfigured by your DPM administrator.
Copy to a network folder	Select this option to copy the recovered database files to a network folder. You can select the location of the network folder on the next screen.

To continue with the recovery, click **Next**.

In This Section

Change Recovery Point

Select Alternate Recovery Location

Specify Destination

Specify Database State

See Also

DPM Self-Service Recovery Wizard

Change Recovery Point

You can only copy a SQL Server database to a network folder from a recovery point that was created from an express full backup. The **Change Recovery Point** page provides new recovery point choices, and you will see this page if the recovery point that you selected was not created from an express full backup. Use this page to select a recovery point that is associated with full express backup.

This page contains the following elements.

Elements

Name	Description
Recovery Points	Select one of the recovery points associated with full express backup listed in the **Recovery points** column.

To continue with the recovery, click **Next**.

See Also

Select Recovery Type

DPM Self-Service Recovery Wizard

Select Alternate Recovery Location

Use the **Specify Alternate Recovery Location** page of the Recovery Wizard to specify an instance of SQL Server, database file location and name of the recovered database for recovery. This page contains the following elements.

Elements

Name	Description
SQL Server Instance Name	Select this option to recover a database to any instance of SQL Server either on the same SQL Server or on another SQL Server that has been preconfigured by your DPM administrator. **Note**

Name	Description
	• You cannot recover a database to its original location. • When recovering to a different instance of SQL Server or to the same instance of SQL Server, make sure that you enter a different database name.
Database file location	You can either select a folder path that is preconfigured by your DPM administrator or select a **custom path** for the selected instance of SQL Server.
Recovered Database Name	Specify the name of the recovered database.
Database file location – custom path	If you select the **custom path**, you can specify a folder path for each database file in the **Database file locations** section, under the **Database file location** column.  **Note** The **custom path** option will be available only if your DPM administrator has configured this option for you on the DPM server.

To continue with the recovery, click **Next**.

See Also

Select Recovery Type

DPM Self-Service Recovery Wizard

Specify Destination

Use the **Specify Destination** page of the Recovery Wizard to copy the database files to a network folder. This page contains the following elements.

Elements

Name	Description
Destination server (FQDN)	Specify the destination server name. You must type the fully-qualified domain name of the server.
Destination folder	Specify the folder path location on the destination server where the database files will be recovered to. For example, to recover the database files to a folder (for example, E:\Folder1) on the server Server1 specify Server1 as the destination server and Folder1 as the destination folder.  **Note** You cannot specify a UNC path (for example, \\servername\sharename) when recovering SQL Server databases as files to a network folder.

To continue with the recovery, click **Next**.

See Also

Select Recovery Type

DPM Self-Service Recovery Wizard

Specify Database State

Use the **Specify Database State** page of the Recovery Wizard to specify the recovery option for recovering the selected SQL Server database. This page contains the following elements. Available options will depend on the selected recovery type.

Elements

Name	Description
Leave database operational	Select this option to perform a full recovery and leave the database ready to use.
Leave database non-operational but able to restore additional transaction logs	Select this option to recover the database but leave it non-operational.

Name	Description
Copy SQL transaction logs between the selected recovery point and the latest recovery point	Select this option if you want to copy transaction logs for the database restoring state. This option is disabled if no transaction logs are available for the selected database.
Copy destination	Specify the folder path location to copy SQL Server transaction logs for the database restoring state.

To continue with the recovery, click **Next**.

See Also

Select Recovery Type

DPM Self-Service Recovery Wizard

Specify Recovery Options

Use the **Specify Recovery Options** page of the Recovery Wizard to specify options to apply to recovery. This page contains the following elements. Available options will depend on the type of recovery.

Elements

Name	Description
Apply security settings of the destination computer	Select this option if you want the recovered data to have the same security settings as the destination server.  **Note** This option is available only if you are recovering databases files to a network folder.
Apply the security settings of the recovery point version	Select this option if you want the recovered data to retain its existing security settings.  **Note** This option is available only if you are recovering databases files to a network

Name	Description
	folder.
Notification	Select the **Send an e-mail when this recovery completes** check box to notify you when the recovery job is completed. **Note** The check box is enabled only if your DPM administrator had configured e-mail notifications on the DPM server.

To continue with the recovery, click **Next**.

See Also

DPM Self-Service Recovery Wizard

Summary

Use the **Summary** page of the Recovery Wizard to review your recovery settings. Click **Recover** to begin recovering your data. To change the recovery settings, click **Back**.

See Also

DPM Self-Service Recovery Wizard

DPM Self-Service Recovery Configuration Tool

System Center 2012 – Data Protection Manager (DPM) includes the DPM Self-Service Recovery Configuration Tool for SQL Server (SSRCT), which is installed on the DPM server and accessed from the **Protection** task area in DPM Administrator Console. You can use this tool to create, modify, or delete DPM roles, which enable users to perform self-service recovery of protected SQL Server databases that they own.

When self-service recovery is enabled, database owners can use the DPM Self-Service Recovery Tool (SSRT) for SQL Server to recover their databases without the need for intervention by a DPM administrator. For more information about the SSRT, see **DPM Self-Service Recovery Tool**.

In This Section

Creating a DPM Role

Modifying a DPM Role

Deleting a DPM Role

See Also

DPM Self-Service Recovery Tool

Creating a DPM Role

System Center 2012 – Data Protection Manager (DPM) includes the DPM Self-Service Recovery Configuration Tool for SQL Server (SSRCT). You can use this tool to create DPM roles, which enable SQL Server database owners to recover their databases without the need for intervention by a DPM administrator. You can configure a DPM role to control which protected databases users can recover and to which instances of SQL Server users can recover databases. Users can recover a database by using the DPM Self-Service Recovery Tool (SSRT) for SQL Server. For more information about the SSRT, see DPM Self-Service Recovery Tool.

You can also use cmdlets in DPM Management Shell to create DPM roles.

To create a DPM role, you must specify the following settings:

- **Security groups**: One or more security groups that contain the users for whom you want to enable self-service recovery of SQL Server databases.
- **Recovery items**: Instances of SQL Server and SQL Server databases that are currently protected by DPM for which you want to enable self-service recovery by users.
- **Recovery targets**: Instances of SQL Server that users can use as targeted locations to recover databases during self-service recovery.

To create a DPM role by using the DPM Self-Service Recovery Configuration Tool

1. In DPM Administrator Console, go to the **Protection** view, and then click **Configure self service recovery**.

   The DPM Self-Service Recovery Configuration Tool for SQL Server opens.
2. To create a new DPM role, click **Create Role**.
3. The Create New Role Wizard opens and guides you through the following pages to create a DPM role:
   a. Getting Started
   b. Specify Security Groups
   c. Specify Recovery Items
   d. Specify Recovery Target Locations
   e. Summary

To create a DPM role by using DPM Management Shell cmdlets

1. Create a DPM role.

   Important
   To create a DPM role, all of the following commands must be run in the following order.

   ```
   New-DPMRole -Name <NewDMPRoleName> -DPMServerName
   <DPMServerName> [-Description <DPMRoleDescription>]
   [<CommonParameters>]
   ```

2. Specify the individual users or security groups that contain the users for whom you want to enable self-service recovery of SQL Server databases.

   ```
   Add-DPMSecurityGroup -SecurityGroups
   <SecurityGroupsToAddToDPMRole> -DpmRole <DPMRoleName>
   [<CommonParameters>]
   ```

   Note
   Specified users can recover their SQL Server databases regardless of the database permissions configured on the instances of SQL Server.

3. Specify the instances of SQL Server and SQL Server databases that are currently protected by DPM for which you want to enable self-service recovery by users.

   ```
   Add-DPMRecoveryItem -Datasources <SQLServerDatabaseName> -
   Type SQLDatabase -DpmRole <DPMRoleName> [<CommonParameters>]
   ```

   -Or-

   ```
   Add-DPMRecoveryItem -SQLInstances <SQLDataSource> -Type
   SQLInstance -DpmRole <DPMRole> [<CommonParameters>]
   ```

4. Identify and add the instances of SQL Server that users can use as targeted locations to recover databases during self-service recovery.

   a. Create a recovery target object.

      ```
      New-DPMRecoveryTarget -Type SQLInstance or SQLDatabase -
      RecoveryTarget <ComputerName\InstanceName> -RecoveredFilesPath
      <FilePath> [<CommonParameters>]
      ```

   b. Add the recovery target object to the role.

      ```
      Add-DPMRecoveryTarget -DpmRole <DMPRoleName> -RecoveryTargets
      <TargetRecoveryTargetName> [<CommonParameters>]
      ```

5. Save the new DPM role.

   ```
   Set-DPMRole -DpmRole <DMPRoleName> -Confirm
   [<CommonParameters>]
   ```

See Also

Modifying a DPM Role

Deleting a DPM Role

Getting Started

You can use wizards to create, modify, or delete a DPM role.

Getting Started page

Read the contents on this page, and then click **Next**.

See Also

Creating a DPM Role

Specify Security Groups

Use this page to specify a name and optionally a description for a new role, and to specify one or more security groups that contain users that this DPM role applies to, or one or more individual users that this DPM role applies to.

Note
Specified users can recover their SQL Server databases regardless of the database permissions configured on the instances of SQL Server.

Specify Security Groups page

To specify a security group or an individual user, click **Add**, and then type a security group in the following format, *domain\security group*, or an individual user in the following format, *domain\user name*.

Note
You can add multiple security groups and users to a DPM role.

To remove a security group or user, select it in the **Security Group** list, and then click **Remove**.

After you have specified all required information, click **Next**.

See Also

Creating a DPM Role

Specify Recovery Items

Use this page to specify instances of SQL Server and SQL Server databases that users for this DPM role can recover.

Note
You can specify multiple instances of SQL Server and SQL Server databases for a DPM role.

Specify Recovery Items page

To specify an instance of SQL Server as a recovery item, click **Add**, and then type the instance name in the following format, <*computer name**instance name*>, and optionally, to specify an SQL Server database, press the TAB key, and then type a database name, or to enable users of this role to recover all databases on the instance, press the TAB key, and then press the Spacebar to clear the text in the **Database Name** column.

Important
When you enable users of a DPM role to recover all SQL Server databases on an instance of SQL Server, those users can also recover any SQL Server databases that are subsequently added to the instance. When you enable access by using DPM roles, ensure that all members of the role have been granted appropriate permission to view and access all databases.

To remove an instance of SQL Server, select it in the **SQL Server Instance** list, and then click **Remove**.

After you have provided all required information, click **Next**.

See Also

Creating a DPM Role

Specify Recovery Target Locations

Use this page to specify one or more recovery target locations and file paths to restrict where users of this DPM role can recover the files for their specified databases. You do not need to specify recovery target locations or paths for users of this DPM role to recover their SQL Server databases files. If you do not restrict the recovery target locations, at the time of recovery, the users can recover database files to any location for which they have write permission. However, users cannot overwrite the original database files, and the DPM Self-Service Recovery Tool (SSRT) for SQL Server blocks them if they attempt to do so. If you do not want to specify recovery target locations for users, leave the **Allow users to recover the databases to another instance of SQL Server** check box clear, and then click **Next**.

Specify Recovery Target Locations page

To restrict the locations to which users can recover SQL Server database files, select the **Allow users to recover the databases to another instance of SQL Server** check box, click **Add**, and then type an instance of SQL Server in the **SQL Server Instance** column, and optionally type a path in the **Recovered File Path** column where users of this role can recover their SQL Server database files, or to enable users to recover to any path on the instance, press the TAB key, and then press the Spacebar to clear the text in the **Recovered File Path** column.

If all of the users for this role are SQL Server database administrators, you might want to enable them to recovery their database files to any location on an instance of SQL Server. However, if the users are not SQL Server administrators, you might want to restrict the locations to which they can recover the database files so that they do not affect the functioning of other SQL Server databases.

Note

You can specify multiple instances of SQL Server.

To remove a recovery target location, select the instance in the **SQL Server Instance** list, and then click **Remove**.

After you have provided all required information, click **Next**.

See Also

Creating a DPM Role

Summary

Use this page to review the settings for the DPM role before you finish creating it.

Summary page

Review the settings on this page, and then click **Finish** to close the wizard and create the role. To change any setting, click **Back**.

See Also

Creating a DPM Role

Modifying a DPM Role

System Center 2012 – Data Protection Manager (DPM) includes the DPM Self Service Recovery Configuration Tool for SQL Server (SSRCT). You can use this tool to create DPM roles, which

enable SQL Server database owners to recover their databases without the need for intervention by a DPM administrator. You can configure a DPM role to control what users can recover and to which instances of SQL Server users can recover databases. Users can recover a database by using the DPM Self-Service Recovery Tool (SSRT) for SQL Server. For more information about the SSRT, see DPM Self-Service Recovery Tool.

You can also use cmdlets in DPM Management Shell to create DPM roles.

To create a DPM role, you must specify the following settings:

- **Security groups**: One or more individual users or security groups that contain the users for whom you want to enable self-service recovery of SQL Server databases.
- **Recovery items**: Instances of SQL Server and SQL Server databases that are currently protected by DPM for which you want to enable self-service recovery by users.
- **Recovery targets**: Instances of SQL Server that users can use as targeted locations to recover databases during self-service recovery.

To modify a DPM role by using the DPM Self-Service Recovery Configuration Tool

1. In DPM Administrator Console, go to the **Protection** view, and then click **Self service recovery**.

   The DPM Self-Service Recovery Configuration Tool for SQL Server opens.
2. To modify a DPM role, select the role, and then click **Modify**.
3. The Modify Role Wizard opens and guides you through the following pages to modify a DPM role:
   a. Getting Started
   b. Specify Security Groups
   c. Specify Recovery Items
   d. Specify Recovery Target Locations
   e. Summary

To rename a DPM role by using DPM Management Shell cmdlets

1. Open the DPM role for editing.

```
Get-DPMRole -Name <DMPRoleName> -DPMServerName
<DPMServerName> -Editable <SwitchParameter>
[<CommonParameters>]
```

2. Rename the DPM role.

```
Rename-DPMRole -Name <NewDMPRoleName> [-Description
<DPMRoleDescription>] -DpmRole <DPMRoleName>
[<CommonParameters>]
```

Note
Users in the specified security groups can recover their SQL Server databases regardless of the database permissions configured on the instances of SQL

Server.

3. Save the modified DPM role.

```
Set-DPMRole -DpmRole <DMPRoleName> -Confirm
[<CommonParameters>]
```

To remove a recovery target location

1. Open the DPM role for editing.

```
Get-DPMRole -Name <DMPRoleName> -DPMServerName
<DPMServerName> -Editable <SwitchParameter>
[<CommonParameters>]
```

Note
The fully qualified domain name (FQDN) is required when removing a targeted location.

2. Remove the recovery target location.

```
Remove-DPMRole -DpmRole <DMPRoleName> [<CommonParameters>]
```

3. Save the modified DPM role.

```
Set-DPMRole -DpmRole <DMPRoleName> -Confirm
[<CommonParameters>]
```

See Also

Creating a DPM Role

Deleting a DPM Role

Deleting a DPM Role

System Center 2012 – Data Protection Manager (DPM) includes the DPM Self-Service Recovery Configuration Tool for SQL Server (SSRCT). You can use this tool to delete DPM roles, which enable SQL Server database owners to recover their databases without the need for intervention by a DPM administrator. You can configure a DPM role to control which protected databases a user can recover and to which instances of SQL Server users can recover databases. A user can recover a database by using the DPM Self-Service Recovery Tool (SSRT) for SQL Server. For more information about the SSRT, see **DPM Self-Service Recovery Tool**.

You can also use cmdlets in DPM Management Shell to delete DPM roles.

To delete a DPM role by using the DPM Self-Service Recovery Configuration Tool

1. In DPM Administrator Console, go to the **Protection** view, and then click **Self service recovery** .

The DPM Self-Service Recovery Configuration Tool for SQL Server opens.

2. To delete a DPM role, select the role, and then click **Delete**.

To delete a DPM role by using DPM Management Shell cmdlets

1. Open the DPM role.

```
Get-DPMRole -Name <DMPRoleName> -DPMServerName
<DPMServerName> -Editable <SwitchParameter>
[<CommonParameters>]
```

2. Delete the DPM role.

```
Remove-DPMRole -DPMRole <DMPRoleName> [<CommonParameters>]
```

See Also

Creating a DPM Role

Modifying a DPM Role

Accessibility for People with Disabilities

Microsoft is committed to making its products and services easier for everyone to use. The following topics provide information about the features, products, and services that make System Center 2012 – Data Protection Manager (DPM) more accessible for people with disabilities.

In This Section

Accessibility Features of DPM

Describes the accessibility features of DPM.

Accessibility Features of DPM Help

Describes the accessibility features of DPM Help.

Accessibility Products and Services from Microsoft

Describes the accessibility products and services that are available from Microsoft.

Accessibility Features of DPM

In addition to accessibility features and utilities in Microsoft Windows, System Center 2012 – Data Protection Manager (DPM) has keyboard shortcuts on all dialog boxes and wizard screens. You can access these commands by using a combination of the Alt key plus the underscored letter in the menu command.

Note

The information in this section may apply only to users who license Microsoft products in the United States. If you obtained this product outside of the United States, you can use the subsidiary information card that came with your software package or visit the Microsoft Accessibility website for a list of Microsoft support services telephone numbers and addresses. You can contact your subsidiary to find out whether the type of products and services described in this section are available in your area. Information about accessibility is available in other languages, including Japanese and French.

Accessibility Features of DPM Help

System Center 2012 – Data Protection Manager (DPM) Help includes features that make it accessible to a wider range of users, including those who have limited dexterity, low vision, or other disabilities. In addition, DPM Help is available on the Web at http://go.microsoft.com/fwlink/p/?LinkId=227136.

Keyboard Shortcuts for Using Help

By using the following keyboard shortcuts in Help, you can quickly accomplish many common tasks.

To do this	Use this keyboard shortcut
Display the Help window.	F1
Switch the cursor between the Help topic pane and the navigation pane (tabs such as **Contents**, **Search**, and **Index**).	F6
Change between tabs (for example, **Contents**, **Search**, and **Index**) while in the navigation pane.	ALT + Underlined letter of the tab
Select the next hidden text or hyperlink.	TAB
Select the previous hidden text or hyperlink.	SHIFT+TAB

To do this	Use this keyboard shortcut
Perform the action for the selected Show All, Hide All, hidden text, or hyperlink.	ENTER
Display the **Options** menu to access any Help toolbar command.	ALT+O
Hide or show the pane containing the **Contents**, **Search**, and **Index** tabs.	ALT+O, and then press T
Display the previously viewed topic.	ALT+O, and then press B
Display the next topic in a previously displayed sequence of topics.	ALT+O, and then press F
Return to the specified home page.	ALT+O, and then press H
Stop the Help window from opening a Help topic (useful if you want to stop a Web page from downloading).	ALT+O, and then press S
Open the **Internet Options** dialog box for Windows Internet Explorer, where you can change accessibility settings.	ALT+O, and then press I
Refresh the topic (useful if you have linked to a Web page).	ALT+O, and then press R
Print all topics in a book or a selected topic only.	ALT+O, and then press P
Close the Help window.	ALT+F4

Procedures

To change the appearance of a Help topic

1. To customize the colors, font styles, and font sizes used in Help, open the Help window.
2. Click **Options**, and then click **Internet Options**.
3. On the **General** tab, click **Accessibility**. Select **Ignore colors specified on Web pages**, **Ignore font styles specified on Web pages**, and **Ignore font sizes specified on Web pages**. You also can choose to use the settings specified in your own style sheet.
4. To change the colors used in Help, see "To change the color of the background or text in Help". To change the font, see "To change the font in Help."

To change the color of the background or text in Help

1. Open the Help window.
2. Click **Options**, and then click **Internet Options**.
3. On the **General** tab, click **Accessibility**. Then, select **Ignore colors specified on Web pages**. You also can choose to use the settings specified in your own style sheet.
4. To customize the colors used in Help, on the **General** tab, click **Colors**. Clear the **Use Windows Colors** check box, and then select the font and background colors that you want to use.

   Note
   If you change the background color of the Help topics in the Help window, the change also affects the background color when you view a Web page in Windows Internet Explorer.

To change the font in Help

1. Open the Help window.
2. Click **Options**, and then click **Internet Options**.
3. On the **General** tab, click **Accessibility**. To use the same settings as those used in your instance of Windows Internet Explorer, select **Ignore font styles specified on Web pages** and **Ignore font sizes specified on Web pages**. You also can choose to use the settings specified in your own style sheet.
4. To customize the font style used in Help, on the **General** tab, click **Fonts**, and then click the font style you want.

   Note
   If you change the font of the Help topics in the Help window, the change also affects the font when you view a Web page in Internet Explorer.

Accessibility Products and Services from Microsoft

Microsoft is committed to making its products and services easier for everyone to use. The following sections provide information about the features, products, and services that make Microsoft® Windows® more accessible for people with disabilities:

- Accessibility Features of Windows
- Documentation in Alternative Formats
- Customer Service for People with Hearing Impairments
- For More Information

Note

The information in this section may apply only to users who license Microsoft products in the United States. If you obtained this product outside of the United States, you can use the subsidiary information card that came with your software package or visit the Microsoft Accessibility website for a list of Microsoft support services telephone numbers and addresses. You can contact your subsidiary to find out whether the type of products and services described in this section are available in your area. Information about accessibility is available in other languages, including Japanese and French.

Accessibility Features of Windows

The Windows operating system has many built-in accessibility features that are useful for individuals who have difficulty typing or using a mouse, are blind or have low vision, or who are deaf or hard-of-hearing. The features are installed during Setup. For more information about these features, see Help in Windows and the Microsoft Accessibility website.

Free Step-by-Step Tutorials

Microsoft offers a series of step-by-step tutorials that provide detailed procedures for adjusting the accessibility options and settings on your computer. This information is presented in a side-by-side format so that you can learn how to use the mouse, the keyboard, or a combination of both. To find step-by-step tutorials for Microsoft products, see the Microsoft Accessibility website.

Assistive Technology Products for Windows

A wide variety of assistive technology products are available to make computers easier to use for people with disabilities. You can search a catalog of assistive technology products that run on Windows at the Microsoft Accessibility website. If you use assistive technology, be sure to contact your assistive technology vendor before you upgrade your software or hardware to check for possible compatibility issues.

Documentation in Alternative Formats

If you have difficulty reading or handling printed materials, you can obtain the documentation for many Microsoft products in more accessible formats. You can view an index of accessible product documentation on the Microsoft Accessibility website. In addition, you can obtain additional Microsoft publications from Learning Ally (formerly Recording for the Blind & Dyslexic, Inc.). Learning Ally distributes these documents to registered, eligible members of their distribution service. For information about the availability of Microsoft product documentation and books from Microsoft Press, contact:

Learning Ally (formerly Recording for the Blind & Dyslexic, Inc.)
20 Roszel Road
Princeton, NJ 08540

Telephone number from within the United States: (800) 221-4792
Telephone number from outside the United States and Canada: (609) 452-0606
Fax: (609) 987-8116
Learning Ally website

Web addresses can change, so you might be unable to connect to the website or sites mentioned here.

Customer Service for People with Hearing Impairments

If you are deaf or hard-of-hearing, complete access to Microsoft product and customer services is available through a text telephone (TTY/TDD) service:

- For customer service, contact Microsoft Sales Information Center at (800) 892-5234 between 6:30 AM and 5:30 PM Pacific Time, Monday through Friday, excluding holidays.
- For technical assistance in the United States, contact Microsoft Product Support Services at (800) 892-5234 between 6:00 AM and 6:00 PM Pacific Time, Monday through Friday, excluding holidays. In Canada, dial (905) 568-9641 between 8:00 AM and 8:00 PM Eastern Time, Monday through Friday, excluding holidays.

Microsoft Support Services are subject to the prices, terms, and conditions in place at the time the service is used.

For More Information

For more information about how accessible technology for computers helps to improve the lives of people with disabilities, see the Microsoft Accessibility website.

Using the DPM Client

System Center 2012 – Data Protection Manager (DPM) enables you to protect and recover the files and folders on your computer in case of data loss or corruption. Your backup administrator configures backup and protection for your computer according to your company protection policy and gives you the ability to manage your backups so that you can perform your own data recoveries.

In This Section

Recover files and folders on your computer

Troubleshoot DPM Client issues

Getting started with the DPM Client

The Client for System Center 2012 – Data Protection Manager (DPM) includes features that make your protected files and folders available to you from the DPM icon displayed in the notification area (also known as the system tray). By default, when you are running the DPM Client, the DPM icon appears in the notification area. When you move the mouse pointer over the DPM icon, the DPM synchronization status information is displayed. For example, **Last sync: 1 hour ago, Automatically every 4 hrs**.

The following options are available when you click the DPM icon in the notification area:

Options

Name	Description
Synchronize now	Starts the synchronization process. When the synchronization process is running, the link changes to **Cancel Synchronization**.
Open DPM Client	Opens the DPM Client, and displays the last viewed tab. To view the company protection policy information set by your backup administrator, on the **Summary** tab, click the **Company Protection Policy** link.
Recover data	Opens the DPM Client, and displays the **Recovery** tab.
Help	Starts DPM Client Help. Provides feature overviews and procedures for performing protection and recovery tasks.

Understand DPM Client protection

What is synchronization?

What happens when I synchronize my data?

When should I synchronize my data?

What is a recovery point?

How do I access my recovery points on the DPM server?

What is synchronization?

When the data changes on your computer, System Center 2012 – Data Protection Manager (DPM) makes a point-in-time copy of your files and folders and copies them to the DPM server. This synchronization process keeps the data on your computer synchronized with the data on the DPM server.

What happens when I synchronize my data?

When you synchronize your data, the changes to the data on your computer are copied to a replica on the server for System Center 2012 – Data Protection Manager (DPM). You synchronize the data on your computer to keep it consistent with the data on the DPM server. Note that the data that you synchronize is not immediately available for recovery. The data will become available for recovery when DPM creates a recovery point, which you will be able to see from the recovery point schedule.

When should I synchronize my data?

You want to synchronize your data according to the amount of data loss you are prepared to sustain. For example, if you synchronize your data just once each day, System Center 2012 – Data Protection Manager (DPM) will restore your data to within a day of a data loss event. If you set up an hourly synchronization schedule, DPM will restore your data to within an hour of a data loss event.

What is a recovery point?

To protect your data, System Center 2012 – Data Protection Manager (DPM) starts by creating a complete point-in-time copy of the files and folders you want to protect on your computer. This copy is called a replica. A recovery point is a point-in-time copy of the replica and it is stored on the DPM server. If you experience data loss or corruption, you can access the recovery points of a previous version of your files and folders to recover your data.

How do I access my recovery points on the DPM server?

You use the Client for System Center 2012 – Data Protection Manager (DPM) to search for your recovery points. Available recovery points are listed in the DPM Client in the display pane and include the time stamps and the open links (backup folder locations on the DPM server) for each of the available recovery points.

Manage protected files and folders

The Client for System Center 2012 – Data Protection Manager (DPM) provides you with current information about your protected files and folders and gives you options to synchronize changes from your computer to the DPM server.

Viewing information and synchronize files and folders

Protecting the files and folders in your computer

Viewing information and synchronize files and folders

The Client for System Center 2012 – Data Protection Manager (DPM) enables you to view summarized information and synchronize your protected files and folders.

To view summarized information and synchronize protected items

1. Click **Start**, point to **All Programs**, click **System Center 2012 – Data Protection Manager (DPM)**, and then click **DPM Client**.

   The DPM Client appears in the task tray.

   Note
   The DPM icon may be hidden by default in Windows 7.
2. In the **Data Protection Manager Client**, click the **Summary** tab.
3. On the **Summary** tab, DPM provides information about disk space that is used by the protected items. The first section lists the last time a synchronization was successfully performed and the synchronization schedule.

   If you experience issues with synchronizing your data, click the **Details** link. The **Backup Failure Details** dialog box appears, which contains a link that your backup administrator can use to display troubleshooting details.

   To synchronize your files and folders at this time, click **Synchronize Now**.
4. To view the company protection policy information set by your backup administrator, on the **Summary** tab, click the **Company Protection Policy** link.
5. The second section displays the latest recovery point on the DPM server, which is the time interval since the last time the recovery point was created.

Protecting the files and folders in your computer

In addition to the files and folders that are backed up by default, your company protection policy may allow you to configure additional files and folders for backup. This setting is controlled by your backup administrator.

Contact your backup administrator to give you permission to configure protection of additional files and folders. You can use the steps described in this section to configure protection.

To protect data items

1. Click **Start**, point to **All Programs**, click **System Center 2012 – Data Protection Manager (DPM)**, and then click **Data Protection Manager Client**.
2. In the **Data Protection Manager Client**, click the **Protected Items** tab.
3. Select the files and folders that you want to protect in the tree view, and then click **OK**.

   To determine the data size of the selected files and folders, click **Calculate**.

   Note
   By default, the company protection policy set by your backup administrator might cause some files and folders to be un-protectable or protectable. To view your company protection policy, on the **Summary** tab, click the **Company Protection Policy** link.

Recover files and folders on your computer

With System Center 2012 – Data Protection Manager (DPM) you can recover your files and folders from your computer in case of data loss or corruption. You start protecting your data by creating recovery points, also referred to as local snapshots of the files and folders on your computer. Your DPM administrator sets a recovery point schedule according to your company protection policy.

Important
Local snapshots cannot be created on Microsoft Windows XP client computers.

Recovering from backups stored locally

Recovering from backups stored on the DPM server

Recovering from backups stored locally

With System Center 2012 – Data Protection Manager (DPM), you can recover files and folders from backups that are stored locally on your computer.

Note
By default, DPM allows only the local administrator to perform recoveries on the computer. For more information, see Enabling non-administrators to recover files

1. Right-click any file or folder that you want to restore, and then click **Restore previous**

versions.

In the **Properties** dialog box, on the **Previous Versions** tab, there is a list of available previous versions of the file or folder. The list includes files and folders that are saved to a backup as well as local recovery points.

2. Before you restore a previous version of a file or a folder, ensure that it is the correct version. To do this, select the previous version, and then click **Open** to view its contents.
3. After you verify that it is the correct version of the file or folder, click **Restore**.

Enabling non-administrators to recover files

If you want to allow users who are not administrators on a computer to recover files, you must create the following registry key on the protected computer.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent\ClientProtection
Value	ClientOwners
Data	Comma-separated list of users who should be allowed to perform recoveries on this computer.
Type	String

Recovering from backups stored on the DPM server

System Center 2012 – Data Protection Manager (DPM) enables you to recover files and folders from backups stored on the DPM server that are managed by your backup administrator. To recover your data, you need to know the name of the DPM server on which the data was backed up. To find out the name of the DPM server, contact your backup administrator.

To recover data from backups stored on the DPM server

1. Click **Start**, point to **All Programs**, click **System Center 2012 – Data Protection Manager (DPM)**, and then click **Data Protection Manager Client**.
2. In the DPM Client, click the **Recovery** tab.
3. In the **Search for recovery points on** text box, type the name of DPM server on which the data was backed up, or click the **Search** button to start the search for the existing recovery points on the DPM server.

   Note
   To find out the name of the DPM server, contact your backup administrator.
4. To access the backups stored on the DPM server, in the list of files and folders, click the

open link that belongs to the respective recovery points.

Note
Available recovery points are listed in the display pane. In the display pane, the **Time** column lists the time stamps and the **Link** column lists the open links (backup folder locations on the DPM server) for the each available recovery points.

5. Select the previous version you want to restore and then click **Restore**.

Troubleshoot DPM Client issues

The following table provides guidance for troubleshooting issues that may occur when you use the Client for System Center 2012 – Data Protection Manager (DPM) to protect data on your computer.

Issue	Cause	Resolution
In DPMClient, on the **Summary** tab, the **Current status** displays **Unable to contact DPM server**.	The client computer is not connected to the corporate network. -OR- The DPM server is unavailable.	Retry the operation after you connect to the corporate network. If you still cannot contact the DPM server, ask your backup administrator to make sure that the DPM server is running.
On the **Summary** tab of the Data Protection Manager dialog box, the **Current Status** displays **Client not configured for protection**.	The client computer has not been added to the protection group list on the DPM server.	Contact your backup administrator. To troubleshoot this issue, they must do the following: Add the client computer to an existing protection group on the DPM server. -OR- Create a new protection group for the client computer on the DPM server.

Managing System Protection

System protection aims to protect you against two scenarios – one where your computer starts, but you have lost system files and registry; and the other where the computer does not start and you have to recover everything. System Center 2012 – Data Protection Manager (DPM) enables you to protect your computer against both these scenarios.

In the past, disaster recovery entailed rebuilding a computer from scratch. This meant installing the operating system, applying updates, installing applications, and then finally recovering data. This was a laborious and error-prone method. DPM saves you the time and trouble of rebuilding your system.

In DPM, System State protection consists of protecting the operating system files, and bare metal recovery (BMR) protection consists of protecting the operating system files and all data except user data on critical volumes.

DPM uses Windows Server Backup (WSB) to perform System State backup and BMR backup. For recovery, DPM will retrieve the backups and you will use the backup data to perform recovery by using WSB.

Prerequisites

- Windows Server Backup installed on the protected computer for BMR.
- Windows Recovery Environment (WinRE) for BMR.

Unsupported Scenarios

The following scenarios are not supported for BMR:

- Computers running Windows Server 2003.
- Computers running client operating systems like Windows XP or Windows Vista or Windows 7.
- A DPM server cannot protect itself for BMR.
- Disk-Tape protection is not supported for BMR. However, long-term to tape with short-term to disk (D-D-T) is supported.

In This Section

Migrating Between System State and BMR Protection
Setting Up Disaster Recovery

Prescriptive Guidance on BMR vs. System State by Data Source

This section provides guidance on how you can effectively use System Center 2012 – Data Protection Manager (DPM) to protect your system information. The information is grouped by data source, so you can decide when to use BMR protection and when to use System State protection.

Unified Backup Strategy

File Servers

- File system backup for data protection.
- BMR backup for system protection.

	Recovery Strategy
Lost file data	File recovery using DPM
Lost or damaged operating system	System State recovery using BMR backup
Lost server (data volumes intact)	BMR recovery using BMR backup
Lost server (data volumes also lost)	BMR recovery followed by file recovery

SharePoint Farm

- SharePoint farm backup for farm data.
- BMR backup on Web front-end server to protect IIS role.
- BMR or System State backup for servers hosting content database.

	Recovery Strategy
Lost site, lists, list items, documents	SharePoint recovery using DPM
Lost or damaged operating system	System State recovery using BMR backup
Disaster recovery	BMR recovery using BMR backup

Hyper-V Virtual Machines

- Hyper-V host-level backup to protect virtual machines.
- BMR backup of host computer at least once a day.

	Recovery Strategy
Lost virtual machine	Use Hyper-V recovery features
Lost or damaged operating system	System State recovery using BMR backup
Lost Hyper-V host (virtual machine intact)	BMR recovery using BMR backup
Lost Hyper-V host (virtual machine also lost)	BMR recovery followed by Hyper-V recovery

SQL Server or Exchange Server

- Application backup to protect data.
- BMR backup for system protection.

	Recovery Strategy
Lost application data	Application-specific recovery using DPM
Lost or damaged operating system	System State recovery using BMR backup
Lost server (database and transaction log files intact)	BMR recovery using BMR backup
Lost server (database and transaction log files also lost)	BMR recovery followed by application-specific recovery

Setting Up BMR Protection

In System Center 2012 – Data Protection Manager (DPM), BMR protection covers protection for operating system files (System State) and critical volumes (excluding user data).

Tip
If your application is installed on a critical volume, you will also be able to restore the application as part of BMR. However, application data is not backed up as part of BMR.

You can set up BMR protection for a computer by using the Create New Protection Group Wizard. You can select BMR protection from under the **System Protection** node on the **Select Group Members** page of the wizard.

Space Requirements

Unlike System State protection, DPM does not have any space requirements on the protected computer for BMR protection. WSB directly transfers the backups to the DPM server.

Warning

DPM will not show you the progress of this job in the Jobs view.

DPM reserves 30 GB of space on the replica volume for BMR. You can change this by using the **Disk Allocation** page in the Modify Protection Group Wizard or the **Get-DatasourceDiskAllocation** and **Set-DatasourceDiskAllocation** cmdlets.

On the recovery point volume, BMR protection requires about 6 GB for retention of five days.

Note

DPM does not calculate the size of BMR data source, but assumes 30 GB for all servers. Admins should change the value as per the size of BMR backups expected on their environments.

Size of BMR backup can be roughly calculated sum of used space on all critical volumes.

Critical volumes = Boot Volume + System Volume + Volume hosting system state data such as AD DIT/log volumes.

Setting Up BMR Protection

1. Install the DPM protection agent on the computer you want to protect. You need to do this only if the protection agent is not already installed on the computer.
2. Using the Create New Protection Group Wizard, add the computer you want to protect to a protection group. BMR will appear as a data source under the **System Protection** node.

When you select BMR, System State gets selected automatically because BMR backup also protects System State for the computer.

Warning

When you stop protection for BMR, System State protection is not stopped automatically. You must specifically clear the **System State** check box to stop System State protection.

Things to Remember

- You cannot protect BMR and System State for the same computer on different protection groups.
- You cannot reduce the replica volume size to less than 15 GB.

See Also

Managing System Protection

Setting Up System State Protection

In System Center 2012 – Data Protection Manager (DPM), System State protection covers protection for operating system files.

You can set up System State protection for a computer by using the Create New Protection Group Wizard. You can select **System State** from under the **System Protection** node on the **Select Group Members** page of the wizard.

Tip
We recommend that you protect BMR for complete protection of your computer.

Space Requirements

For System State protection, WSB first creates a local dump of the System State information and then transfers it to the DPM server. The local dump will typically require 15 GB of space on the computer. If there is insufficient space on the computer, WSB will fail the backup.

Warning
DPM will show the progress of this job in the Jobs view only when data transfer begins.

Setting Up System State Protection

1. Install the DPM protection agent on the computer you want to protect. You need to do this only if the protection agent is not already installed on the computer.
2. Using the Create New Protection Group Wizard, add the computer you want to protect to a protection group. System State will appear as a data source under the **System Protection** node.

Things to Remember

You cannot protect System State and BMR for the same computer on different protection groups.

See Also

Managing System Protection

Setting Up DPM Chaining

Chaining, as the name suggests, lets you create a chain of System Center 2012 – Data Protection Manager (DPM) servers protecting the next DPM server in the chain.

Cyclic protection is aimed at smaller architectures like in a branch office, where two DPM servers can protect each other.

To set up chaining

1. Install the DPM protection agent on the DPM server that you want to protect from the DPM server you want to protect it from.
2. Configure secondary protection for the data sources protected by the DPM server you are protecting.

Note
In the DPM Administrative Console of one DPM server, you cannot view the data sources that the DPM protection agent already protects. This feature prevents you from protecting data sources repeatedly.

Assume an architecture where you have two DPM servers, DPM1 and DPM2. Each of these servers protects one or more data sources of their own. To set up chaining for these two servers, do the following:

1. Install the DPM protection agent from DPM1 to DPM2 and vice versa.
2. Configure secondary protection on DPM2 for servers that DPM1 protects.
3. Configure secondary protection on DPM1 for servers that DPM2 protects.

What is protected on the DPM server

In DPM, the secondary DPM server supports protection for the following items from the primary DPM server:

- The databases in the instance of SQL Server on the primary DPM server.
- All local volumes and application data on the primary DPM server.
- All replicas on the primary DPM server that the primary DPM server directly protects.

Recovering BMR

You need to do a bare metal recovery (BMR) in the following situations:

- Protected computer does not start
- Planned migration
- Unplanned migration
- Hard disk failure

Procedure to Recover BMR

1. On the DPM server, use the Recovery Wizard to recover the last good BMR recovery point to an alternative location.

Warning
Computers in WinPE cannot connect to network shares that have IPsec enabled. The computer should be an IPsec boundary computer so that a computer that is not joined to the domain can access the network share by using a username and password.

2. Start the protected computer using Windows Recovery Environment (WinRE) and go to the command shell.
3. Using the command shell, enable networking - `start /w wpeinit`
4. Using the command shell, retrieve the version of the backup from the restored image - `Wbadmin get versions –backuptarget:\\<computername>\serverbackup$`
5. Using the command shell, start system recovery - `Wbadmin.exe start sysrecovery –version:<version ID from Step 2> -backuptarget:\\<computername>\ServerBackup$ -recreatedisks`

See Also

Managing System Protection

Recover the Operating System or Full Server

Windows Server Backup 2008 Restore from Network Location

Recovering System State

You will do a System State recovery when your computer is able to boot up, but the system files and registry are lost.

Procedure to Recover System State

1. On the DPM server, use the Recovery Wizard to recover the last good System State recovery point to an alternative location.

   Warning
   Start the computer that you want to recover.
2. Start Windows Server Backup.
3. Click **Recover** in the **Actions** pane.
4. Click **This Server**, and then click **Next**.
5. Click **Another Server**. On the **Specify Location Type** page, select **Remote shared folder**. Provide the path to the folder that contains the recovery point. Click **Next**.
6. On the **Select Recovery Type** page, click **System state**, and then click **Next**.
7. On the **Select Location for System State Recovery** page, click **Original Location**, and then click **Next**.

8. On the **Confirmation** page, click **Recover**.
9. After successful recovery of the system state of your computer, you can complete the recovery process using the instructions on the following pages:
   a. For Windows 2008: Recovering Your Server
   b. For Windows 2008 R2: Recover the System State
   c. For Windows 2003: Restore System State data

See Also

Managing System Protection

Recover the System State

Migrating Between System State and BMR Protection

Migrating from System State to BMR Protection

To migrate from System State protection to BMR protection, modify the protection group and select BMR protection. System State will remain selected. Complete the wizard for the changes to take effect.

BMR protection requires less space on the recovery point volume. However, the extra space on the volume is not reclaimed. You can shrink the volume size from the **Modify Disk Allocation** page of the Modify Protection Group Wizard or by using the **Get-DatasourceDiskAllocation** and **Set-DatasourceDiskAllocation** cmdlets.

BMR protection will require more space on the replica volume. The volume will be extended automatically. If you want to change the default space allocations you can use **Modify-DiskAllocation**.

Warning
Disaster Replica will fail because of increased space needs. You must manually increase the space allocation on the server.

Migrating from BMR to System State Protection

You can stop protecting a computer for BMR by using the Modify Protection Group Wizard. When you stop protecting for BMR and retain protection of System State, you must consider the following:

- You will require more space on the recovery point volume.
- You will require space on the protected computer because System State protection first writes the replica to the local computer and then transfers it to the DPM server.

Important

Because of the increased space requirement on the replica volume, DPM may try to automatically grow the volume. If there is insufficient space in the storage pool, you will see an error indicating this.

Tip

If you are trying to remove BMR protection to free up disk space, you must stop protection of BMR and System State.

See Also

Managing System Protection

Setting Up Disaster Recovery

System Center 2012 – Data Protection Manager (DPM) enables you to protect your data sources on a secondary DPM server, preferably at a remote location, as a backup to your primary DPM server for disaster recovery. A disaster can take the following forms:

- The primary DPM server and the protected computers are lost.
- Only the primary DPM server is lost.

In the first case, having a secondary DPM server in a remote location enables you to recover your protected computers quickly. In the second case, you can switch protection so that the secondary DPM server takes over as the primary DPM server for the protected computers until another computer can be set up as the primary DPM server.

Setting Up Protection on a Secondary DPM Server

1. From the secondary DPM server, in the **Management** task area, install a protection agent on the primary DPM server. For step-by-step instructions for installing a protection agent, see Installing and Configuring Protection Agents.
2. On the secondary DPM server, in the **Protection** task area, use the Create New Protection Group Wizard to add the primary DPM server to a protection group. For step-by-step instructions for creating a new protection group, see Creating Protection Groups.

   Tip

   The retention range on the secondary server should be greater than the frequency of Express Full on the primary DPM server.
3. In the Create New Protection Group Wizard, expand the primary DPM server, expand the members under the primary DPM server, and then select which members you want to protect, for example, the DPM database (DPMDB) and computers that are protected on the primary DPM server. When you expand the protected computers, you see System Protection if either bare metal recovery (BMR) or System State is enabled for them.

Note
On the secondary DPM server, the Create New Protection Group Wizard does not differentiate between BMR and System State protection. If either is protected, it appears as System Protection.

Important
We strongly recommend that you protect the DPMDB on the secondary DPM server.

Important
If your primary DPM server is protecting a SharePoint farm, you must provide sufficient time for the secondary DPM server to back up the primary DPM server before the next scheduled backup of the primary DPM server starts. By using the Modify Protection Group Wizard, you can specify when you want the primary DPM server backup to start.

Migrating Between BMR and System State Protection on the Primary DPM Server

If you change system protection from BMR to System State or vice versa for a computer that is protected by the primary DPM server, the disk allocation changes are not automatically applied to the secondary DPM server. You must manually check to see whether the changes are applied correctly.

Improving Usage of WAN Latency

If your deployment of System Center 2012 – Data Protection Manager (DPM) for disaster recovery requires DPM to send large amounts of data over a WAN, you can improve DPM's use of your WAN latency by adjusting the following registry settings:

On the remote DPM server:

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize`

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts`

On the DPM server:

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts`

For example, using the following settings over a 100 Mbps link with 40 ms latency produces the following results:

Settings	
On the remote DPM server: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize`	524288
On both DPM servers: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp132`	3

`3Opts`	
Results	
One job running	3.45 MB/sec
Three jobs running	~3.00 MB/sec per job

Using DPMSync

DpmSync is a command-line tool that enables you to synchronize the DPM database with the state of the disks in the storage pool and with the installed protection agents. The DpmSync tool restores the DPM database, synchronizes the DPM database with the replicas in the storage pool, restores the Report database, and reallocates missing replicas.

DpmSync Syntax

DpmSync **–RestoreDb –DbLoc location –InstanceName server\instance**]

DpmSync **-Sync**

DpmSync **-ReallocateReplica**

DpmSync **-DataCopied**

Parameters

Parameter	Description
-RestoreDb	Restores a DPM database from a specified location.
-Sync	Synchronizes restored databases. You must run DpmSync –Sync after you restore the databases. After you run DpmSync –Sync, some replicas may still be marked as missing.
-DbLoc *location*	Identifies the location of backup of DPM database.
-InstanceName *server\instance*	Instance to which DPMDB must be restored.
-ReallocateReplica	Reallocates all missing replica volumes without synchronization.
-DataCopied	Indicates that you have completed loading data into the newly allocated replica volumes.

Parameter	Description
	This is applicable for client computers only.

Example 1: To restore the DPM database from local backup media on the DPM server.
Run the following command:

DpmSync –RestoreDb -DbLoc G:\DPM\Backups\2005\November\DPMDB.bak

After you restore the DPM database, to synchronize the databases, you run the following command:

DpmSync -Sync

After you restore and synchronize the DPM database and before you restore the replica, you run the following command to reallocate disk space for the replica:

DpmSync -ReallocateReplica

Example 2: To restore the DPM database from a remote database.
Run the following command on the remote computer:

DpmSync –RestoreDb -DbLoc G:\DPM\Backups\2005\November\DPMDB.bak –InstanceName contoso\ms$dpm

After you restore the DPM database, to synchronize the databases, you run the following command on the DPM server:

DpmSync -Sync

After you restore and synchronize the DPM database and before you restore the replica, you run the following command on the DPM server to reallocate disk space for the replica:

DpmSync -ReallocateReplica

Example 3: To move a DPM database from the local DPM server to a remote SQL server.

The following steps illustrate the use of DPMSync in moving a DPM database (DPMDB) from the local DPM server (DPMServer1) to a remote SQL server (DPMRemoteSQL).

1.	Run the following command: **DPMBackup –db**. This will create the file DPMDB.bak at **\Program Files\Microsoft DPM\DPM\volumes\Shadowcopy\Database Backups**. Store this backup in a secure location.
2.	Uninstall DPM from DPMServer1 and choose to retain data.

3.	Delete DPMDB. You have to do this in order to reinstall DPM.
4.	Install DPM on DPMServer1 with the remote SQL Server instance installed on DPMRemoteSQL.
5.	Run the following command on DPMRemoteSQL **dpmsync –restoredb –dbloc** <*dbbackuplocation*> **–instancename** <*instancename*>, where dbbackuplocation is the location of the backup taken in step 1 and instancename is the name of the remote SQL Server instance.
6.	Now run the following command on DPMServer1 Dpmsync –sync

Managing Generic Data Sources

System Center 2012 – Data Protection Manager (DPM) allows you to protect any Microsoft workload as long as they have a VSS writer. The Generic Data Source (GDS) infrastructure allows any VSS-writer-based Microsoft application to be backed up by DPM.

Note
For a list of topics that contain more details about the information covered here, see Generic data source topics.

Supported Features

- Complete backup using Express Full backup
- Original location recovery
- Referential data sources
- Backend data source with shared disk cluster support
- Multi-domain support
- Tape support

What's not supported

DPM does not support disaster recovery for generic data sources.

Generic data source topics

- Register a New Data Source

  Describes how to use the Modify-RegisteredWriters script to add, remove or modify the list of writers registered with DPM.

Register a New Data Source

The Modify-RegisteredWriters command allows you to add or remove the VSS writer ID from the list that is registered with DPM.

Use the Modify-RegisteredWriters command

Syntax

Modify-RegisteredWriters.ps1 [[-DpmServerName] <String>] [-List] [<CommonParameters>]

Modify-RegisteredWriters.ps1 [[-DpmServerName] <String>] [-Remove] [-Writers] <String> [<CommonParameters>]

Modify-RegisteredWriters.ps1 [[-DpmServerName] <String>] [-Add] [-Writers] <String> [<CommonParameters>]

Parameter	Type	Description
DPMServerNAme	String	Specifies the DPM server against which this command should run. By default, the command is run against the local DPM.
List	SwitchParameter	Indicates that the command should display the list of registered writer IDs.
Add	SwitchParameter	Indicates that the command should add the list of writer IDs to the list of the writer IDs that is registered with DPM.
Remove	SwitchParameter	Indicates that the given list of writer IDs must be removed from the list of the writer IDs that is registered with DPM.

Parameter	Type	Description
Writers	String	Comma-separated list of writer ID.

Examples

Example 1

The Modify-RegisteredWriters command displays the list of writers that are currently registered with the local DPM server.

```
Modify-RegisteredWriters -List
```

Example 2

The Modify-RegisteredWriters command adds the two new writer IDs to the list of registered writers on the local DPM server.

```
Modify-RegisteredWriters -Add -Writers "46eef637-28ca-4223-8bb6-2e87bd945179,e1cdedc6-d9d2-4fc3-8af6-5d0d0fe3e8af"
```

Example 3

The Modify-RegisteredWriters command removes the specified writer ID from the list of registered writers on DPM server dpm1.contoso.com.

```
Modify-RegisteredWriters -DpmServerName dpm1.contoso.com -Remove -Writers 46eef637-28ca-4223-8bb6-2e87bd945179
```

Managing Performance

The topics in this section define performance expectations and explain how to optimize System Center 2012 – Data Protection Manager (DPM) performance. Network speed, the performance characteristics of the protected computer, the size of your protected data, and the rate at which the protected data changes will determine your actual results.

In This Section

Improving Performance

Managing DPM Performance on a WAN

How Protection Group Changes Affect Jobs

See Also

Administering DPM Servers

Protecting File Servers and Workstations

Protecting Exchange Servers

Protecting SQL Servers

Protecting SharePoint Servers

Protecting Virtual Servers

Managing Tapes

How DPM Operations Affect Performance

As an administrator, one of your concerns will be the impact of System Center 2012 – Data Protection Manager (DPM) data transfer operations on system and network resources. The primary data transfer operations are:

- **Replica creation**. This occurs once for each protection group member.
- **Change tracking**. This is a continuous process on each protected computer.
- **Synchronization**. This occurs on a regular schedule.
- **Consistency check**. This occurs when a replica becomes inconsistent.
- **Express full backups**. This occurs on a regular schedule.
- **Back up to tape**. This occurs on a regular schedule.

Understanding these operations and DPM processes will help you establish reasonable expectations for DPM performance.

In This Section

Replica Creation

Change Tracking

Synchronization

Consistency Check

Express Full Backup

Backup to Tape

DPM Processes

See Also

Managing Performance

Replica Creation

In System Center 2012 – Data Protection Manager (DPM) a replica is a complete copy of the protected data on a single volume, database, or storage group. The DPM protection agent on the protected computer sends the data selected for protection to the DPM server. A replica of each member in the protection group is created. Replica creation is one of the more resource-intensive DPM operations, with its greatest impact being on network resources.

Typically, the performance of the replica creation will be limited by the speed of the network connection between the DPM server and the protected computers. That is, the amount of time that it takes to transfer a 1-gigabyte (GB) volume from a protected computer to the DPM server will be determined by the amount of data per second that the network can transmit.

The following table shows the amount of time it would take, at different network speeds, to transmit various amounts of data under optimal conditions. Times are given in hours, except where specified as minutes.

Time Required to Transmit Data over a Network at Various Speeds

Data size	Network speed 1 Gbps	Network speed 100 Mbps	Network speed 32 Mbps	Network speed 8 Mbps	Network speed 2 Mbps	Network speed 512 Kbps
1 GB	< 1 minute	< 1 hour	< 1	< 1	1.5	6
50 GB	<10 minutes	1.5 hour	5	18	71	284
200 GB	<36 minutes	6 hours	18	71	284	1137
500 GB	<1.5 hours	15	45	178	711	2844

Note

In the preceding table, Gbps = gigabits per second, Mbps = megabits per second, and Kbps = kilobits per second. The figures for a network speed of 1 Gbps assume that the disk speed on the DPM server and the protected computer are not a bottleneck.
Typically, the time to complete initial replica (IR) creation can be calculated as follows:

IR: hours = ((data size in MB) / (.8 x network speed in MB/s)) / 3600

Note 1: Convert network speed from bits to bytes by dividing by 8.

Note 2: The network speed is multiplied by .8 because the maximum network efficiency is approximately 80%.

On an extremely fast network, such as a gigabit connection, the speed of replica creation will be determined by the disk speed of the DPM server or that of the protected computer, whichever is slower.

The impact of replica creation on network performance can be reduced by using network bandwidth usage throttling. For more information, see Using Network Bandwidth Usage Throttling.

To avoid the network load of replica creation, you can create replicas manually from tape or other removable media when creating the initial replica, which can take from hours to days depending on the amount of data to protect. For more information, see Creating Replicas Manually.

If the network goes down during synchronization, DPM will attempt to continue the synchronization from the point where it left off last. If the network goes down during consistency check, DPM will attempt to continue the check if the network comes back up in five minutes. However, if the network remains down for longer than 5 minutes the replica is marked as Inconsistent.

See Also

How DPM Operations Affect Performance

Managing Performance

Change Tracking

After the replica is created, the System Center 2012 – Data Protection Manager (DPM) protection agent on the computer begins tracking all changes to protected data on that computer. Changes to files are passed through a filter before being written to the volume. This process is similar to the filtering of files through antivirus software, but the performance load of DPM tracking changes is less than the performance load of antivirus software.

See Also

How DPM Operations Affect Performance

Managing Performance

Synchronization

Synchronization is the process by which System Center 2012 – Data Protection Manager (DPM) transfers data changes from the protected computer to the DPM server and then applies the changes to the replica of the protected data.

For a file volume or share, the protection agent on the protected computer tracks changes to blocks, using the volume filter and the change journal that is part of the operating system to

determine whether any protected files were modified. DPM also uses the volume filter and change journal to track the creation of new files and the deletion or renaming of protected files.

For application data, after the replica is created, changes to volume blocks belonging to application files are tracked by the volume filter.

How changes are transferred to the DPM server depends on the application and the type of synchronization. For protected Microsoft Exchange data, synchronization transfers an incremental Volume Shadow Copy Service (VSS) snapshot. For protected Microsoft SQL Server data, synchronization transfers a transaction log backup.

DPM relies on synchronization to update replicas with the protected data. Each synchronization job consumes network resources and can therefore affect network performance.

The impact of synchronization on network performance can be reduced by using network bandwidth usage throttling and compression. For more information, see Using Network Bandwidth Usage Throttling and Using On-the-Wire Compression.

See Also

How DPM Operations Affect Performance

Managing Performance

Consistency Check

A consistency check is the process by which System Center 2012 – Data Protection Manager (DPM) checks for and corrects inconsistencies between a protected data source and its replica.

The performance of the protected computer, DPM server, and network will be affected while a consistency check is running, but it is expected to be optimized because only the changes and checksums are transferred.

The network impact from a consistency check is significantly lower than initial replica creation after a successful replica creation. If the initial replica creation is interrupted or unsuccessful, the first consistency check can have an impact similar to replica creation.

We recommend that consistency checks be performed during off-peak hours.

DPM automatically performs a consistency check in the following instances:

- When you modify a protection group by changing the exclusion list.
- When a daily consistency check is scheduled and the replica is inconsistent.

See Also

How DPM Operations Affect Performance

Managing Performance

Express Full Backup

An express full backup is a type of synchronization in which the protection agent transfers a snapshot of all blocks that have changed since the previous express full backup (or since the initial replica creation, for the first express full backup) and updates the replica to include the changed blocks. The impact of an express full backup operation on performance and time is expected to be less than the impact of a full backup because System Center 2012 – Data Protection Manager (DPM) transfers only the blocks changed since the last express full backup.

See Also

How DPM Operations Affect Performance

Managing Performance

Backup to Tape

When System Center 2012 – Data Protection Manager (DPM) backs up data from the replica to tape, there is no network traffic and therefore no performance impact on the protected computer.

When DPM backs up data from the protected computer directly to tape, there will be an impact on the disk resources and performance on the protected computer. The impact on performance is less when backing up file data than when backing up application data.

See Also

How DPM Operations Affect Performance

Managing Performance

DPM Processes

On the System Center 2012 – Data Protection Manager (DPM) server, three processes can impact performance:

- **DPM protection agent (MsDpmProtectionAgent.exe)**. DPM jobs affect both memory and CPU usage by the DPM protection agent. It is normal for CPU usage by MsDpmProtectionAgent.exe to increase during consistency checks.
- **DPM service (MsDpm.exe)**. The DPM service affects both memory and CPU usage.
- **DPM Administrator Console (an instance of Mmc.exe)**. DPM Administrator Console can be a significant factor in high memory usage. You can close it when it is not in use.

Note

Memory usage for the DPM instance of the SQL Server service (MicrosoftDPMAcct.exe) is expected to be comparatively high. This does not indicate a problem. The service normally uses a large amount of memory for caching, but it releases memory when available memory is low.

See Also

How DPM Operations Affect Performance

Managing Performance

DPM and Memory

When the memory in use by all the existing processes exceeds the amount of RAM available, the operating system will move pages (4 KB pieces) of one or more virtual address spaces to the computer's hard disk, freeing that RAM for other uses. In Microsoft Windows systems, these pages are stored in one or more files, called pagefile.sys, in the root of a partition.

System Center 2012 – Data Protection Manager (DPM)M requires a pagefile size that is 0.2 percent the size of all recovery point volumes combined, in addition to the recommended size (generally, 1.5 times the amount of RAM on the computer). For example, if the recovery point volumes on a DPM server total 3 TB, you should increase the pagefile size by 6 GB.

For more information about modifying the pagefile size, see Change the size of the virtual memory paging file.

There is a Volume Shadow Copy Service (VSS) non-paged pool limitation on 32-bit operating systems. Therefore, if you are protecting more than 10 TB of data, the DPM server must be running on a 64-bit operating system.

See Also

Managing Performance

Performance Counters

One method you can use to monitor System Center 2012 – Data Protection Manager (DPM) server performance is Performance in Administrative Tools. You can configure the monitored data to be saved as a log. You can also configure Performance to generate alerts. For information about how to create and configure performance alerts, see Microsoft Knowledge Base article 324752, How to create and configure performance alerts in Windows Server 2003.

Note

You can use the Management Pack for System Center 2012 – Data Protection Manager (DPM) to centrally monitor the state, health, and performance of multiple DPM servers from an Operations Management server. To download the Management Pack for System Center 2012 – Data Protection Manager (DPM), see System Center Data Protection Manager 2010 Management Pack for Operations Manager 2007.

The **Performance Counters for Monitoring DPM** table lists counters that can be useful for monitoring DPM server performance. For more information about specific performance counters, see Performance Logs and Alerts Help. To open the Performance tool, click **Start**, point to **Administrative Tools**, and then click **Performance**. On the **Action** menu, click **Help**.

Performance Counters for Monitoring DPM

Performance Object and Counter	Description	Value That Might Indicate a Problem	Possible Causes
Memory: Avail/MBytes	Measures the memory that is available to processes running on the specified DPM server. The Avail/MBytes value is the sum of memory assigned to the standby (cached), free, and zero-paged lists.	< 50 megabytes (MB). Indicates low memory on DPM server.	• One or more applications are consuming large amounts of memory. • Multiple DPM jobs are running simultaneously. • The DPM server does not have sufficient memory to handle the current DPM workload.
Processor: % Processor Time	Measures the percentage of time the processor was busy during the sampling interval.	> 95% for more than 10 minutes. Indicates very high CPU usage on the DPM server.	• Multiple DPM jobs are running simultaneously. Synchronization with consistency check jobs are particularly CPU-intensive. • On-the-wire compression has been enabled on the DPM server. On-the-wire compression allows faster data throughput without negatively affecting network performance. However, it places a

Performance Object and Counter	Description	Value That Might Indicate a Problem	Possible Causes
			large processing load on both the protected computer and the DPM server. • A runaway process is exhausting system resources. • The DPM server does not have sufficient processing capacity to handle the DPM workload.
Physical Disk: Current Disk Queue Length (for all instances)	Measures the number of disk requests that are currently waiting and the requests currently being serviced.	> 80 requests for more than 6 minutes. Indicates possibly excessive disk queue length.	• Multiple DPM jobs that are running simultaneously are placing a high demand on disk resources. • Disk performance needs tuning. • Disk resources on the DPM server are not sufficient for the current DPM workload.

See Also

Managing Performance

Improving Performance

Performance is determined by workload and capacity. A slow computer might perform adequately when it has a very light workload. In contrast, the performance of an extremely powerful computer might suffer when challenged by an excessive workload. In operations between two computers on a network, the workload that can be handled effectively will be limited by the component with the least capacity, whether it is one of the computers or the network connection itself.

As a general rule, you can improve performance by making changes to the workload, the capacity, or both.

In This Section

Modifying Workloads

Increasing Capacity

See Also

Managing Performance

Modifying Workloads

System Center 2012 – Data Protection Manager (DPM) offers several methods that you can use to modify protection workloads to improve performance. The following table lists the methods you can use and indicates what you can expect from each method.

Methods for Modifying Protection Workloads

Method	Impact
Network bandwidth usage throttling	Causes jobs to use less bandwidth, but they take longer to complete.
On-the-wire compression	Reduces size of data transfer but increases CPU utilization on the DPM server and the protected computers.
Staggering synchronization start times	Balances the loads of synchronization jobs across protection groups.
Scheduling consistency checks during off-peak hours	Prevents DPM from interfering with regular business use of protected computers.
Creating replicas manually	Might make replica creation faster. There is no performance load on the protected computer or network resources. However, the first consistency check will impact performance of the protected computer.

In This Section

Using Network Bandwidth Usage Throttling

Using On-the-Wire Compression

Staggering Synchronization Start Times

Scheduling Consistency Checks

Creating Replicas Manually

See Also

Increasing Capacity

Managing Performance

Using Network Bandwidth Usage Throttling

Network bandwidth usage throttling limits the amount of network bandwidth that System Center 2012 – Data Protection Manager (DPM) can use to create and synchronize replicas. Throttling helps to ensure that network bandwidth is available to applications other than DPM.

The advantage of using network bandwidth usage throttling is that it enables you to limit the amount of network resources a synchronization job can consume. The disadvantage of network bandwidth usage throttling is that it can lengthen the amount of time each synchronization job takes to complete.

Network bandwidth usage throttling is configured for each protected computer. Set network bandwidth usage throttling in terms of an absolute maximum amount of data to be transferred per second.

To enable network bandwidth usage throttling

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Agents** tab.
3. In the **Display** pane, select a server.
4. In the **Actions** pane, click **Throttle computer**.
5. Click **Enable network bandwidth usage**.

   You can configure network bandwidth usage throttling separately for work hours and non-work hours, and you can define the work hours for the protected computer. Work hours and non-work hours use the time zone of the protected computer.

Network bandwidth usage can be limited by Group Policy. The Group Policy reservable bandwidth limit on the local computer determines the combined reservable bandwidth for all programs that use the Packet Scheduler, including DPM. The DPM network bandwidth usage limit determines the amount of network bandwidth that DPM can consume during replica creation, synchronization, and consistency checks. If the DPM bandwidth usage limit, either by itself or in combination with the limits of other programs, exceeds the Group Policy reservable bandwidth limit, the DPM bandwidth usage limit might not be applied.

For example, if a DPM computer with a 1-gigabit-per-second (Gbps) network connection has a Group Policy reservable bandwidth limit of 20 percent, 200 Mbps of bandwidth is reserved for all programs that use the Packet Scheduler. If DPM bandwidth usage is then set to a maximum of

150 Mbps while Internet Information Services (IIS) bandwidth usage is set to a maximum of 100 Mbps, the combined bandwidth usage limits of DPM and IIS exceed the Group Policy reservable bandwidth limit, and the DPM limit might not be applied.

To resolve this issue, reduce the DPM setting for network bandwidth usage throttling.

See Also

Improving Performance

Modifying Workloads

Using On-the-Wire Compression

Compression decreases the size of data being transferred during replica creation and synchronization, and it allows more data throughput with less impact to network performance. However, this option adds to the CPU load on both the System Center 2012 – Data Protection Manager (DPM) server and the protected computers. The amount of compression and improvement on network performance depends on workload.

Compression is enabled for a protected computer and applies to replica creation, synchronization, and consistency check operations. Recovery jobs also use compression.

To enable on-the-wire compression

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Optimize performance**.
3. On the **Network** tab, select **Enable on-the-wire compression**.
4. To apply your changes, click **OK**.

See Also

Improving Performance

Modifying Workloads

Staggering Synchronization Start Times

You can specify the starting time, in minutes after the hour, of synchronization jobs for each protection group. Staggered starting times minimize the network impact of running multiple large protection jobs simultaneously.

To determine whether staggering the start times of synchronization jobs is appropriate for your needs, first gather information about scheduled protection jobs in System Center 2012 – Data Protection Manager (DPM) Administrator Console:

- In the **Monitoring** task area, on the **Jobs** tab, review jobs that are scheduled for times when the DPM server experiences large disk queues.
- In the **Protection** task area, review details for protection groups to determine the size and frequency of protection jobs.

Offsetting synchronization start times can also be used to optimize secondary protection of another DPM server. Secondary protection is when a DPM server protects the database and replicas of another DPM server, referred to as the primary DPM server. You can offset the synchronization of the primary DPM server to the secondary DPM server to occur after the data sources are synchronized to the primary DPM server.

To stagger synchronization start times

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the display area, select a protection group.
3. In the **Actions** pane, click **Optimize performance**.
4. On the **Network** tab, select the hours and minutes to offset the start of the synchronization job in the **Offset <time> start time by** field.

   The maximum allowed value for offset is the same as the synchronization frequency.
5. To apply your changes, click **OK**.

   Changing the start time offsets recovery points for files by the equivalent amount of time.

You can choose between two modes of synchronization: at regular intervals or just before a recovery point is created.

Synchronization at regular intervals distributes the load on the network throughout the day. In the case of synchronization just before a recovery point is created, the network traffic is potentially greater at the time of synchronization, but data is not sent throughout the day.

If an organization has limited network bandwidth between the protected computer and the DPM server and this limited bandwidth is also expected to be shared by normal corporate usage, consider using synchronization only before recovery point and schedule it during off-peak hours.

Although the impact on network traffic and performance is important, you must also consider how the choice of synchronization mode affects your ability to recover data. If you synchronize only once a day, the maximum loss window is 24 hours. However, if you choose to synchronize every hour, your maximum loss window is 1 hour.

See Also

Improving Performance

Modifying Workloads

Scheduling Consistency Checks

Because consistency checks affect the performance of both the System Center 2012 – Data Protection Manager (DPM) server and the protected computer, you should schedule consistency checks for hours when reduced responsiveness of the protected computer has the least impact on your business operations and there is the least amount of network traffic.

After a protection group is created manually or if a replica becomes inconsistent because of a network outage or another reason, you must perform a manual consistency check.

You can also schedule a daily consistency check to ensure that inconsistent replicas are automatically repaired.

As part of the scheduling options, you can configure a duration or time window when consistency checks jobs can run. For example, you can configure the consistency check to begin at 8:00 P.M. when most of your company's employees are gone, with a maximum duration of 10 hours.

See Also

Improving Performance

Modifying Workloads

Creating Replicas Manually

When you create a protection group, you can choose to create the replicas manually from tape or other removable media to reduce the load on the protected computers and network.

Automatic replica creation is easier; however, depending on the size of the protected data, manual replica creation can be faster. For smaller data sets, we recommend the automatic option. For large data sets and slow networks, the manual option is likely to be a better choice.

After the replica is created, you must run synchronization with consistency check.

See Also

Improving Performance

Modifying Workloads

Increasing Capacity

You can also improve performance by increasing the capacity of the System Center 2012 – Data Protection Manager (DPM) server through hardware upgrades:

- Adding disks to the storage pool and reallocating the replicas across the storage pool can help reduce disk queue length.

- Using striped volumes can increase disk throughput to deal with disk bottlenecks.
- Adding memory is a relatively inexpensive upgrade that can result in a noticeable improvement in performance if the server frequently experiences low available memory.
- Adding more processors or upgrading to faster processors can reduce CPU issues.

Also, consider your data protection requirements: you might need additional DPM servers to balance the workload.

See Also

Improving Performance

Managing Performance

Modifying Workloads

Managing DPM Performance on a WAN

Performance is a serious consideration when the System Center 2012 – Data Protection Manager (DPM) server and the servers that it is protecting are connected by low-speed wide area network (WAN) links, particularly for resource-intensive jobs such as replica creation and consistency checks. For example, transferring a 20 GB volume across a 512 Kbps link would take at least 120 hours.

In this network configuration, you should enable compression for all protection groups. For replica creation of volumes larger than 5 GB, we recommend that you create the replica manually.

Improving usage of WAN latency

If your deployment of DPM disaster recovery requires DPM to send large amounts to data over a WAN, you can improve DPM's use of your WAN latency by adjusting the following registry settings

On the remote DPM server:

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize`

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts`

On the DPM server:

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts`

Example: The following settings over a 100 Mbps link with 40 ms latency, gives the following results.

Settings	
On the remote DPM server: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize`	524288

On both the DPM servers: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize\Tcp1323Opts`	3
Results	
One job running	3.45 MB/sec
Three jobs running	~3 MB/sec/job

How Protection Group Changes Affect Jobs

Changes to the configuration of a System Center 2012 – Data Protection Manager (DPM) protection group can result in the cancellation of some active jobs. A change could affect replica jobs, archive jobs, or both. The following table lists the jobs that are canceled in each category.

Job types

Replica jobs	Archive jobs
• Replica creation • Consistency check • Synchronization • Create recovery point on disk • Recovery from disk	• Create recovery point on tape • Verification of data on tape • Copy data to tape • Back up to tape • Recovery from tape

The following table lists how protection group changes can cause the cancelation of active jobs. Jobs can be canceled for:

- All members of the protection group ("protection group")
- All data sources on the protected computer ("protected computer")
- All protected computers in the same time zone as the computer hosting the data sources in the protection group that is changed ("time zone")

Protection group changes and active jobs

Change to protection group	Job cancellations
Remove tape-based protection	Archive jobs for the protection group
Add disk-based protection	Archive jobs for the protection group if tape-based protection is configured
Remove disk-based protection	Replica and archive jobs for the protection

Change to protection group	Job cancellations
	group
Add or remove data sources	Replica for the protected computer and archive jobs for time zone
Change protected objects, including folder exclusion	Replica and archive jobs for the protected computer and time zone
Change file type exclusion	Replica and archive jobs for the protection group
Delete a protection group	Replica and archive jobs for the protection group
Change the preferred server for clustered Exchange Server data	Replica and archive jobs for the protected computer and time zone
Change protection of a mounted volume to a different mount point	Replica and archive jobs for the protected computer and time zone
Stop protection and delete data on tape	Archive jobs for the time zone
Stop protection and delete data on disk	Replica and archive jobs for the protected computer
Change the tape library that the protection group uses	Archive jobs for the protection group if data verification is enabled
Change the tape data verification selection	Archive jobs for the protection group
Change to number of tape copies	Archive jobs for the protection group
Add or remove tape-based protection	Archive jobs for the protection group
Change data verification setting for tape-based protection	Archive jobs for the protection group
Change data verification setting for disk-based protection	Replica jobs for the protection group
Change compression setting for tape-based protection	Archive jobs for the protection group
Change encryption setting for tape-based protection	Archive jobs for the protection group
Change network bandwidth usage throttling setting for short-term tape-based protection	Archive jobs for the protection group
Change compression, encryption, or network bandwidth usage throttling for disk-based	Replica jobs for the protection group

Change to protection group	Job cancellations
protection	

See Also

Managing Performance

Managing Disks

DPM provides disk management features to help you manage and monitor the disks in the storage pool. The storage pool is a set of disks on which the DPM server stores replicas and recovery points. Before you can start protecting data, you must add at least one disk to the storage pool.

In This Section

What Is a Storage Pool?

How Disk Allocation Works

How to Remove a Disk from the Storage Pool

How to View Disk Allocation Information

How to Modify Disk Allocation

How to Display Storage Pool Data

How to Update Storage Pool Data

How to Modify Allocated Space for a Change Journal

How to Assign a Custom Volume for a Protection Group

See Also

Managing Tapes

What Is a Storage Pool?

The *storage pool* is a set of disks on which the Data Protection Manager (DPM) server stores replicas and recovery points. Before you can start protecting data, you must add at least one disk to the storage pool. Disks added to the storage pool should not have any partitions. To prepare disks for data protection, DPM reformats the disks and erases any data on them.

The DPM server must have at least two disks installed: one dedicated to the startup, system, and DPM installation files; and one dedicated to the storage pool. In the context of DPM, *disk* is defined as any disk device manifested as a disk in the Windows Disk Management tool. DPM does not add any disk containing startup files, system files, or any component of the DPM installation to the storage pool.

Note

DPM does not support USB/1394 disks.

You cannot use Storage Spaces for the DPM disk storage pool.

For information about choosing disk types and calculating capacity requirements for your storage pool, in the DPM Deployment Guide, see Planning for DPM Deployment.

See Also

What Is a Recovery Point?

Understand replicas

Synchronization

How Disk Allocation Works

When you create a new protection group, Data Protection Manager (DPM) allocates disk space for the protection group in the storage pool. Based on retention range, work load type and the size of the protected data, DPM recommends the amount of disk space to allocate in the storage pool and verifies that the protected computer contains sufficient space for the change journal.

Important

To help you in designing a storage layout for DPM, you can use a Storage Calculator that focuses on outlining the storage capacity requirements based on a set of input factors. For more information, see Storage Calculators for DPM (http://go.microsoft.com/fwlink/?LinkID=180658).

Important

With data co-location enabled, DPM will allocate fixed size volumes in the storage pool. For more information, see Co-Locating Data on Disk.

If you are protecting only a subset of the data on the protected volume, you can calculate the size of the protected data so that DPM can adjust its recommendations for disk allocation. To compute the disk allocation using the size of the data on the protected volume, in the **Modify Disk Allocation** dialog box, click **Calculate**.

If the data on the protected volume outgrows the initial allocations, DPM can try to automatically grow the volume by 25% if the option **Automatic grow the volumes** in the **Review Disk Allocation** page of the Create New Protection Group wizard is selected. If the auto-grow operation fails, or if the option **Automatic grow the volumes** is not selected, DPM generates a

“Recovery point volume threshold exceeded” or “Replica disk threshold exceeded” alert and provides guidance for increasing disk allocations appropriately.

During creation of a protection group, DPM calculates default space allocations depending on what type of datasource is being protected. You should accept the recommended disk allocations for the protection group unless you are sure that these allocations do not meet your requirements. If you change the recommended allocations, you might get fewer recovery points than you wanted or DPM might allocate more disk space than is needed.

Generally, the recommended allocations provide sufficient storage for at least a couple of weeks of recovery points. If necessary, you can adjust the disk allocations after monitoring disk usage for data protection.

For more information about disk allocations, see Planning Protection Groups.

You can schedule and view reports in the Reporting task area. To view trends in disk usage for a protection group, review a Disk Utilization Report.

See Also

Disk Utilization Report

How to Modify Disk Allocation

Managing Disks

Using Reports

What Is a Recovery Point?

What Is a Storage Pool?

Synchronization

Co-Locating Data

How to Remove a Disk from the Storage Pool

Removing a disk from the DPM storage pool involves three tasks:

- Identifying protection group members that use the disk to store replicas and recovery points.
- Removing the protection group members from their protection groups.
- Removing the disk from the storage pool.

After you remove the disk from the storage pool, you can add the members back to their protection groups if you want to continue to protect them. If you add the members back before you remove the disk, DPM may allocate space on the disk that you want to remove.

To identify protection group members

1. In DPM Administrator Console, go to the **Management** view, and then open the **Disks** workspace.

2. Select the disk that you want to remove.
3. In the **Details** pane, note the affected protection group members in the **Protected data sources on this disk** area.

To remove protection of group members

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, select the protection group member that you want to remove from protection.

   Note
   You can select multiple members and remove them at the same time.
3. Click **Stop protection** from the tool ribbon. Verify that you want to remove the member displayed in the **Remove from Protection Group** dialog box. If you decide not to remove the member, click **Cancel** at the bottom of the dialog box.

   Note
   Removing protection of group members triggers a consistency check.

To remove a disk from the storage pool

1. In DPM Administrator Console, go to the **Management** view, and then open **Disks** workspace.
2. Select the disk that you want to remove.
3. Click **Remove** on the tool ribbon. The disk is removed from the storage pool.

See Also

Managing Disks

What Is a Storage Pool?

How to View Disk Allocation Information

In the **Management** task area, accessed by clicking **Management** on the DPM Administrator Console navigation bar, you can review storage pool data to find out how much disk space is allocated for data protection, and how much space is still available.

To view disk allocation information

1. In DPM Administrator Console, go to the **Management** view, and then open the **Disks** workspace. The storage pool disk allocation information is displayed.

   At the top of the **Disks** workspace, the total capacity and total disk space allocated for all disks in the storage pool is displayed. In the display pane, the total capacity and

unallocated disk space for each disk in the storage pool is displayed.

Note
Because of rounding, the totals for allocated and unallocated disk space in the storage pool might not equal the exact total capacity of the disks in the storage pool.

2. To review the status and disk allocation data for a specific disk, select the disk and refer to the **Details** pane. DPM stores the following information for each disk in the storage pool:
   - Name
   - Status: Healthy, unhealthy, or missing
   - Used space: Space allocated for protection
   - Unallocated space: Amount of unallocated space
   - Protected data sources on this disk: A list of the data sources protected on the disk

See Also

How Disk Allocation Works

How to Update Storage Pool Data

What Is a Storage Pool?

How to Modify Disk Allocation

When you create a protection group, Data Protection Manager (DPM) recommends and allocates disk space for your protection group based on the size of the data to be protected. It is recommended that you do not change the default allocations until after you monitor disk usage for the protection group. If required, you can modify disk allocation according to the guidelines in the following table.

Protection feature	Disk allocation options	Location
Replica volume	You can increase, but not decrease, the allocated disk space for the replicas.	DPM storage pool
Recovery point volume	You can increase or decrease, the allocated space for recovery points.	DPM storage pool
Change journal	You can increase, but not decrease, the allocated disk space for the change journal.	Protected volume on the file server or workstation

Protection feature	Disk allocation options	Location
Custom volume	DPM does not manage custom volumes.	Any disk attached to the DPM server

Note
In the Create New Protection Group Wizard, DPM displays the **Disk Allocation** page only when a new protection group is created, when new members are added to an existing protection group, or when an existing protection group's properties are changed from short-term protection by using disk to tape.

To modify disk allocation

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, select the protection group for which you want to modify disk allocation.
3. Click **Modify disk allocation**.
4. On the **DPM Server** tab, type the amount of space you want to allocate for **Replica Volume** and for **Recovery Point Volume**, and click **OK**.

   Note
   When creating a protection group, DPM helps to allocate optimal space. Click **Calculate** to have DPM allocate space based on a formula specific to a data source type. If you do not click **Calculate**, DPM allocates approximately two times the volume size for the replicas and recovery points.

   Click **Shrink** to calculate the thresholds to which the recovery point volume size can shrink.
5. If you are modifying disk allocation on a protected computer, on the **Protected Computer** tab, type the amount of space you want to allocate in the **Space Allocated** column, and click **OK**.
6. After reviewing the disk allocation changes, click **OK**.

   Note
   If data co-location is enabled on disk, click **Collocated Protection** to view co-located replica details for each co-located data source.

To modify disk allocation using DPM Management Shell

- Use the following syntax to retrieve the current disk allocation:

  Get-DatasourceDiskAllocation [-Datasource] <*Datasource*> **[-CalculateSize] [-Async] [-Tag** <*Object*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to use the default disk allocation:

Get-DatasourceDiskAllocation [-Datasource] <Datasource> [-Async <SwitchParameter>] [-CalculateShrinkThresholds <SwitchParameter>] [-CalculateSize <SwitchParameter>] [-PrimaryDpmServer <SwitchParameter>] [-Tag <Object>] [<CommonParameters>]

- Use the following syntax to manually set the disk allocation:

  Set-DatasourceDiskAllocation [-Datasource] <Datasource> [-ProtectionGroup] <ProtectionGroup> -Manual [-ReplicaArea <Int64>] [-ShadowCopyArea <Int64>] [-ProductionServerJournalSize<Int64>] [-PassThru] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-ErrorVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]

- Use the following syntax to customize the disk allocation:

  Set-DatasourceDiskAllocation [-Datasource] <Datasource> [-ProtectionGroup] <ProtectionGroup> -CustomRequirements [-ReplicaVolume <DpmServerVolume>] [-ShadowCopyVolume <DpmServerVolume>] [-FormatVolumes <Nullable`1>] [-USNJournalSize <Int64>] [-PassThru] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-ErrorVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]

  For more information, type "**Get-Help Set-DatasourceDiskAllocation -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Set-DatasourceDiskAllocation -full**" in DPM Management Shell.

See Also

New Protection Group Wizard

How Disk Allocation Works

How to Display Storage Pool Data

How to View Disk Allocation Information

Understanding Data Protection

Understanding Data Recovery

Synchronization

How to Display Storage Pool Data

In the **Management** view, you can review storage pool data to find out how much disk space is allocated for data protection and how much space is still available.

To display storage pool data

1. In DPM Administrator Console, go to the **Management** view, and then open the **Disks**

workspace. The storage pool disk allocation information is displayed.

At the top of the **Disks** page, the total capacity and total disk space allocated for all disks in the storage pool is displayed. In the display pane, the total capacity and unallocated disk space for each disk in the storage pool is displayed.

Note
Because of rounding, the totals for allocated and unallocated disk space in the storage pool might not equal the exact total capacity of the disks in the storage pool.

2. To review the status and disk allocation data for a specific disk, select the disk and refer to the **Details** pane. DPM stores the following information for each disk in the storage pool:
   - Name
   - Status: Healthy, unhealthy, or missing
   - Used space: Space allocated for protection
   - Unallocated space: Amount of unallocated space
   - Protected data sources on this disk: A list of the data sources protected on the disk

See Also

How Disk Allocation Works

How to Update Storage Pool Data

Managing Disks

What Is a Storage Pool?

How to Update Storage Pool Data

If you have added a disk to the storage pool and it is not displayed on the **Disks** tab in the **Management** area, you can rescan the disk configuration to display the disk.

For information on how to add disks to the storage pool, see Adding Disks to the Storage Pool.

To update the storage pool data

1. In DPM Administrator Console, click **Management** on the navigation bar, and then select the **Disks** tab.
2. In the **Actions** pane, click **Rescan**. The current disk data is displayed.

See Also

How to Display Storage Pool Data

How to Remove a Disk from the Storage Pool

How to Modify Allocated Space for a Change Journal

A *change journal* provides a persistent log of all changes made to files on a volume. As files, directories, and other NTFS file system objects are added, deleted, and modified, NTFS enters records into the change journal, one for each volume on the computer. Each record indicates the type of change and the object changed.

When you create a protection group, Data Protection Manager (DPM) allocates 300 MB of disk space on the data source volume of the protected computer to store the change journal. It is recommended that you do not change the default allocations until after you monitor disk usage for the protection group.

To modify allocated space for the change journal

1. In DPM Administrator Console, on the navigation bar, open the **Protection** view.
2. Select the protection group for which you want to modify the allocated space for the change journal.
3. Click **Modify disk allocation** on the tool ribbon.
4. On the **Protected Computer** tab, enter a value in the **Space Allocated** box.

   Note
   The default disk space is 300 MB. You can increase, but not decrease, the space allocated for the change journal.
5. Click **OK**.

See Also

Disk Utilization Report

How Disk Allocation Works

Managing Disks

How to View Disk Allocation Information

How to Assign a Custom Volume for a Protection Group

With DPM, you can assign a custom volume to store replicas and recovery points. This can maximize performance in DPM if you choose to keep certain volumes on separate LUNs (Logical Unit Numbers) to enable parallel replication onto these volumes.

After you have created and assigned a custom volume, DPM does not increase the size of this volume as it fills—the administrator must use Disk Management to perform this task. Custom volumes can be assigned only when you create a new protection group or when you add a new member to a protection group.

Important
You cannot create a custom volume from DPM. You must create the volume by using Disk Management.

To assign a custom volume when creating a new protection group

1. Use Disk Management to create a volume of the desired size and name.
2. In DPM Administration Console, go to the **Protection** view.
3. In the display pane, select the protection group you want to modify.
4. Click **New** on the tool ribbon. This starts the Create New Protection Group Wizard.
5. On the Create New Protection Group page, click Next.

   Note
   If you do not want DPM to display the **Welcome** page, select the **Do not show the Welcome page again** box.
6. Select group members for the protection group, and click **Next**.
7. Select the data protection method, and click **Next**.
8. Select your short-term protection objectives, and click **Next**.
9. On the **Review Disk Allocation** page, in the **Disk space allocation for new members** pane, click **Modify**.
10. On the **DPM Server** tab, in the **Storage Type** column, select **Custom Volume** from the pull-down menu.

    Important
    You can specify a custom volume only for the new members of the protection group.
11. In the **Replica Volume** column, from the pull-down menu, select the volume that DPM will use to store the replica volume for the protection group member.
12. In the **Recovery Point** column, from the pull-down menu, select the volume that DPM will use to store the recovery point volume for the protection group member.
13. In the **Custom Volume** column, select whether to format the disk from the drop-down

menu.

> **Note**
> Select **Do not format** when the custom volume is used in a storage area network.

14. Click **OK**, and then click **Next**.
15. Complete the Create New Protection Group Wizard. On the **Summary** page, click **Create Group**.

To assign a custom volume when modifying a protection group

1. Use Disk Management to create a volume of the desired size and name.
2. In DPM Administration Console, go to the **Protection** view.
3. Click **Modify** on the tool ribbon to start the Modify Protection Group Wizard.
4. Select group members for the protection group, and click **Next**.
5. Select the data protection method, and click **Next**.
6. Select your short-term protection objectives, and click **Next**.
7. On the **Review Disk Allocation** page, in the **Disk space allocation for new members** pane, click **Modify**.
8. On the **DPM Server** tab, in the **Storage Type** column, select **Custom Volume** from the pull-down menu.
9. In the **Replica Volume** column, from the pull-down menu, select the volume that DPM will use to store the replica volume for the protection group member.
10. In the **Recovery Point** column, from the pull-down menu, select the volume that DPM will use to store the recovery point volume for the protection group member.
11. In the **Custom Volume** column, select whether to format the disk from the drop-down menu.

> **Note**
> Select **Do not format** when the custom volume is used in a storage area network.

12. Click **OK**, and then click **Next**.
13. Complete the Modify Protection Group Wizard. On the **Summary** page, click **Update Group**.

See Also

New Protection Group Wizard

Managing Disks

Managing Tapes

Magnetic tape and similar storage media offer an inexpensive and portable form of data protection that is particularly useful for long-term storage.

In System Center 2012 – Data Protection Manager (DPM), you can back up data from a computer directly to tape. You can also back up data from the disk-based replica. The advantage of creating your long-term backup on tape from the disk-based replica is that the backup operation can occur at any time with no impact on the computer being protected.

Additionally, a thorough disaster recovery plan will include offsite storage of critical information; you want to be able to recover your organization's data, in a situation where your facility might be damaged or destroyed. Tape is a popular medium for offsite storage.

In This Section

How DPM Uses Tape

To use tape-based protection in DPM, you must attach a tape library or stand-alone tape drive to the DPM server. A *tape library* is a data-storage system that consists of one or more tape drives, a number of slots to hold tape cartridges and a transport system for moving tapes. A *stand-alone tape drive* is a single-drive, non-automated tape drive that holds a single tape.

You can use tape for both short-term and long-term protection of file and application data.

DPM protects data on tape through a combination of full and incremental backups from either the protected computer (for short-term protection on tape or for long-term protection on tape when DPM does not protect the data on disk) or the DPM replica (for long-term protection on tape when short-term protection is on disk).

Note
When an application does not support incremental backups, DPM will perform full backups only.

DPM can either compress or encrypt data on tapes. Compressing encrypted data can increase the data file size instead of decreasing it.

See Also

Encrypt data in a protection group

Managing Tapes

New Protection Group Wizard

How to Add or Remove a Tape

Use the following procedures to add or remove tapes from the tape library.

Note

If you add or remove tapes to the tape library using **Unlock library door** or **Add tape**, DPM will automatically inventory the library. If you add or remove tapes to the tape library without using **Unlock library door** or **Add tape**, you must use the **Inventory library** action to update the information in DPM Administrator Console.

Adding or removing a tape from a stand-alone tape drive is accomplished manually according to the instructions provided by the device manufacturer, without using DPM Administrator Console.

To add a tape by using the Insert/Eject (I/E) port

1. Physically add the tape to the I/E port of the tape library.
2. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
3. In the **Actions** pane, click **Add tape (I/E port)**. DPM performs a fast inventory on the tape library and adds tapes into the free slots available in the tape library. This enables you to add tapes into the I/E port which remains open for a time period of 10 minutes.

   Important

   If sufficient numbers of slots are not free then the tapes are left in the I/E Port and the Add tape (I/E port) operation fails.

To add a tape by using DPM Management Shell

- Use the following syntax to add a tape using the I/E port:

  Lock-DPMLibraryIEPort [-DPMLibrary] <*Library*> **[-Async] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Lock-DPMLibraryIEPort -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Lock-DPMLibraryIEPort -full**" in DPM Management Shell.

To remove a tape by using the I/E port

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library from which you want to remove a tape.
3. Expand **Slots**, and then select the slot that holds the tape to be removed.
4. Click **Remove tape**.
5. Physically remove the tape from the I/E port of the tape library.

To remove a tape by using DPM Management Shell

- Use the following syntax to add a tape using the I/E port:

  Unlock-DPMLibraryIEPort [-DPMLibrary] <*Library*> **[-Async] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Unlock-DPMLibraryIEPort -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Unlock-DPMLibraryIEPort -full**" in DPM Management Shell.

See Also

How to Inventory the Tape Library

How to Lock and Unlock a Library Door

Managing Tapes

How to Inventory Tapes

The purpose of inventory is to identify new tapes and recognize tapes DPM has seen before.

A *fast inventory* involves reading the bar code of each tape in the library. DPM can perform a fast inventory for tapes that have bar codes in a tape library that has a bar code reader.

A *detailed inventory* involves reading the header area of a tape in the library to identify the on-media ID (OMID) on each tape. DPM must perform a detailed inventory when a tape does not have a bar code or the tape library does not have a bar code reader.

A fast inventory detects any tape (with or without a bar code) in any library. However, to uniquely identify the media, perform a detailed inventory.

Note

If a cleaning tape does not have a bar code or the bar code does not start with "CLN" is added to the library, and you run a detailed inventory before you mark the tape as a

cleaning tape and run a fast inventory, a cleaning job will start when DPM mounts this tape during the detailed inventory.

To inventory tapes in a library

1. In DPM Administrator Console, go to the **Management** view.
2. Open the **Libraries** workspace, and then select a library.
3. Click **Inventory**.
4. In the **Inventory** dialog box, select **Fast inventory** or **Detailed inventory**, and then click **Start**.

   If the tape does not have a bar code or the tape library does not have a bar code reader, the fast inventory option is disabled.

See Also

Managing Tapes

How to Mark a Tape as Free

A *free* tape is a tape that is available to be written to by operations such as backup or copy. To reuse an expired tape from another server for System Center 2012 – Data Protection Manager (DPM), you must add it to the tape library or stand-alone tape drive, and then mark it as free. Expired tapes that are being managed by that DPM server can be reused automatically without being marked as free by the administrator.

Blank tapes are automatically marked as free.

To mark a tape as free

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library or stand-alone tape drive, and then select the tape to be marked as free.
3. Click **Mark as free**.

To mark a tape as free using DPM Management Shell

- Use the following syntax to mark a tape as free:

  Set-Tape [-Tape] <*Media[]*> **-Free [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to mark a tape as not free:

  Set-Tape [-Tape] <*Media[]*> **-NotFree [-PassThru] [-Verbose] [-Debug] [-ErrorAction**

<*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

For more information, type "**Get-Help Set-Tape -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Set-Tape -full**" in DPM Management Shell.

To mark a tape containing valid data sets as free

1. Open a new Notepad file, and then copy the following script into it:

```
param ([string] $DPMServerName, [string] $LibraryName,
[string[]] $TapeLocationList)

if(("-?","-help") -contains $args[0])
{
    Write-Host "Usage: ForceFree-Tape.ps1 [[-DPMServerName]
<Name of the DPM server>] [-LibraryName] <Name of the
library> [-TapeLocationList] <Array of tape locations>"
    Write-Host "Example: Force-FreeTape.ps1 -LibraryName "My
library" -TapeLocationList Slot-1, Slot-7"
    exit 0
}

if (!$DPMServerName)
{
    $DPMServerName = Read-Host "DPM server name: "

    if (!$DPMServerName)
    {
        Write-Error "Dpm server name not specified."
        exit 1
    }
}

if (!$LibraryName)
{
    $LibraryName = Read-Host "Library name: "
```

```
    if (!$LibraryName)
    {
        Write-Error "Library name not specified."
        exit 1
    }
}

if (!$TapeLocationList)
{
    $TapeLocationList = Read-Host "Tape location: "

    if (!$TapeLocationList)
    {
        Write-Error "Tape location not specified."
        exit 1
    }
}

if (!(Connect-DPMServer $DPMServerName))
{
    Write-Error "Failed to connect To DPM server
$DPMServerName"
    exit 1
}

$library = Get-DPMLibrary $DPMServerName | where
{$_.UserFriendlyName -eq $LibraryName}

if (!$library)
{
    Write-Error "Failed to find library with user friendly
name $LibraryName"
    exit 1
}
```

```
foreach ($media in @(Get-Tape -DPMLibrary $library))
{
    if ($TapeLocationList -contains $media.Location)
    {
        if ($media -is
[Microsoft.Internal.EnterpriseStorage.Dls.UI.ObjectModel.Libr
aryManagement.ArchiveMedia])
        {
            foreach ($rp in @(Get-RecoveryPoint -Tape
$media))
            {
                Get-RecoveryPoint -Datasource $rp.Datasource
| Out-Null

                Write-Verbose "Removing recovery point
created at $($rp.RepresentedPointInTime) for tape in
$($media.Location)."
                Remove-RecoveryPoint -RecoveryPoint $rp -
ForceDeletion -Confirm:$false
            }

            Write-Verbose "Setting tape in $($media.Location)
as free."
            Set-Tape -Tape $media -Free
        }
        else
        {
            Write-Error "The tape in $($media.Location) is a
cleaner tape."
        }
    }
}
```

2. Save the file as ForceFree.ps1.

3. The syntax to run the script is **ForceFree.ps1 -DPMServerName <Name of server> -LibraryName <Name of library> -TapeLocation <slot numbers>.**

See Also

Managing Tapes

How to Identify an Unknown Tape

When a tape containing data is added to the tape library and the tape label displays as "Unknown", you can use DPM to identify the tape.

When DPM identifies the tape, it reads the tape header and updates the tape label as follows:

- A tape created by the DPM server displays the assigned tape label.
- A tape created by another DPM server displays **Imported** as the tape label.
- A tape that contains content that was not created by DPM displays **Unrecognized** as the tape label.
- A tape that has conflicting identification information, such as the bar code or the on-media identifier, displays **Suspect** as the tape label.

To identify an unknown tape

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library or stand-alone tape drive and select the unknown tape.
3. Click **Identify unknown tape**.

See Also

Managing Tapes

How to Recatalog an Imported Tape

An *imported tape* contains content that was created by another DPM server.

During the recatalog operation, DPM reads from the tape and adds information about the data that it contains to the database. After the recatalog operation is completed, you can recover data from the tape by selecting a recovery point from the data on the tape.

To recatalog an imported tape

1. In DPM Administrator Console, go to the **Management** view.
2. On the **Libraries** workspace, select the tape to import.
3. Click **Recatalog imported tape**.

To recatalog an imported tape using DPM Management Shell

- Use the following syntax to recatalog an imported tape:

  Start-TapeRecatalog [-Tape] <*Media[]*> **[-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Start-TapeRecatalog -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Start-TapeRecatalog -full**" in DPM Management Shell.

To recatalog a tape from a shared library

- If you try to recatalog a tape in a shared library from a DPM server other than the one from which the backup was taken, you will not see the **Recatalog** and **View Contents** options in the tool ribbon.
  Run a detailed inventory on that tape. After the inventory is completed, the **Recatalog** and **View Contents** options are enabled on the tool ribbon.

See Also

Managing Tapes

How to Inventory the Tape Library

How to View Tape Contents

Use the following procedure to view tape contents in the DPM Administrator Console. When you view the contents of a tape, you can also copy the data that is on the tape to disk.

To view tape contents

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, select the tape to view.
3. Click **View tape contents**.

See Also

How to Copy a Tape

Managing Tapes

How to View a Tape List

You can use the following procedure to view a tape list, which displays the tape or tapes associated with a protection group.

To view a tape list

1. In DPM Administrator Console, go to the **Protection** view.
2. In the display pane, click a protection group.
3. Click **View tape list**.

See Also

Managing Tapes

How to Erase a Tape

You can reuse an expired tape without erasing the contents of the tape. However, you can erase a tape to remove sensitive or critical information, if you choose.

To erase a tape

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library or stand-alone tape drive and select the tape that you want to erase.
3. Click **Erase tape**.

To erase a tape using DPM Management Shell

- Use the following syntax to erase a tape:

  Start-TapeErase [-Tape] <*Media[]*> **[[-JobStateChangeHandler]** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction**<*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable**<*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Start-TapeErase -detailed**" in DPM Management

Shell.

For technical information, type "**Get-Help Start-TapeErase -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Import Tapes

An *imported tape* contains content that was created by another DPM server. When you add an imported tape to the tape library, you must recatalog the tape to identify the contents of the tape.

During the recatalog operation, DPM reads from the tape and adds information about the data that it contains to the database. After recatalog completes, you can recover data from the tape by selecting a recovery point from the data on the tape.

To import tapes

1. In DPM Administrator Console, go to the **Management** view.
2. Open the **Libraries** workspace, and then select the tape to import.
3. Click **Recatalog imported tape**.

See Also

Managing Tapes

How to Copy a Tape

Use the following procedures in DPM to copy a tape. When you configure a protection group to use tape-based protection, you can specify how many copies of each tape that DPM should create. However, you can also copy the tapes manually.

To copy a tape to disk

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library or stand-alone tape drive, select the tape that you want to copy, and then click **View tape contents**.
3. In the tape contents dialog box, select the data to be copied, and then click **Copy**.
4. In the **Specify Alternate Recovery Destination** dialog box, specify a destination on a

computer that has the protection agent installed, and then click **OK**.

5. Click **Yes** to proceed with the copy operation.
6. Click **OK** to close the message.
7. You can view the progress of the copy job in the **Monitoring** task area on the **Jobs** tab.

To copy a tape to another tape

1. In DPM Administrator Console, go to the **Recovery** view.
2. Select the data that you want to copy to tape, and then click **Recover**. The Recovery Wizard opens.
3. On the **Review Recovery Selection** page, you can confirm which tape or tapes the data is on. Click **Next** to continue.
4. On the **Specify Recovery Type** page, select the copy to tape option, and then click **Next**.
5. On the **Specify Library** page, in **Primary library**, select a library to use for recovery.
   a. When the data is being copied from tape and the tape library has multiple tape drives, the library you select in **Primary library** reads from the source tape and copies the data to another tape.
   b. When the data is being copied from tape and the tape library has only a single tape drive, the library you select in **Primary library** reads from the source tape and the library you select in **Copy library** copies the data to tape.
6. On the **Specify Recovery Options** page, you can specify e-mail addresses to receive notification upon completion of the recovery. Click **Next** to continue.
7. On the **Summary** page, review the settings and then click **Recover**.

To copy a tape using DPM Management Shell

- Use the following syntax to copy a tape:

  Copy-DPMTapeData [-RecoveryPoint] <*RecoverySource*> **-SourceLibrary** <*Library*> **-TargetLibrary** <*Library*> **-TapeLabel** <*String*> **-TapeOption** <*TapeOptions*> **[-RecoveryPointLocation** <*RecoverySourceLocation*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to copy the recovery points from a tape:

  Copy-DPMTapeData [-RecoveryPoint] <*RecoverySource*> **[-RecoveryPointLocation** <*RecoverySourceLocation*>**] -Tape** <*Media*> **[-Restore] -OverwriteType** <*OverwriteType*> **[-RecreateReparsePoint] [-RestoreSecurity] -TargetServer** <*String*> **-TargetPath** <*String*> **[-RecoveryNotification** <*NotificationObject*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable**<*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to copy headless data from a tape:

Copy-DPMTapeData -IncompleteDataset <*HeadlessDataset*> **-Tape**<*Media*> **[-Restore] -OverwriteType** <*OverwriteType*> **[-RecreateReparsePoint] [-RestoreSecurity] -TargetServer** <*String*> **-TargetPath** <*String*> **[-RecoveryNotification** <*NotificationObject*>**] -DPMServerName** <*String*> **[-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

For more information, type "**Get-Help Copy-DPMTapeData -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Copy-DPMTapeData -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Mark a Tape as a Cleaning Tape

To clean a drive in a tape library using DPM, you specify which tape to use for cleaning, and then start the cleaning job. If the bar code on a tape starts with "CLN" (for example, bar code CLN0000812), DPM identifies the tape as a cleaning tape after a fast inventory.

However, if the cleaning tape does not have a bar code or the bar code does not start with "CLN", you must mark the tape as a cleaning tape and then run a detailed inventory. If you do not mark the tape as a cleaning tape before you run a detailed inventory, a cleaning job will start when DPM mounts this tape during the detailed inventory.

Follow the guidelines from the manufacturer of your tape device for cleaning frequency.

To mark a tape as a cleaning tape

1. In DPM Administrator Console, go to the **Management** view.
2. Open the **Libraries** workspace.
3. In the display pane, select the tape to be used for cleaning, and then click **Mark as cleaning tape**.
4. Go to the **Management** view.
5. In the **Libraries** workspace, select a library.
6. Click **Inventory**.
7. In the **Inventory** dialog box, select **Detailed inventory**, and then click **Start**.

To mark a tape as a cleaning tape using DPM Management Shell

- Use the following syntax to mark a tape as a cleaning tape:

Set-Tape [-Tape] <*Media[]*> **-Cleaner [-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

For more information, type "**Get-Help Set-Tape -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Set-Tape -full**" in DPM Management Shell.

See Also

How to Clean a Tape Drive

How to Inventory the Tape Library

Managing Tapes

How to Specify Tape Catalog Retention

DPM maintains metadata for each tape in a database, referred to as the *tape catalog*. You can manage the retention settings for the tape catalog to determine when the catalog is *pruned*, which consists of removing entries from the catalog.

DPM will automatically prune the catalog when the retention range for the protection group expires. You can direct DPM to prune the catalog for all protection groups sooner to reduce the size of the database. Because the duration of the catalog retention impacts the size of the DPM database, you can use the **Tape Catalog Retention** dialog box to alert you when the DPM database reaches a specific size.

To specify tape catalog retention

1. In DPM Administrator Console, go to the **Protection** view.
2. Select a protection group.
3. Click **Specify tape catalog retention**.
4. To prune the catalog when the retention range expires, select **Prune catalog when protection group retention range expires.**

   -or-

   To prune the catalog for a specific tape duration, select **Prune catalog for tapes older than**, and then select the tape duration that you want to use.

   Note
   You cannot retain catalog data longer than the retention range for the protection group.
5. If you want DPM to alert you when the DPM database reaches a specific size, in the **DPM Database** section, select **Alert me when the DPM database size reaches**, and then specify the size of the database.

6. Click **OK**.

See Also

Managing Tapes

How to Verify Data on Tape

The **Verify tape** action verifies whether the selected recovery point on tape is recoverable. During verification, DPM mounts and reads the tape on which the data exists. You can monitor the progress of verification in the **Monitoring** task area on the **Jobs** tab.

If the selected recovery point is stored on tape that is not in the tape library, DPM will queue the job for one hour. You must add the tape that contains the selected recovery point to the library within the one hour timeframe or the job will expire.

To verify data on tape by selecting a recovery point

1. In DPM Administrator Console, go to the **Recovery** view.
2. Select a recovery point that is on tape.
3. Click **Verify tape** from the tool ribbon.

To verify data on a tape by selecting a recovery point using DPM Management Shell

- Use the following syntax to verify the data on a tape:

  Test-DPMTapeData [-RecoveryPoint] <*RecoverySource*> **[-RecoveryPointLocation** <*RecoverySourceLocation*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Test-DPMTapeData -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Test-DPMTapeData -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Reschedule a Maintenance Job

You can set the schedules for maintenance jobs to be carried out on the DPM server only by using DPM Management Shell.

To schedule a maintenance job

- Use the following syntax to retrieve the current schedule for maintenance jobs to run on a DPM server:

  Get-MaintenanceJobStartTime [-DPMServerName] <*String*> **[-MaintenanceJob]** <*HouseKeepingJobs*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to set the schedule for maintenance jobs to run on a DPM server:

  Set-MaintenanceJobStartTime [-DPMServerName] <*String*> **[-MaintenanceJob]** <*HouseKeepingJobs*> **[[-StartTime]** <*DateTime*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to remove the schedule for maintenance jobs to run on a DPM server:

  Set-MaintenanceJobStartTime [-DPMServerName] <*String*> **[-MaintenanceJob]** <*HouseKeepingJobs*> **[-Remove] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Set-MaintenanceJobStartTime -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Set-MaintenanceJobStartTime -full**" in DPM Management Shell.

See Also

How to Reschedule a Protection Job Using DPM Management Shell

Managing Tapes

Rotating Tapes Offsite

DPM Administrator Console indicates when a tape in the library should be removed and stored in your archive location by displaying a green icon in the **Offsite Ready** column. You can also view all tapes ready to be stored offsite in the Tape Management Report. The Tape Management Report lists tapes that will be due for offsite storage in the upcoming period selected for the report.

A tape can be marked as **Offsite Ready** for one of three reasons.

Reason	Description
Tape is full	When a tape is full, DPM marks it as **Offsite Ready**.
Expired data set	A data set on the tape has expired.
Write Period Ratio has been crossed	Write Period Ratio is calculated as (Time of first backup + 15% of retention range).

When the data on a tape expires, return the tape to the tape library. Expired tapes not returned to the tape library are marked as "overdue" in the Tape Management Report. Overdue tapes expired during an earlier reporting period. Expired tapes should be returned to the tape library for reuse.

See Also

Managing Tapes

Recovering Data from Tapes

Recovering Data from Tapes Created by Another DPM Server

To recover data from tapes created by another DPM server, such as when a DPM server fails and critical information must be recovered before the server can be restored, you must first physically add the tape to a DPM server and then use the **Recatalog imported tape** action.

During the recatalog operation, DPM reads from the tape and adds information about the data it contains to the database. After recatalog completes, you can recover data from the tape by selecting a recovery point from the data on the tape.

Recovering Data When a Tape Set Is Missing a Tape

When protected data, such as a volume or a SQL Server database, spans multiple tapes, all tapes from the tape set must be available for DPM to recover the data. When a tape from a tape set is missing, perform the following steps to access the remaining data:

1. Add the tape to the tape set. You might need to recatalog the tape.
2. View the contents of the tape.

3. Copy the contents of the tape to the desired location.

After you copy the contents of the remaining tapes, you can use the copied data as you like.

See Also

How to Add or Remove a Tape

How to Import Tapes

How to View Tape Contents

How to Copy a Tape

Recovering Data from Expired Tapes

DPM does not allow you to recatalog a tape that has expired. To recover data from such a tape, use the following procedure.

Note

After you recatalog the contents of an expired tape, the recovery points from this tape will appear as **External DPM Tapes** on the Recovery tab.

To recover data from an Expired tape

1. On the Administrator Console, right-click the expired tape, and then click **Mark tape as free**.

   This changes the status of the tape to **Free (contains data)**.
2. Right-click the tape again and then click **Unmark tape as free**.

   This changes the status of the tape to **Imported <original tape label>**.
3. Right-click the tape again and then click **Recatalog imported tape**.

See Also

Recovering Data from Tapes

Working with Certificates

System Center 2012 – Data Protection Manager (DPM) uses certificates to encrypt the backups to tape. You can use one or a combination of multiple certificates to encrypt your backups. During installation, DPM creates two folders, DPMBackupStore and DPMRestoreStore, in the DPM Certificate Store.

Storing Certificates

You must store you current certificates in DPMBackupStore folder in the Certificate Store. DPM will use these certificates to encrypt data. You can store multiple certificates there if you want DPM to create a key by using more than one certificate.

Storing Expired Certificates

When your certificates expire, you must move them into the DPMRestoreStore folder in the Certificate Store. This ensures that you can recover the expired certificates from an encrypted tape by using a certificate that is no longer active.

Tip

We recommend that you move your expired certificates and your tapes to the DPMRestoreStore folder.

Short Erase

By default, when you erase a tape by using System Center 2012 – Data Protection Manager (DPM), it performs a long erase. If your tape drive supports short erase, you can use DPM to enable it to perform a short erase by following the instructions in this topic.

Enabling Short Erase

If your tape drive supports short erase, you can enable it on the DPM server by creating the DWORD **UseShortErase** under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent`.

Set the value of the DWORD to 00000000.

After this value is set, all erase operations on the DPM server will be short erases. To revert to long erases, remove this registry key.

Important

Though short erase is much faster than long erase, it does not completely erase the data from the tape. If you have a policy that all data from the tape must be erased and unrecoverable, do not enable short erase.

How DPM Uses Stand-Alone Tape Drives

For stand-alone tape drives, System Center 2012 – Data Protection Manager (DPM) does the following for each protection group:

- Appends all short-term backups to a single tape.

- Appends all long-term backups to a single tape that is different from the short-term backup tape.

When a tape fills up, DPM raises an alert to add a new free tape.

How DPM Uses Tape Libraries

System Center 2012 – Data Protection Manager (DPM) may allocate two or more tapes for each protection group.

All the data sources in a protection group will always append to the same tape regardless of whether short-term or long-term protection is specified.

If the user specifies the allocation of more than one drive while creating the protection group, the data sources will be split across tapes. For example, if there are five data sources and a drive with a maximum limit of two sources, DPM may write three data sources on one tape and two on another. Depending on the size of the data sources, other scheduled backup jobs to tape in other protection groups, and the number of tape drives available at the time, you may find an uneven distribution of data sources going to the various tapes.

Short-Term Tape Protection

The following table shows how the backup mode influences the number of tapes required for short-term protection.

Backup mode	Tapes required
Short-term tape "full" option	Backup jobs will require a free tape for each scheduled job.
Short-term tape "full and incremental" option	The full backup will require a free tape for each scheduled job, and the incremental backup for all data sources will be appended to a single separate tape. As tapes fill up, new free tapes will be allocated. When the next full backup occurs, it will require another free tape, and subsequent incremental backups will be appended to another free tape.

Example: If a full backup is scheduled weekly and incremental backups are scheduled daily, then the first full backup will go to a new free tape and all subsequent incremental backups for six days will be appended to another new free tape.

If a full backup job fails before it is completed, all the subsequent incremental jobs will use the existing tape that has valid previous incremental backups.

Note

If the customer manually triggers two individual “create recovery point (tape)” actions for two protection group members, DPM will create two tape backup jobs and will need two tapes to store tape backup. However, if two protection group members are selected (multi-select in Protection view) and “create recovery point (tape)” is triggered, DPM will use a single tape. This is designed to co-locate the data for selected protection group members for ad-hoc tape backups onto the same tape.

Long-Term Tape Protection

A tape will be allocated for each full backup job. The reason long-term full tape backups are on separate tapes is because they are meant to be stored offline, and possibly offsite. So each long-term backup recovery point created will always be on a new tape.

Note

Available free tapes will be decremented as tapes are allocated to either short-term or long-term tape jobs. However, for short-term protection, creating a new recovery point will succeed even when the "available free tapes = 0" because DPM will append the backup job to the tape that is currently in use. Only long-term tape backups require a new tape each time, and these backups will issue an alert if no tapes are available.

More Information

You cannot free or erase a tape that contains valid recovery points from any protected source. Before you can free a tape, you must perform one of the following steps:

- Remove the sources from the protection group and choose to expire recovery points on the tape.
- Change the protection group’s options and clear the tape protection options. Then, under **Inactive protection for previously protected data**, right-click each data source and select **Remove inactive protection**.

To restore data from an expired tape, mark the tape as free, then unmark the tape as free, and then recatalog the tape.

Managing Tape Libraries

In This Section

How to Remap Tape Drives
How to Rename a Tape Library
How to Remove Tape Libraries
How to Lock and Unlock a Library Door
How to Enable and Disable a Drive
How to Clean a Tape Drive
How to Set Up Tape Library Sharing

See Also

Managing Disks

How to Enable and Disable a Library

You can temporarily disable a tape library or stand-alone tape drive in DPM to perform maintenance or repairs. When you are ready to return the tape library or stand-alone tape drive to operation, you must enable it.

To enable a library

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the **Display** pane, select the tape library or stand-alone tape drive that is disabled.
3. Click **Enable library**.

To enable a library using DPM Management Shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to enable a library:

  Enable-DPMLibrary [-DPMLibrary] <*Library[]*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Enable-DPMLibrary -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Enable-DPMLibrary -full**" in DPM Management Shell.

To disable a library

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the **Display** pane, select the tape library or stand-alone tape drive to be disabled.
3. Click **Disable library**.

To disable a library using DPM Management Shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to disable a library:

  Disable-DPMLibrary [-DPMLibrary] <*Library[]*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**] [-WhatIf] [-Confirm]**

  For more information, type "**Get-Help Disable-DPMLibrary -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Disable-DPMLibrary -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Display Tape Libraries and Drives in DPM Administrator Console

To install a tape library or stand-alone tape drive on the DPM server, follow the instructions provided with the tape device. An installed tape device will be listed in Device Manager.

DPM supports a number of tape libraries for backup, recovery, and archive of business-critical data. Ensure that the medium changer and the tape drives have serial numbers.

DPM will identify a tape library or stand-alone tape drive that is physically attached to the DPM server and display the tape device information in DPM Administrator Console in the **Libraries** workspace of the **Management** view.

Ensure the following,

If the tape library or stand-alone tape drive is not displayed in DPM Administrator Console, use the **Rescan** action to update the display. After you perform **Rescan**, ensure that the medium

changer is displayed in the device manager and number of tape drives displayed in the device manager and in the tape library are same.

If your tape library is displayed as a stand-alone tape drive or if the state of your library in DPM Administrator Console does not reflect the physical state accurately, you might need to correct the tape drive mapping. For more information about remapping tape drives, see Managing Tapes.

To check for new tape libraries or stand-alone tape drives

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. Click **Rescan**.

See Also

How to Rename a Tape Library

Managing Tapes

How to Inventory the Tape Library

The purpose of an inventory operation is to identify new tapes and recognize tapes DPM has seen before.

A *fast inventory* involves reading the bar code of each tape in the library. DPM can perform a fast inventory for tapes that have bar codes in a tape library that has a bar code reader.

A *detailed inventory* involves reading the header area of a tape in the library to identify the on-media identifier (OMID) on each tape. DPM must perform a detailed inventory when a tape does not have a bar code or the tape library does not have a bar code reader.

A fast inventory will detect any tape (with or without a bar code) in any library. However, to uniquely identify the media, perform a detailed inventory.

To inventory tapes in a library

1. In DPM Administrator Console, go to the **Management** view.
2. In the **Libraries** workspace, select a library.
3. Click **Inventory**.
4. In the **Inventory** dialog box, select **Fast inventory** or **Detailed inventory**, and then click **Start**.

To inventory tapes in a library using DPM Management Shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer**

<*Int32*>**]**

- Use the following syntax to perform a fast inventory:

  Start-DPMLibraryInventory [-DPMLibrary] <*Library*> **[-FastInventory] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

- Use the following syntax to perform a detailed inventory:

  Start-DPMLibraryInventory [-DPMLibrary] <*Library*> **-DetailedInventory [-Tape** <*Media[]*>**] [-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Start-DPMLibraryInventory -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Start-DPMLibraryInventory -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Remap Tape Drives

The **Rescan** action on the tool ribbon in the **Libraries** workspace of the **Management** view causes DPM to examine the tape drives that are attached to the DPM server and update the information displayed on the **Libraries** tab. The **Libraries** tab displays each stand-alone tape drive, and each tape library and its drives.

When the physical state of the tape drives does not display correctly in DPM Administrator Console, you need to remap the tape drive information. For example, drives from a tape library are listed as stand-alone tape drives, a drive for Library 1 is listed as belonging to Library 2, or a stand-alone tape drive is reported as a drive within another library rather than as a stand-alone tape drive.

Note
If a tape drive is not mapped correctly, jobs that require the tape drive that is incorrectly mapped will fail.

You can either use the DPMDriveMapping.exe or manually create the DPMLA.xml to remap a tape drive.

Remapping Tape Drive Using DPMDriveMapping.exe

To correct the tape drive mapping, you must create a file named DPMLA.xml with the correct information, and then click **Rescan**. You can create this file using DPMDriveMapping.exe from the <*DPM Install*>\Bin folder.

Ensure the following before you run DPMDriveMapping.exe:

- DPMLA service should not be running.
- There should not be any tapes in the drive.
- There should be at least one tape in each library which is not marked as Cleaner.

Procedure to Remap Tape Drive using DPMDriveMapping.exe

1. Run DPMDriveMapping.exe from <*DPM Install*>\Bin folder.
2. Start the DPM Administrator Console.
3. Click **Rescan**.

Remapping Tape Drive Manually

Procedure to remap tape drive manually

1. Create DPMLA.xml.
2. Start DPM Administrator Console.
3. Click **Rescan**.

Creating DPMLA.xml

You can create the DPMLA.xml using the template provided with DPM.

Procedure to create DPMLA.xml

1. Open LADriveRemappingTemplate.xml from Microsoft Data Protection Manager\DPM\Config in an XML editor or Notepad
2. Follow the instructions in the template file
3. Save the file as DPMLA.xml in the Microsoft Data Protection Manager\DPM\Config folder. You must save the file using the Unicode format.

Important

You should not make changes to LADriveRemappingTemplate.xml because future updates to DPM might include changes to the template file. If you modify LADriveRemappingTemplate.xml, updates to DPM cannot replace the template file.

The following is an example of the contents of a DPMLA.xml file that maps a drive that is reported as a stand-alone tape drive into a library at the drive bay 0 in the library:

```
<?xml version="1.0" encoding="utf-16"?>
<LAConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.microsoft.com/2003/dls/LAConfig.xsd">
  <DriveReMapInfo IsMannuallyMapped="true">
    <DriveLibraryAssociation>
      <Drive SerialNumber="HUL4B06579" SCSIPort="10" SCSIBus="23" SCSITargetId="80"
SCSILun="4" DriveBayIndex="0" />
      <Library SerialNumber="2B41146637" SCSIPort="6" SCSIBus="5" SCSITargetId="0"
SCSILun="1" />
    </DriveLibraryAssociation>
  </DriveReMapInfo>
</LAConfig>
```

How to Rename a Tape Library

You can use the default name assigned to the tape library or stand-alone tape drive when it was installed, or you can assign it a new name. When you use DPM to rename a tape library or stand-alone tape drive, the device name is changed only in DPM Administrator Console.

To rename a tape library

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, select the tape library or stand-alone tape drive that you want to rename.
3. Click **Rename library**.
4. In the **Rename Library** dialog box, type the new name, and then click **Rename**.

To rename a tape library using DPM Management Shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] <*String*> **[-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to rename the library:

  Rename-DPMLibrary [-DPMLibrary] <*Library*> **[-NewName]** <*String*> **[-PassThru] [-**

Verbose] [-Debug] [-ErrorAction <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

For more information, type "**Get-Help Rename-DPMLibrary -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Rename-DPMLibrary -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Remove Tape Libraries

If you physically disconnect a tape library or stand-alone tape drive, or physically remove a drive from inside a library that is associated with a protection group, DPM Administrator Console displays the disconnected or removed tape library or stand-alone tape drive as offline.

If you disconnect or remove a tape library or stand-alone tape drive that is not associated with a protection group, the entry for the tape library or stand-alone tape drive is removed from DPM Administrator Console during the daily inventory or when rescan runs, whichever occurs first.

If you remove a tape library that is associated with a protection group and you do not intend to bring the tape library online again, you should modify the protection group to specify a different tape library. When all protection groups that were associated with the tape library that you removed are associated with other tape libraries, the entry for the tape library or stand-alone tape drive will be removed from DPM Administrator Console during the daily inventory or when rescan runs, whichever occurs first.

See Also

How to Enable and Disable a Library

How to Enable and Disable a Drive

How to Lock and Unlock a Library Door

If your tape library does not have an insert/eject (I/E) port, you can use the following procedures to lock or unlock the tape library door.

To lock a tape library door

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** tab.

2. In the display pane, select the library that you want to lock.
3. Click **Lock library door**.

To lock a tape library door using DPM Management Shell

- Use the following syntax to unlock a library door:

  Lock-DPMLibraryDoor [-DPMLibrary] <*Library*> **[-Async] [-DoorAccessJobStateChangeEventHandler** <*DoorAccessJobStateChangeEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Lock-DPMLibraryDoor -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Lock-DPMLibraryDoor -full**" in DPM Management Shell.

To unlock a tape library door

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, select the library that you want to unlock.
3. Click **Unlock library door**.

To unlock a tape library door using DPM Management Shell

- Use the following syntax to unlock a library door:

  Unlock-DPMLibraryDoor [-DPMLibrary] <*Library*> **[[-Timeout]** <*Int32*>**] [-Async] [-DoorAccessJobStateChangeEventHandler** <*DoorAccessJobStateChangeEventHandler*>**] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Unlock-DPMLibraryDoor -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Unlock-DPMLibraryDoor -full**" in DPM Management Shell.

See Also

How to Add or Remove a Tape

Managing Tapes

How to Enable and Disable a Drive

You can temporarily disable a drive in tape library or stand-alone tape drive in DPM to perform maintenance or repairs. When you are ready to return the drive to operation, you must enable it.

To enable a drive

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library or stand-alone tape drive, and click the drive that is disabled.
3. Click **Enable drive**.

To enable a drive using DPM Management Shell

- Use the following syntax to retrieve the drive:

  Get-DPMTapeDrive [-DPMLibrary] <*Library[]*> **[-Verbose] [-Debug][-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**][-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to enable the drive:

  Enable-DPMTapeDrive [-TapeDrive] <*Drive[]*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Enable-DPMTapeDrive -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Enable-DPMTapeDrive -full**" in DPM Management Shell.

To disable a drive

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, expand the tape library or stand-alone tape drive, and click the drive to be disabled.
3. Click **Disable drive**.

To disable a drive using DPM Management Shell

- Use the following syntax to retrieve the drive:

  Get-DPMTapeDrive [-DPMLibrary] <*Library[]*> **[-Verbose] [-Debug][-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**][-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to disable the drive:

Disable-DPMTapeDrive [-TapeDrive] <*Drive[]*> **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**] [-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**] [-WhatIf] [-Confirm]**

For more information, type "**Get-Help Disable-DPMTapeDrive -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Disable-DPMTapeDrive -full**" in DPM Management Shell.

See Also

Managing Tapes

How to Clean a Tape Drive

To clean a drive in a tape library, you must specify which tape to use for cleaning, and then start the cleaning job. If a cleaning tape is online and marked as a cleaning tape, you only need to run the cleaning job.

Follow your hardware manufacturer's recommendations for cleaning frequency. To clean a stand-alone tape drive, load a cleaning tape and follow the hardware manufacturer's instructions.

To clean a tape drive

1. In DPM Administrator Console, go to the **Management** view, and then open the **Libraries** workspace.
2. In the display pane, select the drive to be cleaned, and then click **Clean drive**.

To clean a tape drive using DPM Management Shell

- Use the following syntax to retrieve a tape drive:

  Get-DPMTapeDrive [-DPMLibrary] <*Library[]*> **[-Verbose] [-Debug][-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**][-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**
- Use the following syntax to clean a drive:

  Start-DPMTapeDriveCleaning [-TapeDrive] <*Drive[]*> **[-JobStateChangedEventHandler** <*JobStateChangedEventHandler*>**] [-Verbose] [-Debug][-ErrorAction** <*ActionPreference*>**] [-ErrorVariable** <*String*>**][-OutVariable** <*String*>**] [-OutBuffer** <*Int32*>**]**

  For more information, type "**Get-Help Start-DPMTapeDriveCleaning -detailed**" in DPM Management Shell.

  For technical information, type "**Get-Help Start-DPMTapeDriveCleaning -full**" in DPM Management Shell.

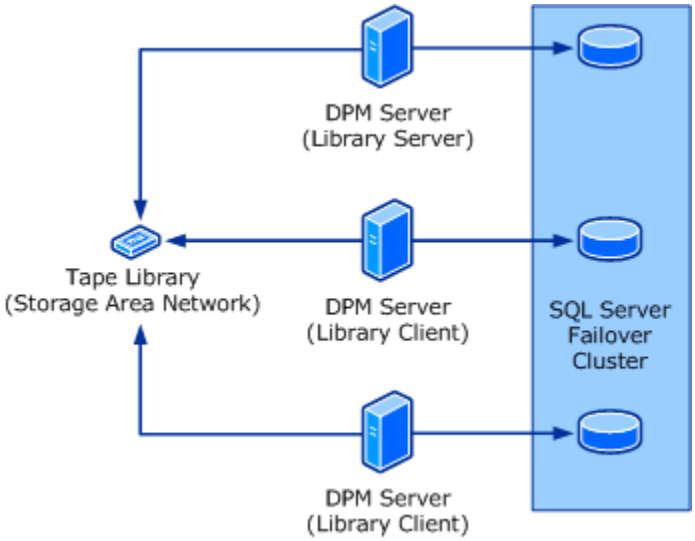
See Also

[How to Mark a Tape as a Cleaning Tape]

[Managing Tapes]

How to Set Up Tape Library Sharing

With System Center 2012 – Data Protection Manager (DPM), you can share a single tape library across multiple DPM servers. The following illustration shows the topology of a shared library.



- The tape library is typically a collection of tape drives that automatically mount and dismount tape media.

  Note

  The tape library must be in a storage area network (SAN) environment.
- The *library server* is a computer on which DPM is installed, the library-sharing command has been run, and the medium changer is enabled.
- A *library client* is a computer on which DPM is installed, the library-sharing command has been run, and the medium changer is not enabled.

Note

- We recommend that the system configuration of the library server computer and all library client computers be as similar as possible, and that you do not configure any protection groups on the library server.
- All DPM servers using a shared library must use a similar SQL Server setup for hosting DPM databases. For example, they should all use a local instance of the DPM database or all of them should use a remote instance. You cannot have some DPM servers using local instance and others using a remote instance.

Setting up library sharing

Use the following steps to set up library sharing:

1. On the computer that will be the library server for the shared library, enable the medium changer by using Device Manager.
2. On each library client computer, ensure that the medium changer is not enabled.
3. Enable Named Pipes protocol for the SQL Server instances of the library server and library client computers. Then restart the SQL service.
4. Run the following commands to configure the DPM servers to use a shared library:
5. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

   AddLibraryServerForDpm.exe –DpmServerWithLibrary <FQDN of library server>

   where <*FQDN of library server*> is the fully qualified domain name of the library server.

6. On the library server computer, open an elevated Command Prompt window, and then run the following commands one time for each library client. For example, if your library server supports three library clients, you must run this command three times on the library server.

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

   AddLibraryServerForDpm.exe – ShareLibraryWithDpm <FQDN of library client>

   where <*FQDN of library client*> is the fully qualified domain name of the library client.

7. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

   Important

   Do not run these commands on the library server.

   Note

   Before you run the following commands, on all library client computers ensure that both the SQL Server (MSDPM2012) and SQL Server Agent (MSDPM2012) services use a domain user account as the logon account, not a local account, which is the default configuration, and that the domain account that is used is a member of the local Administrator group on all of the computers that are sharing the library.

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

   SetSharedDpmDatabase -DatabaseName <**SqlServer\Instance\DatabaseName**> [-DoNotMoveData]

   where <*SQLServer\Instance\Databasename*> is the database name of the library server.

   Tip

You can find this information in the **About DPM** window as DPM's SQL Server. You can copy this information from there, using your mouse.

8. In DPM Administrator Console on the library server, perform a rescan, and then perform a rescan or refresh on each of the library client computers.

   Note
   The quickest way to see all media on all of the DPM servers is to perform a rescan on each, followed by a detailed inventory. Next, on any one of the servers, mark a number of media as free, and then perform a refresh on the other servers.

After you have configured library sharing, you can use the shared tape library as if it were attached to each DPM server.

Turning on AutoRefresh for the DPM server

You can set the auto-refresh interval for the library by using the **Set-DPMGlobalProperty** cmdlet in DPM Management Shell. The syntax for the cmdlet is as follows:

`Set-DPMGlobalProperty -DPMServerName` *<DPMServerName>* `-LibraryRefreshInterval` *<LibraryRefreshInterval>*

where *<DPMServerName>* is the computer name of the DPM server and *<LibraryRefreshInterval>* is the time interval in minutes.

You must set **LibraryRefreshInterval** to a value greater than or equal to five (5). Setting it to less than five automatically resets it to zero (0), which means the refresh does not occur.

Note
After you have run the **Set-DPMGlobalProperty** cmdlet, you must close, and then reopen DPM Administrator Console for the auto-refresh settings to take effect.

Library server failure

If the library server fails, DPM detects the failure and raises an alert. All tape jobs scheduled to run fail while the library server is down. DPM checks at 20-minute intervals to see if the library server is working again.

If you cannot resolve the problem on the library server, or do not want to wait for the library server to come back online, you can promote another DPM server as the library server.

To promote another DPM server to library server

Use the following procedure to promote another server to library server:

1. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

SetSharedDpmDatabase.exe –RemoveDatabaseSharing

AddLibraryServerForDpm.exe –DpmServerWithLibrary <FQDN of the library server> -remove

where <*FQDN of library server*> is the fully qualified domain name of the old library server.

Note
Also ensure that the DPM Administrator Console is functioning correctly on each library client.

2. On the computer that you want to promote as the new library server, enable the medium changer in Device Manager.
3. On the computer that you want to promote as the new library server, open an elevated Command Prompt window, and then run the following commands one time for each of the library client computers:

   cd <system drive>:\Program Files\Microsoft DPM\DPM\Setup

   AddLibraryServerForDpm.exe –ShareLibraryWithDPM <FQDN of client library>

   where <*FQDN of client library*> is the fully qualified domain name of the library client.

4. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

   cd <system drive>:\Program Files\Microsoft DPM\Setup

   SetSharedDpmDatabase -DatabaseName <**SqlServer\Instance\DatabaseName**> [-DoNotMoveData]

   where <*SQLServer**Instance**Databasename*> is the database name of the library server.

   Tip
   You can find this information in the **About DPM** window as DPM's SQL Server. You can copy this information from there, using your mouse.

Known issues

DPM cmdlets that apply to library sharing only work when they are run on the local computer.

Co-Locating Data

System Center 2012 – Data Protection Manager (DPM) allows you to co-locate your protection groups on a volume or tape. Co-locating your protection groups allows you to use your storage more effectively.

In This Section

Co-Locating Data on Disk

In System Center 2012 – Data Protection Manager (DPM), you must have one replica volume and one recovery point volume per protected data source. DPM supports data co-location, which allows you to have multiple data sources mapping on a single replica and recovery point volume. This enables you to store data more efficiently on a DPM server.

DPM supports co-location for the following data sources:

- Hyper-V virtual machines
- Laptop/desktop
- SQL Server 2005 and SQL Server 2008 databases

See Also

Enabling Data Co-Location

You can enable co-location through the Create New Protection Group Wizard. If DPM supports co-location for the data source you are protecting, the Review Disk Allocation page of the wizard will show you a checkbox that allows you to select co-location. If you have not selected any co-locatable data sources, this option will be grayed out.

Since the data sources now share a volume, they will also share recovery points. Removing the recovery point for any one of the co-located data sources, will mean losing recovery points of the other data sources sharing this volume.

You can look at the size allocated to each volume and the number of data sources co-located on each volume by clicking **Modify** on the Review Disk Allocation Page. Each row in the table represents one volume. Click **Collocated Protection** to see the data sources that share that volume.

Colocating Hyper-V data

System Center 2012 SP1 increases the scale supported for Hyper-V virtual machines. The 250 GB colocation size in System Center 2012 is not sufficient when you protect large scale deployments of Hyper-V virtual machines. For example, if the virtual machine is 100 GB in size, DPM will be able to put one virtual machine in a volume. DPM supports protecting up to 800 virtual machines on one DPM server. This requires increasing the colocation limits to 450 GB. You can do this by editing the following registry keys:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Collocation\HyperV
Value	CollocatedReplicaSize
Data	**Enter value in bytes**
Type	DWORD

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Collocation\HyperV
Value	DSCollocationFactor
Data	**Enter a number between 1 and 8** The recommended value is 3.
Type	DWORD

Collocation will reduce the number of volumes that will be required on DPM server to support the scale of 800 Hyper V data sources.

See Also

New Protection Group Wizard

Stopping Protection for Co-Located Data

You can stop protection for co-located data sources like you would for any data source using the Modify Protection Group Wizard and removing the data source from the protection group.

- If you stop protection with the **Retain Data** option, DPM will retain the recovery points of the selected data sources as long as the retention range of the data source is not exceeded.

After the retention range has been exceeded, DPM will remove the recovery points as part of its daily pruning job. However, the replica of that data source will be preserved until the replica volume is eliminated or the data sources that coexisted with the deleted data source are deleted from protection.

- If you re-protect the data source that you removed from a protection group in another protection group, the pruning schedule will depend on which of the protection groups has a longer retention range. For more information about the behavior when data sources are migrated out of a co-located protection group, see Moving Between Co-Located and Non-Co-Located Protection Groups
- If you stop protection without **Retain Data**, DPM will remove the records of that data source from the DPMDB. The replica volume space that was used by the replica of those data sources will be made available for co-locating more data sources in the same protection group.
- If you try to restore a database that was once co-located and then later removed, the status of the replica will show as **Inconsistent**. To handle this situation, run a consistency check on the replica. This will allow you to proceed with the recovery.

See Also

Moving Between Co-Located and Non-Co-Located Protection Groups

Moving Between Co-Located and Non-Co-Located Protection Groups

Reprotecting Non–Co-Located Data to a Co-Located Protection Group

DPM first tries to add the inactive data source to an existing replica volume that has the required space for reprotecting the inactive data source. If DPM does not find space on an existing replica volume, it creates a new volume and then copies data from the inactive replica to the selected replica volume in the destination protection group.

After copying the data to the destination protection group, the member data source at the destination protection group is marked as Inconsistent and a consistency check is recommended.

The recovery points associated with the old replica will be deleted according to the retention range of the new protection group. After the last recovery point has been pruned, the old replica volume will be deleted.

Reprotecting Co-Located Data to a Non–Co-Located Protection Group

A new volume will be created and the data source will be added to it. If the volume has other data sources on it, all of which are inactive, only then the volume will be reused for one of the data sources. The old recovery points will be pruned as per the data source with the longest retention period.

The following examples take you through various scenarios to explain this behavior.

Scenario 1: Assume data source DS1 was protected on a co-located protection group PG1 that had a retention range of 3 days. If you were to remove DS1 from PG1 and re-protect it as a part of another protection group PG2 that has a retention range of 5 days, at the time of pruning the recovery points of PG1, the retention range of PG2 will take precedence as long as there are recovery points for DS1 on the recovery point volume.

Scenario 2: Assume protection group PG1 with retention range of 3 days has five data sources DS1 to DS5. Of these data sources DS1 is moved to PG2 that has a retention range of 4 days and DS3 is moved to PG3 that has a retention range of 5 days. Pruning of the recovery points for PG1 will follow the retention range of PG3 until there are no more recovery points of DS3 left. Then it will follow the retention range of PG2, if there are any recovery points of DS1 remaining. Finally when the recovery points of DS1 and DS3 are all pruned off, the retention range schedule will revert to PG1's schedule.

Co-Locating Data on Tape

System Center Data Protection Manager (DPM) allows you to co-locate protection groups on a tape. Using this feature, you can group recovery points of multiple protection groups on a single tape. This optimizes the tape usage in case you have many small protection groups.

Restrictions

The following restrictions apply to using data co-location in DPM:

- You cannot apply co-location selectively. If enabled, it applies to all protection groups.
- Only protection groups with the same retention period can be co-located on the same tape.
- Encrypted and non-encrypted datasets cannot be co-located on the same tape.
- Datasets from short-term backup to tape and long-term backup to tape cannot be collocated.

See Also

Enabling Data Co-Location

Stopping Protection for Co-located Data

Enabling Data Co-Location

Enabling Data Co-Location on DPM

1. Open DPM Management Shell.
2. Set-OptimizeTapeUsage to True using the Set-DPMGlobalProperty cmdlet.
   Set-DPMGlobalProperty -DPMServerName <name of DPM server> -OptimizeTapeUsage $True

After data co-location has been enabled, DPM will check for the following conditions before allocating a tape:

1. The expiry date of the current dataset should fall in between the following dates:
   Upper bound: **furthest expiry date among all the datasets on the tape - (furthest expiry date among all the datasets on the tape - current date) * ExpiryToleranceRange**
   Lower Bound: **furthest expiry date among all the datasets on the tape + (furthest expiry date among all the datasets on the tape - current date) * ExpiryToleranceRange**.
2. Current time should be less than **first backup time of the dataset on the media + TapeWritePeriodRatio * RetentionRangeOfFirstDataset**.

A dataset will be collocated only if both the above conditions are true.

Term	Description
TapeWritePeriodRatio	Indicates the number of days for which data can be written on to a tape as a fraction between 0 and 1. The default value is 0.15.
ExpiryToleranceRange	Indicates the time window within which the expiry date of the dataset to be written to the tape must fall. It is expressed as a percentage. The default value is 17 percent. This is a DWORD type registry value located under HKLM\Software\Microsoft\Microsoft Data Protection Manager\1.0\Colocation. DPM does not create this key automatically. You must manually create this key if you want to set the ExpiryToleranceRange.

Note
When tape co-location is enabled, a tape on to which offsite backup is written will not be shown as **Offsite Ready** unless one of the following conditions are met:

- The tape is full.
- One of the datasets has expired.

- Write-period ratio has been crossed. (By default, this is first backup time + 15 per cent of retention range.)

Stopping Protection for Co-located Data

Stopping Data Co-Location

1. Open DPM Management Shell.
2. Set **-OptimizeTapeUsage** to False using the **Set-DPMGlobalProperty** cmdlet.
   Set-DPMGlobalProperty -DPMServername <name of DPM server> -OptimizeTapeUsage $False

Tape Optimization Setup

Use the tape optimization feature in System Center 2012 – Data Protection Manager (DPM) to allow multiple protection groups to share a tape to store their backups. DPM aims to improve the support for this feature to allow more flexibility to you around what you colocate and how.

To optimize tape usage, DPM uses protection group sets. A protection group set is a set of protection groups whose backups the DPM administrator wants to colocate on to a tape. However, just because a set of protection groups belong to a set, does not mean that they will be colocated to a tape. This is decided by the write period and expiration tolerance values.

Write period is the length of time for which a tape is available for writing new backups. The tape is marked as Offsite Ready after this.

Expiration tolerance is the maximum length of time for which an expired recovery point can remain on a tape until the tape is marked as expired.

Setting up a protection group

1. Go to the Library view.
2. Click **Optimize usage** on the **Actions** pane.

   This brings up the Tape Optimization Setup dialog box.

   You can use this screen to create, modify or delete protection group sets.

Tape Optimization Setup - Create/Modify Protection Group Set

Create a protection group set

1. Click **Create** on the Tape Optimization Setup dialog box.
2. Enter a unique name to identify the protection group set.
3. Select the protection groups to add to the protection group set.
4. If you do not want protection groups with different retention periods to use the same tape, select **Don't allow backups of different retention periods to co-locate on the same tape**.
5. Click **Advanced** to set Write Period and Expiry Tolerance values.

Modify a protection group set

1. Select the protection group set you want to modify.
2. Click **Modify** on the Tape Optimization Setup dialog box.
3. On the Modify Protection Group screen you can:
   - Edit the name for the protection group set.
   - Add or remove protection groups from the protection group set.
   - Select the checkbox to allow backups of different retention periods to collocate on the same tape.
   - Click **Advanced** to set Write Period and Expiry Tolerance values.

Delete a protection group set

1. Select the protection group set you want to delete.
2. Click **Delete** on the Tape Optimization Setup dialog box.

   Warning
   You cannot delete a protection group set that has protection groups associated with it.

See Also

Tape Optimization Setup - Advanced Options

Tape Optimization Setup - Advanced Options

Write period is the length of time for which a tape is available for writing new backups. The tape is marked as Offsite Ready after this.

Expiration tolerance is the maximum length of time for which an expired recovery point can remain on a tape until the tape is marked as expired.

The following scenarios will explain how you can set these values.

Scenario 1

Protection Groups	Frequency	Retention	Occurs on
1,2,3	1 day	1 week	Daily
1,2,3	1 week	1 month	Every Monday
1,2	1 month	1 year	First of every month

Conditions

- For a given retention range, all backups happen on the same day across the protection groups.
- Tapes are taken out of the library every week.
- Month retention tapes are sent to one physical vault and year retention tapes are taken to another.
- Corporate policy dictates that tapes cannot contain expired datasets (Zero tolerance policy).

Policy/Intent

The administrator sets the following co-location policy:

- Do not co-locate different retention ranges to the same tape.
- Write period should be 1. That is, a tape can be written to only on the day of the first backup to that tape.
- Expiry tolerance is 0.

Tape Usage

- Every day at least one tape will be offsite-ready. The daily backups of protection groups 1, 2, and 3 will be co-located. This tape will expire at midnight of the eighth day.
- Every Monday, all the weekly backups of protection groups 1, 2, and 3 will be co-located. These tapes will be offsite-ready after the last backup is written, and will expire a month later.
- On the first day of every month, all the monthly backups of protection groups 1 and 2 will be co-located. These tapes will be offsite-ready after the last backup is written, and will expire a year later.

Scenario 2

Protection Groups	Frequency	Retention	Occurs on
1	1 day	1 week	Every day
	1 week	1 month	Monday
	1 month	1 year	First of every month
2	1 day	1 week	Every day
	1 week	1 month	Wednesday
	1 month	1 year	Second of every month
3	1 day	1 week	Every day
	1 week	1 month	Friday
	1 month	1 year	NA

Conditions

- For a given retention range (except a week's retention), backups are staggered across days across the protection groups.
- Tapes are taken out of the library every week.
- Month retention tapes are sent to one physical vault and yearly retention tapes are sent to another.
- Corporate policy dictates that tape may contain expired datasets, but for not more than a week (low tolerance policy).

Policy/Intent

- Do not co-locate different retention ranges to the same tape.
- Write period is six days. That is, a tape can be written to until six days after the first backup day.
- Expiry tolerance is six days.

Tape Usage

- Every week at least one tape will be offsite-ready. The daily backups of protection groups 1, 2, and 3 will be co-located on it. This tape will expire at midnight of the fifteenth day.
- Every Monday, Wednesday, and Friday, weekly backups of protection groups 1, 2, and 3 will be co-located. These tapes will be offsite-ready on the Sunday of the week, and will expire a month later.

Scenario 3

Protection Groups	Frequency	Retention	Occurs on
1,2	1 week	2 weeks	Every Saturday
1,2,3	1 month	1 month	Second of every

Protection Groups	Frequency	Retention	Occurs on
			month
1,2,3	1 month	1 year	First of every month

Conditions

- For a given retention range, all backups happen on the same day across the protection groups.
- 1-year retention backups are sent outside the library. There is no need to co-locate them.
- Expired datasets may remain on tapes for up to a month (medium tolerance policy).

Policy/Intent

- Allow the co-location of different retention ranges to the same tape.
- Write period is 13 days. That is, a tape can be written to until 13 days after the first backup day.
- Expiry tolerance is one month.

Tape Usage

Every second week, at least one tape will be offsite-ready. The weekly backups of protection groups 1 and 2 will be co-located on it.

This tape may also have one monthly backup of each protection group.

Setting advanced options for tape optimization

1. Set the write period value.
2. Set the expiry tolerance value.

Appendix A: Quick Reference to DPM Tasks

The following table matches administrative tasks with the object that you select to perform the task.

To perform this task	Select
• Manually synchronize a replica • Perform a manual consistency check on a replica • Manually create a recovery point • Remove a member from a protection group • Delete a replica	The protected data source in the **Protection** task area

To perform this task	Select
• Modify the schedules for synchronization, express full backups, consistency checks, and recovery points • Enable compression • Add a member to a protection group • View a list of tapes • Stop protection of a group	The protection group in the **Protection** task area
• Configure tape catalog retention	Either the protected computer or the protection group in the **Protection** task area
• Modify disk allocation	Either the protected data source or the protection group in the **Protection** task area
• Configure network bandwidth usage throttling • Update, disable, enable, or uninstall a protection agent	The protected computer on the **Agents** tab in the **Management** task area
• Lock or unlock the tape library door • Rescan the tape library	The tape library or stand-alone tape drive on the **Libraries** tab in the **Management** task area
• Clean a tape library drive	The tape drive on the **Libraries** tab in the **Management** task area
• Run a fast or detailed inventory	Any tape library, stand-alone tape drive, drive, slot, or tape on the **Libraries** tab in the **Management** task area
• Erase a tape • Mark a tape as free • Mark a tape as a cleaning tape • View the contents of a tape	A tape on the **Libraries** tab in the **Management** task area

Appendix B: DPM Schema Extension

The DPMADSchemaExtension tool performs the following tasks to support end-user recovery:

- Extends the schema
- Creates a container (MS-ShareMapConfiguration)
- Grants the System Center 2012 – Data Protection Manager (DPM) server permissions to change the contents of the container
- Adds mappings between source shares and shares on the replicas

This appendix describes the classes and attributes that DPM adds to Active Directory to support end-user recovery.

Classes Added by DPM describes the classes that are added to Active Directory when you enable end-user recovery on DPM.

Attributes Added by DPM describes the attributes that are added to Active Directory when you enable end-user recovery on DPM.

Classes Added by DPM

DPM adds one class, **ms-SrvShareMapping**, to the Active Directory directory service when you enable end-user recovery. This class contains the mapping from the protected computer (and share) to the DPM server (and share).

Caution

It is recommended that you do not modify this class.

The following table provides a detailed description of the **ms-SrvShareMapping** class:

Attribute	Value
objectClass	Top
objectClass	classSchema
instanceType	4
possSuperiors	Container
possSuperiors	organizationalUnit
subClassOf	Top
governsID	1.2.840.113556.1.6.33.1.22
mustContain	ms-backupSrvShare
mustContain	ms-productionSrvShare
rDNAttID	Cn
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-SrvShareMapping
lDAPDisplayName	ms-SrvShareMapping
adminDescription	Maps servers with shared resources.
objectClassCategory	1

Attributes Added by DPM

DPM adds two attributes to Active Directory when you enable end-user recovery. The following table lists the added attributes:

Attribute	Description
ms-BackupSrv-Share Attribute	Provides the DPM share name and DPM computer name in a string.
ms-ProductionSrv-Share Attribute	Provides the protected computer share name and protected computer computer name in a string.

ms-BackupSrv-Share Attribute

The following table provides a detailed description of the **ms-BackupSrv-Share** attribute:

Attribute	Value
objectClass	Top
objectClass	attributeSchema
attributeID	1.2.840.113556.1.6.33.2.23
attributeSyntax	2.5.5.12
rangeUpper	260
isSingleValued	TRUE
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-BackupSrv-Share
adminDescription	Identifies a server with shared resources.
oMSyntax	64
IDAPDisplayName	ms-backupSrvShare
objectCategory	CN=Attribute-Schema,<SchemaContainerDN>

ms-ProductionSrv-Share Attribute

The following table provides a detailed description of the **ms-ProductionSrv-Share** attribute:

Attribute	Value
objectClass	Top
objectClass	attributeSchema
attributeID	1.2.840.113556.1.6.33.2.24
attributeSyntax	2.5.5.12
rangeUpper	260
isSingleValued	TRUE
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-ProductionSrv-Share
adminDescription	Identifies a computer with shared resources.
oMSyntax	64
IDAPDisplayName	ms-productionSrvShare
objectCategory	CN=Attribute-Schema,<SchemaContainerDN>

Appendix C: Custom Report Views

System Center 2012 – Data Protection Manager (DPM) includes several SQL views to help you create custom reports.

SQL views simplify your queries by populating columns with data collected from multiple tables in the database. These views offer several advantages over querying the tables directly:

- You do not need in-depth knowledge of the entire database or the relationship between tables and keys.
- If the database structure changes in future versions of the product, the views can be updated so that they behave the same.

For DPM installations that use a separate, dedicated computer for the SQL Server database, the views are queried on the database computer, not the computer running DPM. This results in less competition for resources when large numbers of views are queried over a short period of time.

The potential disadvantages of the SQL views include the following:

- Because the view runs each time it is queried, server performance may be degraded if the view is used too frequently.
- The available supported views might not include all of the columns you need.

This appendix lists the views available in DPM.

Vw_DPM_Agents: Contains the list of computers on which a DPM protection agent from this DPM server has been installed.

Field	Data type	Description
ServerName	String	The name of the computer
Version	String	The version of the DPM agent on that computer

Vw_DPM_Alerts: List of all alerts from the last 30 days.

Field	Data type	Description
Severity	Integer 0=Error 1=Warning 2=Information	The severity level of the alert
Resolution	Integer 0 = Active 1 = Recommended action in progress 2 = Resolved	The state of the alert
OccurredSince	Date and time	The first time this alert was raised
ResolvedTime	Date and tiime	The time at which the alert was resolved
Type	Integer See "Alert Types" in this appendix	The type of the alert

Vw_DPM_CurrentOnlineMedia: The tapes that are online in DPM owned libraries currently, as of the last inventory.

Field	Data type	Description
UserFriendlyName	String	The name of the library
ImportPoolMediaCount	Integer	Tapes imported to this DPM server
FreePoolMediaCount	Integer	Tapes marked as free or blank

Field	Data type	Description
AdminPoolMediaCount	Integer	Tapes with active data. Expired tapes change to free when the tape is marked free or the protection group is deleted.

Vw_DPM_Disk_Usage_Replica: Disk usage statistics for replicas in the storage pool.

Field	Data type	Description
PhysicalPath	String	The name of the protected data source
ReplicaId	GUID	Unique identifier for the replica on DPM disks
PGId	GUID	Unique identifier for the protection group to which this data source belongs
ProductionServerName	String	The name of the server on which the data source exists
DiskAllocated	Big integer	Total disk space allocated to this data source
DiskUsed	Big integer	Total disk space used by this data source
FreeSpace	Big integer	DiskAllocated – DiskUsed
ReplicaAllocated	Big integer	The part of DiskAllocated that is reserved for the replica of the data source
ReplicaUsed	Big integer	The part of ReplicaAllocated that is actually in use
ShadowCopyAllocated	Big integer	The part of DiskAllocated that is reserved for the recovery points of the data source
ShadowCopyUsed	Big integer	The part of ShadowCopyAllocated that is actually in use
StartDateTime	Date and time	The time this statistic was

Field	Data type	Description
		collected
EndDateTime	Date and time	Internal field
ScheduleType	Integer 0=Weekly 1=Monthly 2=Quarterly 3=Yearly	The schedule period which this data represents

Vw_DPM_DiskRecoveryPoints: Counts for disk recovery points available for each data source.

Field	Data type	Description
DataSourceName	String	The name of the protected data source
PGId	GUID	The unique identifierentifier for the protection group to which this data source belongs
ServerId	GUID	The unique identifierentifier for the server to which this data source belongs
Frequency	Integer	The number of available recovery points

Vw_DPM_LongRecoveries: Provides historical information about recoveries that took longer than 24 hours.

Field	Data type	Description
DataSourceName	String	The data source that was recovered
TargetServerName	String	The name of the server to which recovery was done
WriterId	GUID	Identifies the type of the data source that was recovered
StartTime	Date and time	The time at which the recovery was started

Field	Data type	Description
EndTime	Date and time	The time at which the recovery ended
RecoverySize	Big integer	The size of the data recovered by the job
RecoverySource	Integer 0=Disk 1=Tape	The recovery source

Vw_DPM_Media: Provides information about state of all tapes known to DPM.

Field	Data type	Description
MediaLabel	String	The label on the tape
MediaBarcode	String	The barcode for the tape
IsOnline	Integer	Whether the tape is online
LibraryName	String	The name of the library in which the tape exists. NULL if tape is offline
MediaSlotNumber	Integer	The slot number in which the tape exists. NULL if tape is offline If in a drive, this represents the home slot of the tape (to which the tape returns on a dismount).
PGName	String	The name of the protection group in which the tape exists
MediaExpiryDate	Date and time	The time when all data sets on this tape will expire. Can have the date in the past or NULL if the tape is free.

Vw_DPM_MediaPool_Media: Tape counts for a given library.

Field	Data type	Description
LibraryName	String	The name of the library
FreeMedia	Integer	Number of tapes that are free in this library
FreeMediaThreshold	Integer	The threshold below which this library generates an alert

Vw_DPM_ProtectedDataSource: Current disk space usage by various data sources.

Field	Data type	Description
ReplicaId	GUID	Identifier of the replica
PGId	GUID	Identifier of the protection group to which the replica belongs
AllocatedSize	Big integer	Disk space allocated to the data source
UsedSize	Big integer	Disk space currently used by the data source
ProductionServerName	String	The name of the computer on which the data source exists
StorageNode	String	Always set to the DPM server

Vw_DPM_ProtectedGroup: Table with information about all protection groups.

Field	Data type	Description
PGId	GUID	Unique identifierentifier for the protection group
ProtectionGroupName	String	Name of the protection group
CreationTime	Date and time	The time at which the protection group was created

Vw_DPM_RecoveryDuration: History of counts for recovery jobs in various time durations.

Field	Data type	Description
StartDateTime	Date and time	The time at which the statistic

Field	Data type	Description
		was collected
EndDateTime	Date and time	Internal
ScheduleType	Integer	The frequency for which this particular statistic was collected
RecoveryDuration	Integer	Indicates if the recovery was less than 6 hours, between 6-24 hours, or greater than 24 hours
RecoveryCount	Integer	Number of recoveries

Vw_DPM_RecoveryJob: Detailed information about recent recovery jobs.

Field	Data type	Description
DataSourceName	String	The data source for which recovery was run
ServerName	String	The server to which recovery was performed
CreationTime	Date and time	Time at which the recovery job was run
FailureCode	Integer	Error code in case of failure of the recovery job
Status	Integer 0/1=Progress 2=Succeeded 3=Failure	Status of the recovery job

Vw_DPM_RecoveryPointDisk: Status of recent recovery point creation jobs on disk.

Field	Data type	Description
DataSourceName	String	The data source for which the backup was created
ServerName	String	The server on which the data source exists

Field	Data type	Description
CreationTime	Date and time	The time at which the recovery point creation job was run
Status	Integer 0/1=Progress 2=Succeeded 3=Failure	Status of the recovery point creation job
ErrorCode	Integer	Zero if succeeded. Else, set to a DPM error code.

Vw_DPM_RecoveryPointTape: Status of recent recovery point creation jobs on tape.

Field	Data type	Description
DataSourceName	String	The data source for which the backup was created
ServerName	String	The server on which the data source exists
CreationTime	Date and time	The time at which the recovery point creation job was run
Status	Integer 0/1=Progress 2=Succeeded 3=Failure	Status of the recovery point creation job
ErrorCode	Integer	Zero if succeeded. Else, set to a DPM error code.

Vw_DPM_Replica: Listing of all replicas managed by DPM.

Field	Data type	Description
ReplicaId	GUID	Unique identifierentifier generated by DPM for the replica volume

Field	Data type	Description
PhysicalPath	String	The name of the data source on the replica
ServerName	String	Name of the server to which the data source belongs
ValidFrom	Date and time	When the replica was created
ValidTo	Date and time	The date on which the replica was made inactive
PGId	GUID	Unique identifierentifier generated by DPM for the protection group to which the data source belongs
StorageNode	String	Always set to the DPM server

Vw_DPM_Server: List of all protected computers.

Field	Data type	Description
ServerId	GUID	Unique identifierentifier generated by DPM for the protected computer
ServerName	String	Fully qualified domain name for the computer
NetBiosName	String	Name
DomainName	String	Domain in which the computer belongs
IsRG	Integer	If this computer represents a Resource Group

Vw_DPM_TapeRecoveryPoints: Counts for tape recovery points available for each data source.

Field	Data type	Description
DataSourceName	String	The name of the protected data source
PGId	GUID	The unique identifierentifier for the protection group to which

Field	Data type	Description
		this data source belongs
ServerId	GUID	The unique identifierentifier for the server to which this data source belongs
Frequency	Integer	The number of available recovery points
Term	Integer 0=ShortTerm 1=LongTerm	The schedule to which this recovery point corresponds

Vw_DPM_TapeStat: Historical information on tape usage counts.

Field	Data type	Description
StartDateTime	Date and time	
EndDateTime	Date and time	
ScheduleType	Integer	Integer 0=Weekly 1=Monthly 2=Quarterly 3=Yearly
Free	Integer	Number of free tapes at end-time
Online	Integer	Number of online tapes at end time

Vw_DPM_TapeUsagePerPG: Historical tape usage data per protection group.

Field	Data type	Description
StartDateTime	Date and time	Start time
EndDateTime	Date and time	End time
PGName	String	Name of the protection group
ScheduleType	Integer	Integer 0=Weekly

Field	Data type	Description
		1=Monthly 2=Quarterly 3=Yearly
Online	Integer	Number of online tapes at end time
Offline	Integer	Number of offline tapes at end time

Vw_DPM_Total_Disk_Trend: Total disk space usage historical trend.

Field	Data type	Description
StartDateTime	Date and time	
EndDateTime	Date and time	
ScheduleType	Integer	Integer 0=Weekly 1=Monthly 2=Quarterly 3=Yearly
DiskSpaceCapacity	Big integer	The total storage in storage pool at end-time
PreviousDiskSpaceCapacity	Big integer	Total storage in storage pool in previous corresponding period
DiskSpaceAllocated	Big integer	The disk space from storage pool that has been allocated
PreviousDiskSpaceAllocated	Big integer	The disk space from storage pool that was allocated in the previous corresponding period
DiskSpaceUsed	Big integer	The actual disk space usage
PreviousDiskSpaceUsed	Big integer	The used disk space in the previous corresponding period

Vw_DPM_Total_RecoveryPoint: Information about all recent recovery point jobs.

Field	Data type	Description
DataSourceName	String	The name of the protected data source
ServerName	String	The server to which the data source belongs
CreationTime	Date and time	The time at which the recovery point creation job was run
Status	Integer 0/1=Progress 2=Succeeded 3=Failure	Status of the recovery point creation job
ErrorCode	Integer	Error code in recovery point creation

Alert Types

-1	RestoreDBAlert
0	NullType
1	AgentIncompatibleAlert
2	AgentUnreachableAlert
5	MediaVerificationFailedAlert
6	MediaEraseFailedAlert
7	DetailedInventoryFailedAlert
8	MediaDecommissionedAlert
9	MediaDataEraseAlert
10	FreeMediaThresholdAlert
11	DataSetCopyFailedAlert
12	BackupToTapeFailedAlert
13	BackupToTapeCatalogFailedAlert

14	LibraryDriveAlert
15	LibraryNotAvailableAlert
16	LibraryNotWorkingEfficientlyAlert
17	MediaRequiredAlert
18	ReplicaInitializationInProgressAlert
19	SynchronizationFailedAlert
20	StopProtectionFailedAlert
21	RecoveryInProgressAlert
22	RecoveryPartiallySuccessfulAlert
23	RecoverySuccessfulAlert
24	RecoveryFailedAlert
25	ShadowCopyFailedAlert
26	ReplicaInMissingStateAlert
27	ReplicaInInvalidStateAlert
28	PartialDeployedClusterAlert
29	AgentTaskFailAlert
30	SqmOptInAlert
31	DiskThresholdCrossedAlert
32	VerificationInProgressAlert
33	DiskMissingAlert
34	CatalogThresholdCrossedAlert
35	DatasetDataVerificationFailed
36	SCDiskThresholdCrossedAlert
37	ConfigureProtectionFailedAlert
38	ReplicaManualLoadPendingAlert
39	ReplicaInitializationPendingAlert
40	CertificateExpiringAlert
41	EvalShareInquiryAlert
42	ShadowCopyConsolidationRequired

Appendix E: Windows Server Logo Certification

This topic provides details about the System Center 2012 – Data Protection Manager (DPM) certification for the Windows Server logo program.

Custom Actions

For a list of custom actions that are checked during DPM Setup, see DPM Setup Custom Action Details. These checks are part of the System Center 2012 – Data Protection Manager (DPM) certification for the Windows Server logo program.

The following table lists the custom actions that are performed for the DPM installation files.

<table>
<tr><th>File</th><th>Custom Action</th></tr>
<tr><td>DPMCentralConsoleServer.msi</td><td>
<table>
<tr><th>Action</th><th>Type</th><th>Description</th></tr>
<tr><td>_SetGroupNameProperties</td><td>1</td><td>Sets local group properties. This is required for localization</td></tr>
<tr><td>SchedServiceConfig</td><td>1</td><td></td></tr>
<tr><td>_RunConfigureFirewallforTokenService</td><td>1025</td><td>Adds firewall exception for 6075 port for token service.</td></tr>
<tr><td>_UnConfigureFirewallforTokenService</td><td>1089</td><td>Removes firewall exception for 6075 port for token service.</td></tr>
<tr><td>_RunConfigureFirewallforTokenServiceRollback</td><td>1345</td><td>Removes firewall exception for 6075 port for token service as part of rollback, in case installation</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>File</th><th>Custom Action</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td>fails.</td></tr>
<tr><td>ExecServiceConfig</td><td>3073</td><td></td></tr>
<tr><td>RollbackServiceConfig</td><td>3329</td><td></td></tr>
</table>
</td></tr>
<tr><td>dpmui.msi</td><td>
<table>
<tr><th>Action</th><th>Type</th><th>Description</th></tr>
<tr><td>_DetectMonad</td><td>1</td><td>Checks if PowerShell is installed.</td></tr>
<tr><td>_DetectR2</td><td>1</td><td>Checks if operating system version is later than Windows 2003 SP2</td></tr>
<tr><td>_SetAllGroupNameProperties</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
<tr><td>_SetAllGroupNameProperties.9D6B8595_5D05_4871_B36A_08D2B42397C0</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
<tr><td>_DeleteMMCSnapinRegKeys</td><td>1089</td><td>Deletes MMC snap-in registry keys</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>File</th><th>Custom Action</th></tr>
<tr><td></td><td>
<table>
<tr><td>_DeletePowershellSnapinRegKeys</td><td>1089</td><td>Deletes PowerShell snap-in registry keys</td></tr>
<tr><td>_ChangePowershellExecutionPolicy.9D6B8595_5D05_4871_B36A_08D2B42397C0</td><td>1105</td><td>Sets PowerShell execution policy to RemoteSigned if it is Restricted or AllSigned</td></tr>
</table>
</td></tr>
<tr><td>dpmV3ui.msi</td><td>
<table>
<tr><th>Action</th><th>Type</th><th>Description</th></tr>
<tr><td>_DetectMonad</td><td>1</td><td>Checks if PowerShell installed.</td></tr>
<tr><td>_DetectR2</td><td>1</td><td>Checks if operating system version is later than Windows 2003 SP2</td></tr>
<tr><td>_SetAllGroupNameProperties</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
<tr><td>_SetAllGroupNameProperties.30D31365_1674_4E38_816E_F39B82AAABBB</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
<tr><td>_DeleteMMCSnapinRegKeys</td><td>1089</td><td>Delete MMC snap-in registry keys</td></tr>
<tr><td>_DeletePowershellSnapinRegKeys</td><td>1089</td><td>Delete PowerShell snap-in registry keys</td></tr>
<tr><td>_ChangePowershellExecutionPolicy.</td><td>1105</td><td>Sets PowerShell</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>File</th><th>Custom Action</th></tr>
<tr><td></td><td>
<table>
<tr><td>30D31365_1674_4E38_816E_F39B82AAABBB</td><td></td><td>execution policy to RemoteSigned if it is Restricted or AllSigned</td></tr>
</table>
</td></tr>
<tr><td>msdpm.msi</td><td>
<table>
<tr><th>Action</th><th>Type</th><th>Description</th></tr>
<tr><td>_PreserveRegistrySettings</td><td>1</td><td>Preserves registry settings during upgrade</td></tr>
<tr><td>FirstRun</td><td>1</td><td></td></tr>
<tr><td>_DisableCPWrapperServices.88BD42D4_8EBE_4E98_B407_81775C1F7E9C</td><td>1</td><td>Disables CPWrapper service during upgrade</td></tr>
<tr><td>_SetAllGroupNameProperties.9D6B8595_5D05_4871_B36A_08D2B42397C0</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
<tr><td>_CheckUSNRebootRequied.88BD42D4_8EBE_4E98_B407_81775C1F7E9C</td><td>17</td><td>Checks the DEFFERRED_CA_REQUIRES_REBOOT in Global Atom table and schedules a reboot if required</td></tr>
<tr><td>_DelMSDPMTrustedMachinesGroup.5064F488_BAD3_B02C_1DD0_6323356F38C0</td><td>65</td><td>Deletes MSDPMTrustedMachine group</td></tr>
<tr><td>_DelDPMDRTrustedMachinesGroup.5064F488_BAD3_B02C_1DD0_6323356F38C0</td><td>65</td><td>Deletes DPMDRTrustedMachine group</td></tr>
<tr><td>_DeleteUSNKeys.88BD42D4_8EBE_4E98_B407_81775C1F7E9C</td><td>81</td><td>Deletes USN registry keys</td></tr>
<tr><td>_UninstallationActionForNonAd.88BD42D4_8EBE</td><td>81</td><td>Purges all non-</td></tr>
</table>
</td></tr>
</table>

File	Custom Action		
	_4E98_B407_81775C1F7E9C		active-directory user accounts
	_DeleteDPMRAService.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	81	Deletes DPMRA service
	_InstallDPMStores	1025	Creates system store for DPM backup and restore
	_AddUsersPermissionToMsdpmDirs	1025	Adds user permission To MSDPM folders during upgrade
	_UpdateMaxSizeDpmAlertsRegKey	1025	Increases the maximum size registry key for DPM alerts
	_AddMSDPMTrustedMachinesGroup.5064F488_BAD3_B02C_1DD0_6323356F38C0	1025	Adds MSDPMTrustedMachine group
	_AddDPMDRTrustedMachinesGroup.5064F488_BAD3_B02C_1DD0_6323356F38C0	1025	Adds DPMDRTrustedMachine group
	_AclMsdpmExeForMSDPMTrustedMachines.5064F488_BAD3_B02C_1DD0_6323356F38C0	1025	Adds permissions for MSDPMTrusted machines group on MSDPM exe
	_InstallDLSACConfig.30209D72_E634_4A82_BCDD_26A22DBF0A15	1025	Installs DLSAC Config
	_CreateDPMRAService.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Creates DPMRA service
	_DoMachineIndependentDPMConfiguration.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Cleans DCOM launch and activates permissions for previous server. Ignore if this fails since cleaning is best effort.

File	Custom Action		
	_CreateMTAShare.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Creates MTA share
	_DoMachineSpecificDPMConfiguration.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Configures DCOM and firewall for a given server
	_CreateSystemStateRegKeyForLongHornServer.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Creates SystemState registry key for Windows 2008 Server
	_AddAclToMTATempStorePath.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Gives DPMRATrustedMachines group read-write access on the MTATempStorePath
	_ReconfigureCertificatesPostUpgradeIfNeeded.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Configures certificates after an upgrade
	_AddDCOMLaunchPermissionsForCmdlets.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Adds DCOM launch permissions for cmdlets
	_UpdatePSDataSourceConfigXML.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Updates the XML during upgrade if there are changes in Config.XML
	_ConfigureDCInUpgrade.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Adds config element for RA agent to DLSConfig authorization XML file
	_UpgradeForRADCOMGroup.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1041	Upgrade for RA DCOMGroup
	_IncreaseIRPStackSize.C68D0BFC_654C_4ECF_B861_D846DC06E64D	1041	Increases IRPStackSize
	_InstallDpmFilterDriver.C68D0BFC_654C_4ECF_B861_D846DC06E64D	1041	Installs DPM filter driver

File	Custom Action		
	_AddLibraryAgentConfiguration.EDC48038_97FD_470D_AC87_7437E289FA5D	1041	Add LibraryAgent configuration
	_AddLibraryAuthorizedMachine.EDC48038_97FD_470D_AC87_7437E289FA5D	1041	Add LibraryAuthorized machine
	_DisableRSMService.EDC48038_97FD_470D_AC87_7437E289FA5D	1041	Disable RSMService
	_UninstallDPMStores	1089	Deletes system store for DPM backup and restore
	_UninstallACConfig.A97E7F08_AB47_4A39_B1A5_1EE76BB9B9C3	1089	Uninstall AC configuration
	_UninstallConfig.A97E7F08_AB47_4A39_B1A5_1EE76BB9B9C3	1089	Delete configuration
	_UninstallConfigRoot.A97E7F08_AB47_4A39_B1A5_1EE76BB9B9C3	1089	Uninstall Config root
	_UninstallACAppID.A97E7F08_AB47_4A39_B1A5_1EE76BB9B9C3	1089	Uninstall AC AppID
	_DeleteLocalGroup.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Delete local group
	_DeleteMTAShare.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Delete MTAShare
	_DeleteActiveOwnerDir.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Delete ActiveOwner directory
	_UnregisterDPMRADistributedCOMUser.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Unregister DPMRA DCOM user
	_DeleteDPMRAConfiguration.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Delete DPMRA configuration
	_CreateUSNKeys.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Create USN registry keys
	_DeleteDPMRAAppID.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1105	Delete DPMRA AppID
	_UninstallDpmFilterDriver.C68D0BFC_654C_4ECF_B861_D846DC06E64D	1105	Uninstall DpmFilter driver

File	Custom Action		
	_DeleteLibraryAgentConfiguration.EDC48038_97FD_470D_AC87_7437E289FA5D	1105	Delete LibraryAgent configuration
	_DeleteDPMLAService.EDC48038_97FD_470D_AC87_7437E289FA5D	1105	Delete DPMLAService
	_ChangePowershellExecutionPolicy.9D6B8595_5D05_4871_B36A_08D2B42397C0	1105	Sets PowerShell execution policy to RemoteSigned if it is Restricted or AllSigned
	_UninstallDPMStoresRollback	1345	Deletes DPM stores as rollback action if installer fails
	_Rollback_InstallDLSACConfig.30209D72_E634_4A82_BCDD_26A22DBF0A15	1345	Rolls back CustomAction for InstallDLSACConfig
	_CreateDPMRAServiceRollback.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1361	Rolls back CustomAction for CreateDPMRAService
	_RollbackMachineIndependentDPMConfiguration.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1361	Rolls back CustomAction for MachineIndependentDPMConfiguration
	_CreateMTAShareRollback.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1361	Rolls back CustomAction for CreateMTAShare
	_RollbackAddRADlsTrustedGroupForDCInUpgrade.88BD42D4_8EBE_4E98_B407_81775C1F7E9C	1361	Rolls back CustomAction for AddRADlsTrustedGroupForDCInUpgrade
	_RollbackDpmFilterDriverUninstall.C68D0BFC_654C_4ECF_B861_D846DC06E64D	1361	Rolls back CustomAction for DpmFilterDriverUninstall
	_RollbackDpmFilterDriver.C68D0BFC_654C_4ECF_B861_D846DC06E64D	1361	Rolls back CustomAction for

<table>
<tr><th>File</th><th>Custom Action</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td>DpmFilterDriver</td></tr>
<tr><td>_DeleteLibraryAgentConfigurationRollback.EDC48038_97FD_470D_AC87_7437E289FA5D</td><td>1361</td><td>Rolls back CustomAction for DeleteLibraryAgentConfiguration</td></tr>
</table>
</td></tr>
<tr><td>DPMSQLEur_x64.msi</td><td>
<table>
<tr><th>Action</th><th>Type</th><th>Description</th></tr>
<tr><td>_SetGroupNameProperties</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
</table>
</td></tr>
<tr><td>DPMSQLEur_x86.msi</td><td>
<table>
<tr><th>Action</th><th>Type</th><th>Description</th></tr>
<tr><td>_SetGroupNameProperties</td><td>1</td><td>Sets local group properties. This is required for localization.</td></tr>
</table>
</td></tr>
</table>

Third party binaries

Test Case 2.1.2

The following is a list of third-party binaries installed by DPM that show an ICE27 error.

\Redist\DotNetFrameworks\dotNetFX30\Netfx30a_x64.msi

\Redist\DotNetFrameworks\dotNetFX30\Netfx30a_x86.msi

\Redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x64.msi

\Redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x86.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\Netfx30a_x64.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\Netfx30a_x86.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x64.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x86.msi

Test Case: 2.8.2

The following is a list of third-party binaries installed by DPM that do not have publisher information for the Windows Server logo program.

c:\Program Files\Common Files\Microsoft Shared\DW\DWDCW20.dll

c:\Program Files\Microsoft DPM\DPM\Setup\PidGen.dll

c:\Program Files\Microsoft DPM\SQL\90\DTS\Binn\Microsoft.SqlServer.ForEachFileEnumeratorWrap.dll

c:\Program Files\Microsoft DPM\SQL\90\DTS\Binn\Microsoft.SQLServer.msxml6_interop.dll

c:\Program Files\Microsoft DPM\SQL\90\DTS\Binn\Microsoft.SqlServer.SQLTaskConnectionsWrap.dll

c:\Program Files\Microsoft DPM\SQL\MSSQL.1\MSSQL\Binn\sqlmap90.dll

c:\Program Files\Microsoft SQL Server\90\Shared\sqlwvss_xp.dll

c:\Program Files (x86)\Common Files\Microsoft Shared\MSDesigners8\msddsp.dll

c:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE11\UCS20.DLL

c:\Program Files (x86)\Microsoft DPM\SQL\90\DTS\Binn\interop.msdasc.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\DTS\Binn\Microsoft.SqlServer.ForEachFileEnumeratorWrap.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\DTS\Binn\Microsoft.SqlServer.SQLTaskConnectionsWrap.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\DdsShapesLib.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\Interop.DPDPL_7_0.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\Interop.MergeModule_2_0.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\interop.msdasc.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\Interop.MSI_2_0.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\Interop.SHDocVw.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\Interop.Vdt70.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\Interop.VisioGraph_2_100.dll

c:\Program Files (x86)\Microsoft DPM\SQL\90\Tools\Binn\VSShell\Common7\IDE\sqlresolver.dll

c:\Program Files (x86)\Microsoft Office\OFFICE11\UCSCRIBE.dll

C:\Program Files\Microsoft SQL Server\MSRS10_50.MSSQLSERVER\Reporting services\RSTempFiles\reportserver\b030430a\dcad33e5\App_global.asax.anwora4x.dll

C:\ProgramFiles Folder\Microsoft System Center 2012\DPM\DPM\ProtectionAgents\AC\<build number>\amd64\msvcr80.dll

C:\ProgramFiles Folder\Microsoft System Center 2012\DPM\DPM\ProtectionAgents\AC\<build number>\i386\msvcr80.dll

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX20\Netfx20a_x64.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX20\Netfx20a_x86.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX20\Netfx20a_x64.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX20\Netfx20a_x86.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX30\Netfx30a_x64.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX30\Netfx30a_x86.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x64.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x86.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX30\x64\msxml6.msi

\DPM2012_BUILD\Redist\DotNetFrameworks\dotNetFX30\x86\msxml6.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\redist\RemoteBlobStore\RBS.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\redist\Upgrade Advisor\SqlUA.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\MasterDataServices.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\OWC11.MSI

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\rsSharePoint.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sqlbrowser.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\SQLServerBestPracticesPolicies.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\SQLServerBOL.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_as_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_bids_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_is_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_rs_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_ssms_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_tools_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\SSCERuntime.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\SSCESqlWbTools.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\StreamInsight.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\StreamInsightClient.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\Synchronization.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\SyncServicesADO.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\vs_shell.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql2008support\sqlsupport.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sqlsupport_msi\SqlSupport.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_common_core_loc_msi\sql_common_core_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_engine_core_inst_loc_msi\sql_engine_core_inst_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_engine_core_shared_loc_msi\sql_engine_core_shared_loc.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\x64\msxml6.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\x64\sqlncli.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\x64\SQLServer2005_BC.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\x64\SQLSysClrTypes.msi

\DPM2012_BUILD\SQLSVR2008R2\1033_ENU_LP\x64\Setup\x64\SqlWriter.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX20\Netfx20a_x64.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX20\Netfx20a_x86.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\Netfx30a_x64.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\Netfx30a_x86.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x64.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x86.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\x64\msxml6.msi

\DPM2012_BUILD\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\x86\msxml6.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\redist\watson\dw20sharedamd64.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\rsfx.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sqlsqm.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_as.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_as_spi.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_bids.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_fulltext.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_is.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_rs.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_ssms.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_tools.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\trin_aide.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\msreportviewer90sp1\vb_ros.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_common_core_msi\sql_common_core.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_engine_core_inst_msi\sql_engine_core_inst.msi

\DPM2012_BUILD\SQLSVR2008R2\x64\Setup\sql_engine_core_shared_msi\sql_engine_core_shared.msi

Test Case 2.10.1

The following is a list of third-party binaries installed by DPM that may miss the Upgrade table.

\DPM2012\setup\redist\dw20sharedamd64.msi

\Redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x64.msi

\Redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x86.msi

\SQLSVR2008R2\1033_ENU_LP\x64\redist\RemoteBlobStore\RBS.msi

\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_as_loc.msi

\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_rs_loc.msi

\SQLSVR2008R2\1033_ENU_LP\x64\Setup\sql_engine_core_inst_loc_msi\sql_engine_core_inst_loc.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x64.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX30\RGB9RAST_x86.msi

\SQLSVR2008R2\x64\redist\watson\dw20sharedamd64.msi

\SQLSVR2008R2\x64\Setup\sql_as.msi

\SQLSVR2008R2\x64\Setup\sql_fulltext.msi

\SQLSVR2008R2\x64\Setup\sql_rs.msi

\SQLSVR2008R2\x64\Setup\sql_engine_core_inst_msi\sql_engine_core_inst.msi

\SQLSVR2008R2\1033_ENU_LP\x64\Setup\OWC11.MSI

Test Case 2.11.3

The following is a list of third-party binaries installed by DPM that have custom columns.

\Redist\DotNetFrameworks\dotNetFX20\Netfx20a_x64.msi

\Redist\DotNetFrameworks\dotNetFX20\Netfx20a_x86.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX20\Netfx20a_x64.msi

\SQLSVR2008R2\redist\DotNetFrameworks\dotNetFX20\Netfx20a_x86.msi

Test Case 3.1.1

The following third-party redistributables require higher privileges during installation. These are part of the DPM agent installation prerequisites and require administrator privileges.

<Install location>\DPM\ProtectionAgents\AC\<build number>\amd64\vcredist_x64.exe

<Install location>\DPM\ProtectionAgents\AC\<build number>\i386\vcredist_x86.exe

The following redistributables are third-party software and do not have manifests.

<Install location>\DPM\ProtectionAgents\AC\<build number>\amd64\vcredist.exe

<Install location>\DPM\ProtectionAgents\AC\<build number>\amd64\WindowsServer2003-KB975759-v2-x64-ENU.exe

<Install location>\DPM\ProtectionAgents\AC\<build number>\i386\vcredist.exe

<Install location>\DPM\ProtectionAgents\AC\<build number>\i386\WindowsServer2003-KB975759-v2-x86-ENU.exe

Appendix F: Tested hardware VSS providers

This table lists Volume Shadow Copy Service (VSS) hardware providers that have been tested to be compatible with System Center 2012 – Data Protection Manager (DPM) for protecting virtual machines deployed on clustered shared volumes (CSV). If a VSS hardware provider is not listed, it has not been tested.

Model	Firmware version	VSS hardware provider version	Download location	Remarks
IBM				
DS6000 DS8000	6000= 6.2.2.108 8000= 64.30.x.x	4.0.1.1020	Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service	The same VSS provider is used for SVC, DS6k, and DS8k
IBM XIV Storage	10.1.0.a	IBM XIV xProv Version: 2.2.2	Download xProvSetup-x64-2.2.2	
NEC				
iStorage D series		2.1.1 (x64)	iStorage VSS	The following software is

Model	Firmware version	VSS hardware provider version	Download location	Remarks
(D1-30)			Provider	needed in order to take snapshot in the iStorage D series: • iStorage basic software: iStorage Manager; iStorage Access Control is included. • WebSAM RepNavi Suite: iStorage Dynamic Data Replication Lite, iStorage Control Command, iStorage VSS Provider. • iStorage Storage Path Savior: Software to control disk array path load.
EMC				
Symmetrix series		4.2.1	EMC	
Clarion series		4.2.1	EMC	
Hitachi				
Adaptable Modular Storage 2000 family: AMS2100,		v03.5.0 and above	Optimize Microsoft environments with	

Model	Firmware version	VSS hardware provider version	Download location	Remarks
AMS2300, AMS2500			proven Hitachi solutions	
Compellent				
Compellent Storage center 4.2 and above		05.00.01.004	Distributed as part of the Replay Manager product (separate purchase required).	
Dell				
EqualLogic PS series	4.2.1 or later	3.3.1 or later	Downloads	
HP				
EVA 4x00, 6x00, 8x00	XCS 09006000	6.05	Storage Integration Utility Software	
NetApp				
FAS2000 Series FAS3000 Series FAS3100 Series FAS6000 Series V3100 Series V3100 Series V6000 Series	Data ONTAP 7.3.0 or above	6.2.0.4508 or above	Support	
Fujitsu				
ETERNUS DX storage systems ETERNUS2000 (model 100 or higher) ETERNUS4000 (model 300 or higher) ETERNUS8000		1.5.0 or later	ETERNUS VSS Hardware Provider	

Privacy Statement for System Center 2012 - Data Protection Manager

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power, and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of System Center 2012 – Data Protection Manager (DPM).

System Center 2012 – Data Protection Manager (DPM) is a server software application that enables disk and tape based data protection for servers and clients.

As the standard for Windows backup and recovery, DPM offers near continuous data protection for Microsoft application and file servers using seamlessly integrated disk and tape media.

DPM performs replication, synchronization, and recovery point creation to provide reliable protection and rapid recovery of data by both system administrators and end users.

Collection and Use of Your Information

The information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to enable the features you are using and provide the service(s) or carry out the transaction(s) you have requested or authorized. It may also be used to analyze and improve Microsoft products and services.

We may send certain mandatory service communications such as welcome letters, billing reminders, information on technical service issues, and security announcements. Some Microsoft services may send periodic member letters that are considered part of the service. We may occasionally request your feedback, invite you to participate in surveys, or send you promotional mailings to inform you of other products or services available from Microsoft and its affiliates.

In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services. We may also supplement the information we collect with information obtained from other companies. For example, we may use services from other companies that enable us to derive a general geographic area based on your IP address in order to customize certain services to your geographic area.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as packaging, sending and delivering purchases and other mailings, answering customer questions about products or services, processing event registration, or performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public.

Information that is collected by or sent to Microsoft by DPM may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union.

Collection and Use of Information about Your Computer

When you use software with Internet-enabled features, information about your computer ("standard computer information") is sent to the Web sites you visit and online services you use. Microsoft uses standard computer information to provide you Internet-enabled services, to help improve our products and services, and for statistical analysis. Standard computer information typically includes information such as your IP address, operating system version, browser version, and regional and language settings. In some cases, standard computer information may also include hardware ID, which indicates the device manufacturer, device name, and version. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each DPM feature, software or service listed in this privacy statement describe what additional information is collected and how it is used.

Security of your information

Microsoft is committed to helping protect the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities.

Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products, services, and customer feedback. When we post changes, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

For More Information

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement or believe that we have not adhered to it, please contact us here:

Microsoft Privacy

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Or Email Us

Specific features

The remainder of this document will address the following specific features:

Customer Experience Improvement Program

What This Feature Does:

The Customer Experience Improvement Program (“CEIP”) collects basic information about your hardware configuration and how you use our software and services in order to identify trends and usage patterns. CEIP also collects the type and number of errors you encounter, software and hardware performance, and the speed of services. We will not collect your name, address, or other contact information.

Information Collected, Processed, or Transmitted:

For more information about the information collected, processed, or transmitted by CEIP, see the CEIP privacy statement at http://www.microsoft.com/products/ceip/EN-US/privacypolicy.mspx.

Use of Information:

We use this information to improve the quality, reliability, and performance of Microsoft software and services.

To turn CEIP on or off in the DPM user interface select the “Action” menu item, then click “Options…”. Go to the “Customer Feedback” tab and select “Yes” or “No” to turn on or off.

Windows Azure Online Backup

What This Feature Does:

This feature enables you to backup data from your DPM server onto Windows Azure by using the Windows Azure Online Backup service.

Information Collected, Processed, or Transmitted:

For more information about the information collected, processed, or transmitted to Windows Azure Online Backup, see the Windows Azure Online Backup privacy statement at http://go.microsoft.com/fwlink/p/?LinkID=221308.

Use of Information:

The information collected by this service is used to provide you with online backup for DPM data. If you do not wish to use this feature, do not sign up for this service.

Microsoft Error Reporting

What This Feature Does:

Microsoft Error Reporting provides a service that allows you to report problems you may be having with DPM to Microsoft and to receive information that may help you avoid or solve such problems.

Information Collected, Processed, or Transmitted:

For information about the information collected, processed, or transmitted by Microsoft Error Reporting, see the Microsoft Error Reporting privacy statement at http://oca.microsoft.com/en/dcp20.asp.

Use of Information:

We use the error reporting data to solve customer problems and improve our software and services.

Choice/Control:

Microsoft Error Reporting for DPM is a per instance choice. With each error report instance, the user is given a choice to send or not send the information collected to

Important
Enterprise customers can use Group Policy to configure how Microsoft Error Reporting behaves on their computers. Configuration options include the ability to turn off Microsoft Error Reporting. If you are an administrator and wish to configure Group Policy for Microsoft Error Reporting, technical details are available at http://technet.microsoft.com/en-us/library/cc754364.aspx.

Help

What This Feature Does:

DPM does not include an online help function. Help files are shipped with the product, but it does have some links to KB articles.

Microsoft Update

What This Feature Does:

Microsoft Update is a service that provides Windows updates as well as updates for other Microsoft software.

Information Collected, Processed, or Transmitted:

For details about what information is collected and how it is used, see the Update Services Privacy Statement at http://update.microsoft.com/microsoftupdate/v6/privacy.aspx?ln=en-us.

Use of Information:

For details about what information is collected and how it is used, see the Update Services Privacy Statement at http://update.microsoft.com/microsoftupdate/v6/privacy.aspx?ln=en-us.

Choice/Control:

For details about controlling this feature, see the Update Services Privacy Statement at http://update.microsoft.com/microsoftupdate/v6/privacy.aspx?ln=en-us.

Microsoft Update is not enabled by default by DPM but can be enabled during the installation process by setting a checkmark by “Use Microsoft Update when I check for updates (recommended)” during the “Microsoft Update Opt-in” stage of the Setup Wizard. To disable Microsoft Update, the user will have to go to the Control Panel in Windows and disable it from there.